Entwicklung eines methodischen Ansatzes zur Durchführung von PSA der Stufe 1 für Kraftwerksstandorte mit Small Modular Reactors

Development of a Methodological Approach for Performing Level 1 PSA for Nuclear Power Plant Sites With Small Modular Reactors

GRS - 781

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Entwicklung eines methodischen Ansatzes zur Durchführung von PSA der Stufe 1 für Kraftwerksstandorte mit Small Modular Reactors

Development of a Methodological Approach for Performing Level 1 PSA for Nuclear Power Plant Sites With Small Modular Reactors

Technischer Bericht

Florian Berchtold
Manuel Obergfell
Siegfried Babst
Gerhard Mayer
Marina Röwekamp
Jan Stiller

September 2024

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen RS1596 durchgeführt.

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

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

GRS - 781
ISBN 978-3-910548-74-9

Deskriptoren
Multi-Modul-PSA, Probabilistische Sicherheitsanalyse, PSA der Stufe 1, Small Modular Reactor

Kurzfassung

Eine wesentliche Zielsetzung des Forschungs- und Entwicklungsvorhaben RS1596 bestand darin, die methodischen Grundlagen für eine probabilistische Sicherheitsbewertung (PSA) von Small Modular Reactors (SMRs) zu entwickeln. Die Weiterentwicklung und Anpassung von Methoden zur probabilistischen Sicherheitsanalyse (PSA) der Stufe 1 für herkömmliche Leistungsreaktoren erfolgte dabei auf der Basis internationaler Anforderungen an PSA und einer umfangreichen Recherche zu den Anforderungen an SMR-Konzepte und Dokumenten zu den geplanten technischen Umsetzungen dieser Konzepte für unterschiedliche Arten von SMRs.

Die Verifizierung der entwickelten Methoden für die grundlegenden Schritte zur Erstellung einer PSA der Stufe 1 für SMR erfolgte anhand eines repräsentativen Anlagenkonzepts. Der bereits vollständig entwickelte SMR VOYGR™ von NuScale mit bis zu zwölf Reaktormodulen wurde ausgewählt und eine PSA der Stufe 1 zunächst für ein Modul und darauf aufbauend für die ganze Anlage mit zwölf Reaktormodulen erstellt.

Basierend auf international veröffentlichter Ereignislisten wurden die möglichen auslösenden Ereignisse für die Anlage identifiziert und deren Eintrittshäufigkeiten quantifiziert. Mögliche Unfallabläufe, die sich aus den auslösenden Ereignissen heraus entwickeln könnten, wurden identifiziert und mittels Ereignisablaufanalysen untersucht. Die Systemausfallwahrscheinlichkeiten der eingesetzten betrieblichen Systeme und Notfallsysteme wurden über Fehlerbäume quantifiziert. Diese Systeme werden in ähnlicher Form auch in anderen SMRs verwendet, dazu zählen beispielsweise das Nachwärmeabfuhrsystem und das Notkühlsystem.

Eine Besonderheit bei SMRs ist, dass diese Systeme meist passiv ausgelegt sind. Das heißt, dass nach der Initialisierung des Systems keine aktiven oder mechanischen Komponenten wie Ventile oder Pumpen eingesetzt werden, sondern die Systeme nur auf physikalischen Prinzipien für einen Naturumlauf, wie Auftriebskräften, Wärmeübertragung und Phasenübergängen, beruhen. Die möglichen Auswirkungen, die zu einem funktionalen Versagen des Naturumlaufes in einem passiven System beitragen und damit zu einem Systemausfall führen können, wurden analysiert.

Die Kernschadenhäufigkeiten wurden aus der PSA der Stufe 1 für ein einzelnes Reaktormodul bestimmt und sieben unterschiedliche Endzustände als Basis für eine PSA der Stufe 2 unterschieden. Im Leistungsbetrieb zeigten sich vor allem das funktionale Ver-

sagen des Naturumlaufes im Primärkühlkreis und der Ausfall der Stromversorgung nach einem anlageninternen Brand als häufigste Ursache für einen Kernschaden.

Das PSA-Modell für ein einzelnes Reaktormodul wurde auf zwölf baugleiche Module in der gleichen Anlage als Mehrblock-PSA erweitert. Es wurden insbesondere mögliche Ausfälle aus gleicher Ursache in mehreren Modulen quantifiziert, auslösende Ereignisse in mehreren Modulen bestimmt, ein einfaches Fehlermodell für die Betriebsmannschaft, die für alle Module gleichzeitig zuständig ist, entwickelt und für die Systeme überarbeitet, die von mehreren Modulen genutzt werden.

Die Multi-Modul-PSA besteht aus speziell dafür entwickelten Ereignisablaufanalysen und Fehlerbäumen. In den Minimalschnitten zeigt sich ein Ereignisablauf mit einer besonders hohen Anforderung an die Betriebsmannschaft, wenn nach einem anlageninternen Brand das System zur automatischen Auslösung der Sicherheitssysteme in sechs Modulen gleichzeitig ausfällt und alle notwendigen Systeme zur Unfallbeherrschung in den sechs Modulen von Hand gestartet werden müssen.

Abstract

One of the main objectives of the research and development project RS1596 was to develop the methodological basis for a probabilistic safety assessment (PSA) of small modular reactors (SMRs). The enhancements and adaptation of methods for Level 1 probabilistic safety analysis (PSA) for conventional nuclear power reactors has been carried out based on international requirements for PSA and extensive research regarding the requirements for SMR concepts and documents on the intended technical implementation of these concepts for different types of SMRs.

The verification of the methods developed for the basic steps for the preparation of a Level 1 PSA for SMRs has been carried out for a representative reactor concept. The NuScale SMR VOYGR™ with up to twelve reactor modules, which has already been fully developed, has been selected and a Level 1 PSA developed, first for one reactor module and, based on this, for the entire plant with twelve reactor modules.

Based on internationally published event lists, the potential initiating events for the plant have been identified and their occurrence frequencies quantified. Possible accident sequences that could develop from the initiating events have been identified and analysed by means of event sequence analyses. The system failure probabilities of the implemented operational and emergency systems have been quantified using fault trees. These systems, for example the residual heat removal system and the emergency cooling system, are also used in a similar manner in other SMRs.

A special feature of SMRs is that these systems are usually designed to be passive. After initialisation, the system does not rely on active or mechanical components such as valves or pumps but solely on physical principles for natural circulation, such as heat transfer, buoyance forces and phase transitions. Possible effects which may contribute to a functional failure of the natural circulation have been analysed.

The core damage frequencies have been determined within the Level 1 PSA for a single reactor module. Seven different end states have been distinguished forming the basis for a Level 2 PSA. During power operation, particularly the functional failure of the natural circulation in the primary circuit and the loss of the power supply have been identified as the main causes of core damage.

The PSA model for a single reactor module has been extended to twelve identical modules of the same plant as a multi-unit PSA. In particular, possible failures in several reactor modules by a common cause have been quantified, initiating events determined for several modules, and a simple fault model has been developed for the operating team being which is responsible for all modules simultaneously, and revised for those systems shared by several modules.

The multi-module PSA consists of specifically developed event sequence analyses and fault trees. The minimal cut sets show an event sequence with a particularly high demand on the operating team if the system for automatically actuating the safety systems in six modules fails simultaneously after a plant internal and all systems required to control the accident in the six modules have to be started manually.

Inhaltsverzeichnis

1 Einführung

Im vorliegenden Bericht werden Methoden und Werkzeuge für probabilistische Sicherheitsanalysen für Small Modular Reactors (SMRs) nach aktuellem Stand von Wissenschaft und Technik beschrieben und auf eine ausgewählte repräsentative Anlage, einem SMR von NuScale, angewendet. Diese Anlage ist allerdings nur für SMRs mit Druckwasserreaktor (DWR) repräsentativ; diese Art der Anlagen ist unter den bisherigen SMR-Anlagen allerdings weit verbreitet und die entsprechenden Konzepte sind teilweise schon gut ausgearbeitet.

Die Vielfalt der bisherigen SMR-Konzepte ist erheblich, was eine exakte Definition des Begriffs SMR schwierig macht. Die folgenden wesentliche Merkmale ermöglichen eine Annäherung an eine strikte Definition entsprechend /PIS 21/ und /SCH 21/:

- Leistung: SMRs haben typischerweise eine elektrische Leistung zwischen 10 MW und 300 MW und eine maximale thermische Leistung von 1 GW.
- Modularität: SMR-Anlagen bestehen in der Regel aus mehreren gleichartigen Reaktormodulen an einem Standort. Verschiedene Anlagenteile können von mehreren Modulen verwendet werden (z. B. die Nachwärmesenke, die Aufbereitung von Deionat, ein System zur Flutung des Sicherheitsbehälters).
- Herstellung und Transport: Reaktormodule können zur Kostenreduktion in Kleinserie gefertigt und als fertiges Modul an den Anlagenstandort transportiert werden.
- Kommerzielle Nutzung: Die Nutzung der Energie ist recht flexibel, Möglichkeiten sind neben der Stromerzeugung auch beispielsweise die Nutzung von Prozesswärme und der Einsatz zur Meerwasserentsalzung.
- Kühlmittel: Als Kühlmittel kommt überwiegend leichtes Wasser zum Einsatz.
- Kostenminimierung: Die Herstellungskosten oder auch Betriebskosten lassen sich z. B. durch eine Serienfertigung der Komponenten und Strukturen oder vergleichsweise schnelle Genehmigungsverfahren aufgrund der Einfachheit der Anlage im Vergleich zu herkömmlichen Anlagen verringern.
- Qualität: Eine Fabrikfertigung mit einer standardisierter Qualitätssicherung und Produktprüfständen führt zu einer höheren Qualität der größeren Komponenten.
- Risiken: Finanzielle Risiken, z. B. wetterbedingte Projektverzögerungen bei Fertigung und Errichtung werden durch eine Fabrikfertigung reduziert.

- Technologie: Die Nutzung fortschrittlicher Technologien (z. B. passiver Systeme), inhärenter Sicherheitsmerkmale und neuartiger Systemauslegungen wurde bisher nicht in Genehmigungsverfahren geprüft. Die Konzepte setzen typischerweise auf ein hohes Maß an Automatisierung und eine sparsame Verwendung aktiver Komponenten (insbesondere Pumpen) bei sicherheitsrelevanten Systemen im Vergleich zu aktuellen Leichtwasserreaktoren.

Verschiedene Organisationen, u. a. die IAEA, die OECD/NEA und die U.S. NRC, verwenden einige dieser Merkmale für ihre Definition von SMRs. Das am häufigsten genannte Merkmal ist die Leistung, an zweiter Stelle folgen Herstellung und Transport /SCH 21/.

Bei verschiedenen SMR-Konzepten gibt es besondere Auslegungsmerkmale, die zu einer inhärenten Sicherheit der Anlagen oder zumindest zu einer wesentlich erhöhten Sicherheit einer SMR-Anlage gegenüber konventionellen Reaktoren beitragen /IAE 17/. Ein Beitrag zur erhöhten Sicherheit ist beispielsweise durch die niedrigere Reaktorleistung und dem damit verbundenen niedrigeren Radionuklidinventar gegeben. Dies führt zu geringeren Quelltermen und einer kleineren Evakuierungszone im Fall eines auslegungsüberschreitenden Ereignisses.

SMR-Konzepte versuchen darüber hinaus auch die Schwachstellen bestehender Kernkraftwerke zu vermeiden. Das dynamische Verhalten der geplanten Anlagen (z. B. hohe Wärmekapazitäten, niedriger Arbeitsdruck und Ausnutzung der Naturkonvektion) kann so ausgelegt sein, dass eine inhärente Sicherheit unter abnormalen oder Unfallbedingungen gewährleistet ist. Zur Gewährleistung einer inhärenten Sicherheit sind typischerweise passive Sicherheitssysteme vorgesehen. Allerdings ist bzgl. der passiven Systeme von der internationalen Begriffsverwendung auszugehen. Entsprechend der Beschreibung der IAEA /IAE 91/ können passive Systeme auch über aktive Ventile in Betrieb genommen werden, was nach deutschem Verständnis für passive Systeme nicht möglich wäre /BEC 17/.

In den europäischen Ländern (außer Russland) werden derzeit noch keine SMRs betrieben. Es existieren jedoch unterschiedliche Konzepte und Designs für SMR /IAE 18/, z. B. von Herstellern aus China (Universität Tsinghua), Russland (AKME Engineering, OKBM), Republik Korea (KAERI), Japan (Mitsubishi, Toshiba), USA (Flibe Energy, General Atomic, GE-Hitachi, NuScale, University of California), Großbritannien (Moltex Energy), Kanada (Terrestrial Energy) oder Dänemark (Seaborg Technologies). Ver-

schiedene SMRs befinden sich derzeit in der Genehmigungsphase (z. B. NuScale in den USA), haben bereits eine Lizenz (SMART in der Republik Korea) oder werden als Pilotanlagen gebaut (z. B. KLT-40S in Russland, HTR-PM in China und CAREM in Argentinien) bzw. wurden bereits gefertigt (z. B. RITM-200M in Russland).

Eine globale Übersicht über die SMR-Konzepte ist u. a. in /IAE 17/ zu finden, vgl. auch die nachfolgende Tab. 1.1.

Tab. 1.1 Überblick über verschiedene grundsätzliche SMR-Konzepte /IAE 17/

Design	Type	Technology developers	Modules per plant	Total plant MW(e)
		Water cooled		
CAREM-25	iPWR	CNEA, Argentina	1	27
SMART	iPWR	KAERI, Republic of Korea	1	100
mPower	iPWR	B&W Generation mPower, USA	2	360
NuScale	iPWR	NuScale Power, USA	12	540
ACP100	iPWR	CNNC/NPIC, China	2	200
IRIS	iPWR	IRIS Consortium/Polimi, Italy	1	325
VBER-300	iPWR	OKBM Afrikantov, Russian Federation	1	300
Westinghouse SMR	iPWR	Westinghouse Electric, USA	1	225
SMR-160	iPWR	Holtec, USA	1	160
AHWR300-LEU	HWR	BARC, India	1	300
		Marine based		
KLT-40S	FPU, TNPP	OKBM Afrikantov, Russian Federation	2	70
Flexblue	Seabed moored	DCNS, France	1	160
		Gas cooled		
HTR–PM	HTGR	INET, Tsinghua University, China	2	210
EM^2	HTGR	General Atomic, USA	1	240
PBMR	HTGR	Eskom PBMR, South Africa	1	165
		Liquid metal cooled fast spectrum		
SVBR-100	LMFR	AKME-engineering, Russian Federation	1	101
BREST-OD-300	LMFR	RDIPE, Russian Federation	1	300
PRISM	LMFR	GE Nuclear Energy, USA	4	1244
4S	LMFR	Toshiba, Japan	1	10–30

Vor diesem Hintergrund kann nicht ausgeschlossen werden, dass in näherer Zukunft auch in Europa fortschrittliche SMRs zur Energieversorgung in Betrieb gehen werden. Um das von SMRs ausgehende Risiko bewerten zu können, sind probabilistische Sicherheitsanalysen erforderlich. Angesichts des radiologischen Gefahrenpotenzials durch das Inventar eines SMR (insbesondere mit höheren Leistungen von ca. 300 MW pro Reaktormodul) ist die Erstellung einer PSA der Stufe 1 für einen solchen Reaktortyp sinnvoll, um – wie in vielen Ländern gefordert – ergänzend zu deterministischen Sicherheitsbewertungen das Sicherheitsniveau auch mit probabilistischen Methoden ermitteln zu können.

Das Ziel des Forschungs- und Entwicklungsvorhabens RS1596 bestand darin, einen methodischen Ansatz für eine PSA der Stufe 1 für einen ausgewählten, fortschrittlichen SMR entsprechend dem Stand von Wissenschaft und Technik zu entwickeln, da die in Deutschland gebräuchlichen PSA-Vorgaben für bestehende Kernkraftwerke mit Leichtwasserreaktoren vom Typ DWR und SWR erstellt wurden und nicht unmittelbar auf neue Reaktorkonzepte, insbesondere nicht ohne Weiteres auf SMRs (entsprechend der o. g. Definition), übertragbar sind.

Es besteht wissenschaftlicher Konsens darüber, dass auch für SMRs mit Leistungen von weniger als ca. 200 MW die Nachzerfallsleistung sicher abgeführt und eine Kernschmelze verhindert werden muss. Aufgrund der geringen thermischen Leistungen kommen in den SMR-Konzepten hierzu vermehrt passive Sicherheitssysteme zum Einsatz, deren Funktion ausschließlich auf physikalischen Phänomenen, wie freier Konvektion, Verdampfung oder Kondensation, basiert /SCH 19/.

Die GRS hat darüber hinaus (siehe /NIE 17/, /NIE 17a/) konzeptionelle Analysen von SMR-Konzepten durchgeführt. Wesentliche Arbeiten zur Sicherheit und zu internationalen Entwicklungen von SMRs hat die GRS zudem im Rahmen der BMWi-Vorhaben RS1507 /BUC 15/, RS1519 /BUC 16/ und insbesondere RS1521 /BUC 15a/ durchgeführt. Ziele des letzteren Vorhabens waren

- die Schaffung eines fundierten Überblicks zur SMR-Thematik,
- die Identifizierung wichtiger Fragestellungen für die Reaktorsicherheitsforschung und zukünftiger Forschungs- und Entwicklungsvorhaben sowie
- die Identifizierung des Anpassungsbedarfs von Rechencodes.

Darüber hinaus hat die GRS SMR-Projekte in verschiedenen Ländern verfolgt. Hier wurden insbesondere die politischen Rahmenbedingungen, die kerntechnische Infrastruktur und der Ablauf der Genehmigungsverfahren betrachtet.

In Bezug auf probabilistische Sicherheitsanalysen für SMR bestanden zu Beginn des Forschungs- und Entwicklungsvorhabens RS1596 bei der GRS allerdings noch keine Erfahrungen.

Die durchgeführten Arbeiten dienen dazu, die Kenntnis der GRS hinsichtlich der Anlagen- und Sicherheitstechnik fortschrittlicher SMR-Konzepte deutlich zu erhöhen und die Fachleute damit in die Lage zu versetzen, probabilistische Bewertungen der Sicherheit von SMR vornehmen zu können. Dabei standen insbesondere die Bewertung inhärent sicherer bzw. passiver Systeme sowie die Beurteilung der Ausgewogenheit der Sicherheitssysteme von SMRs im Vordergrund.

2 Stand von Wissenschaft und Technik zur PSA der Stufe 1 für Small Modular Reactors

Die Durchführung von PSA-Studien für Kernkraftwerke stellt in Deutschland mittlerweile eine etablierte Vorgehensweise dar, um das Sicherheitsniveau der Anlagen zu ermitteln, technische Schwachstellen zu identifizieren und die Bereitstellung bzw. Verbesserung von Prozeduren im präventiven und mitigativen Bereich zu veranlassen. Darüber hinaus ist die Durchführung von PSA im Rahmen der periodischen Sicherheitsüberprüfungen vorgeschrieben. Die Anforderungen an die Durchführung von PSA für Kernkraftwerke finden sich im deutschen kerntechnischen Regelwerk, u. a. in den Sicherheitsanforderungen an Kernraftwerke /BMU 15/ sowie dem PSA-Leitfaden /BMU 05/ mit seinen Fachbänden zu PSA-Methoden und -Daten /FAK 05/, /FAK 05a/ und /FAK 16/.

Anders sieht es mit der Erstellung einer PSA für SMRs aus. Da in Deutschland keine SMRs gebaut werden bzw. keine Zulassungsverfahren beantragt wurden, gibt es auch keine Veranlassung, im deutschen Regelwerk methodische Anforderungen an eine probabilistische Sicherheitsanalyse für diese festzulegen. Um eine PSA der Stufe 1 für einen SMR zu erstellen, sind deshalb internationale Quellen heranzuziehen, deren Auswertung nachfolgend dargestellt ist.

2.1 Anforderungen der IAEA

Vor dem Hintergrund der Reaktorunfälle von Fukushima Dai-ichi stellt das IAEA-TECDOC-1785 /IAE 16a/ Ansätze und Maßnahmen zur Verbesserung des gestaffelten Sicherheitskonzeptes („defence in depth“) wassergekühlter SMR-Auslegungskonzepte zur Berücksichtigung extremer naturbedingter, übergreifender Einwirkungen von außen im Sicherheitskonzept vor. Für Mitgliedsstaaten, die mit der Nutzung von Kernenergie mittels SMRs beginnen, werden eingehende Empfehlungen (indicative requirements) vorgestellt, mit denen derartige Unfälle verhindert werden können.

In diesem TECDOC wird zunächst der Unfallablauf von Fukushima erläutert, danach werden für verschiedene SMR-Designs die Sicherheitsmerkmale diskutiert, bevor die empfohlenen Gegenmaßnahmen herausgearbeitet werden.

Bezüglich der Sicherheitsmerkmale werden für verschiedene Arten von SMR die spezifischen Ausführungen diskutiert. Im Einzelnen handelt es sich dabei um:

- Abschaltsysteme,
- Wärmeabfahrsysteme,
- Sicherheitseinspeisesysteme (Hochdruck/Niederdruck),
- Aufbau und Technik des Sicherheitsbehälters (Containment) sowie
- mitigative Systeme für Unfallszenarien.

Bezüglich der durchzuführenden Sicherheitsanalysen nimmt das TECDOC Bezug auf die IAEA Safety Requirements SSR-2, Rev. 1 /IAE 16/.

Tabelle 15 des TECDOCs stellt Betrachtungen für eine Nutzung der PSA bzw. Risikobewertung und -management dar. Eine Übersetzung der wesentlichen Inhalte, die sich auf die Referenzen /LYU 11/ und /IAE 16/ beziehen, sind in der nachfolgenden Tab. 2.1 zu finden.

Tab. 2.1 Betrachtungen für eine Nutzung der PSA bei Risikobewertung und -management

Tiefe des gestaffelten Sicherheits-konzepts (Defence in Depth)	**Kritisches Problem**	**Überlegungen und zusätzliche technische Vorkehrungen**
Verhinderung (Stufe 1)	Cliff-Edge-Effekt	Die PSA-Ergebnisse helfen bei der Bestimmung von Systemen, die gestärkt werden müssen, damit bei steigendem Ausmaß von Einwirkungen von außen der Cliff-Edge-Effekt vermieden werden kann. Dies kann einerseits in Bezug auf die Kernschadenshäufigkeit und andererseits auf die Häufigkeit großer, früher Freisetzungen als Verbesserungsziel berücksichtigt werden. Die Verhinderung großer, früher Freisetzungen kann eine Möglichkeit der Entwicklung mitigativer Maßnahmen darstellen, um Freisetzungsmengen zu reduzieren oder Freisetzungsverläufe zu verzögern.
Vermeidung (Stufe 1)	Erfolgskriterien	Erfolgskriterien können definiert werden, um niedrigere Wahrscheinlichkeiten von Kernschäden in häufigeren und großen frühen Freisetzungen in selteneren Ereignissen zu erkennen. – Aktualisierungen der Analysekriterien bzgl. übergreifender Einwirkungen von außen und deren Häufigkeitsbestimmung – Beachtung gemeinsam auftretender übergreifender Einwirkungen

Tiefe des gestaffelten Sicherheits-konzepts (Defence in Depth)	Kritisches Problem	Überlegungen und zusätzliche technische Vorkehrungen
		– Untersuchung der Auswirkungen extremer übergreifender Einwirkungen von außen – Untersuchungen zu mehreren Reaktormodulen – Berücksichtigung von Ausfällen der für die Störfallbeherrschung ausgelegten Systeme
Vermeidung (Stufe 1), Unfallablauf-kontrolle und Begrenzung schwerer Unfälle	Gesamt-umfängliche PSA	Aufgrund verschiedenster Möglichkeiten für Komponentenunverfügbarkeiten und Unfallabläufe sollte eine gesamtumfängliche PSA durchgeführt werden.
Vermeidung (Stufe 1)	Konzept zum Risikobewusst-sein	SMRs sollten das Konzept zum Risikobewusstsein von der Planungsphase an berücksichtigen, um die Stabilität der Sicherheitsebenen zu stärken. Eine umfassende und konservative Analyse sollte für alle Maßnahmen der Betriebsmannschaft angenommen werden, um den Einfluss einer externen Einwirkung auf die Verfügbarkeit, die Leistung und menschliche Fehler zu berücksichtigen. Das Konzept zum Risikobewusstsein wird in Anlagenüberarbeitungen berücksichtigt.

In den IAEA Safety Requirements SSR-2 (Rev. 1) /IAE 16/ werden zum einen Anforderungen an technische Auslegungsmerkmale zum sicheren Betrieb von Kernkraftwerken und zum anderen Anforderungen an deterministische wir probabilistische Sicherheitsanalysen gestellt (Requirement 42). Besondere Hinweise hinsichtlich SMRs finden sich nicht.

Spezifischer greift der Bericht der IAEA „Technology Roadmap for Small Modular Reactor Deployment“ /IAE 21a/ SMR-spezifische Themen auf. Treibende Kräfte bei der Entwicklung von SMRs sind u. a.

- durch die Möglichkeit einer flexiblen Energieerzeugung einen erweiterten Kundenkreis anzusprechen und neue Anwendungsbereiche für die Kernenergie zu erschließen;
- Kraftwerke zur Energieerzeugung aus fossilen Energieträgern ersetzen bzw. die Netzstabilität auch bei einem hohen Anteil zyklisch einspeisender Kraftwerke aus erneuerbaren Energien zu gewährleisten. Dies ist technisch realisierbar, aber eine Herausforderung aus Sicht der beteiligten Wirtschaftsunternehmen.

- sicherheitstechnische Verbesserungen durch inhärente und passive Sicherheitseinrichtungen;
- eine bessere Finanzierbarkeit;
- Anwendungsgebiete außerhalb der Stromerzeugung;
- Schaffung von Angeboten für abgelegene Regionen mit schlechter Netzinfrastruktur;
- Schaffung von Möglichkeiten für Synergien zwischen nuklearer und alternativer Energieerzeugung.

Das Dokument enthält jedoch keine technischen Details zu SMRs.

Dokumente der IAEA und weitere Literaturquellen werden im Folgenden bzgl. besonders relevanter, SMR-spezifischer PSA-Fragestellungen behandelt. Zunächst wird in Abschnitt 2.2 die besonderen Anforderungen der Leittechnik in SMR behandelt. Viele SMR-Konzepte basieren auf einem höheren Automatisierungsgrad im Vergleich zu bisherigen Reaktoranlagen. Darüber hinaus werden die Systeme in SMRs häufiger passiv ausgelegt, Arbeiten zu passiven Systemen sind in Abschnitt 2.3 beschrieben.

Einige PSA-Konzepte sehen die Verwendung mehrerer Reaktoren in einer Anlage vor. Konzepte zur Erstellung einer Mehrblock- oder Multi-Modul-PSA werden in Abschnitt 2.4 behandelt. Darüber hinaus gibt es noch weitere Möglichkeiten zur Erweiterung der PSA-Methoden, die Entwicklung moderner PSA-Werkzeuge ist in Abschnitt 2.5 dargelegt.

2.2 Leittechnik in Small Modular Reactors

Der IAEA-Bericht „Instrumentation and Control Systems for Advanced Small Modular Reactors” /IAE 17/, analysiert die besonderen Anforderungen an SMRs im Bereich der Leittechnik. Einige SMRs zeichnen sich durch einen höheren Automatisierungsgrad gegenüber herkömmlichen Reaktoranlagen aus. Darüber hinaus gibt es integrierte Konzepte, die die Hauptkühlmittelpumpen oder die Steuerstabantriebe innerhalb des Reaktordruckbehälters (RDB) anbringen. Hier gibt es Einschränkungen in den Möglichkeiten zur Überwachung dieser Komponenten und Umgebungsbedingungen, welche die Lebensdauer der Komponenten einschränken können. Weitere SMR-Konzepte verwenden alternative Kühlmittel, wie flüssige Metalle, Natrium, Blei oder Gase. Messsensoren müs-

sen für diese Kühlmittel chemisch geeignet sein und die unterschiedlichen Druck- und Temperaturbedingungen aushalten.

Spezifisch für integrierte Druckwasserreaktoren sind die nachfolgend aufgeführten Herausforderungen anzugehen, wobei es sich um DWR mit in den Reaktordruckbehälter integrierten Dampferzeugern, Steuerstabantrieben oder integriertem Druckhalter handelt.

Messtechnische Herausforderungen bei integrierten Dampferzeugern

Konzentrische, schraubenförmige Dampferzeuger sind in mehreren SMR-Konzepten vorhanden. Im Unterschied zu Dampferzeugern aus herkömmlichen Reaktoranlagen wird hier die sekundäre Seite durch Rohrleitungen geführt. Der genaue Füllstand in den dünnen Rohrleitungen auf der Sekundärseite und damit verbunden das sekundärseitige Kühlmittelinventar des Dampferzeugers sind sehr schwer exakt zu messen. Darüber hinaus arbeitet dieses Dampferzeugerkonzept mit einem geringeren Kühlmittelinventar auf der Sekundärseite der Dampferzeuger im Vergleich zur Primärseite. Dabei kommt es zu schnellem dynamischem Verhalten bei Lastwechseln. Zur Verhinderung der Austrocknung der Rohrleitungen ist eine sehr zuverlässige Speisewasserversorgungsteuerung erforderlich. Eine konventionelle, füllstandorientierte Steuerung des Frischdampfes (FD) scheidet damit aus, eine Steuerung über den Massendurchsatz von Frischdampf und Speisewasser erscheint zielführender. Im Bereich des Frischdampfes sind die Zustandsgrößen Druck und Temperatur für die genaue Bestimmung des Frischdampfdurchsatzes besonders wichtig. Gegenüber konventionellen Anlagen mit Füllstandssensoren müssen die Unsicherheiten in der Messung des Frischdampfdurchsatzes deutlich verringert werden.

Auch auf der Primärseite können aufgrund der geometrischen Verhältnisse keine Durchflussmesser, die auf dem Prinzip der Venturi-Durchflussmessung beruhen, verwendet werden. Bisherige SMR-Konzepte sehen keine Durchflussmessungen auf der Primärseite vor. Darüber hinaus ist die Verwendung von Füllstandssensoren im Primärkühlkreislauf durch die integrierte Bauweise und die Vermeidung von Durchführungen durch den RDB schwierig. Im Fall eines schweren Unfalls sind Füllstandssensoren besonders wichtig, wie die Unfälle von Three Miles Island und Fukushima Dai-ichi zeigen. Messungen von durchflussinduzierten Vibrationen in den Dampferzeuger sind aufgrund der folgenden beiden Faktoren schwierig:

- Aufgrund anderer benötigter Sensoren ist der Platz für die Sensoren begrenzt.
- Die Sonden sind in Kontakt mit strömendem Reaktorkühlmittel und damit chemischen Zersetzungsprozessen und radioaktiver Strahlung ausgesetzt.

Die chemischen Einflüsse auf die längerfristige Zersetzung der Dampferzeuger-Rohrleitungen und besonders die zusätzliche radioaktive Belastung und längere Inspektionsintervalle müssen untersucht werden. Hier könnten auch zusätzliche Sensoren zum Einsatz kommen. Rohrfraß und Korrosion könnten zu kleine Lochöffnungen führen, die eine kleine Leckage von Kühlmittel aus dem Primärkühlkreislauf in den Sekundärkühlkreislauf verursachen. Die messtechnische Erfassung solcher Leckagen ist schwierig und könnte eine chemische Untersuchung notwendig machen. Größere Leckagen können durch Unterschiede im Massendurchfluss detektiert werden.

Integrierte Steuerstabantriebe

Integrierte Steuerstabantriebe sind eine Herausforderung für die Reaktorentwickler aufgrund der notwendigen Zuverlässigkeit im Betrieb und bei der Wartung während einer Revision. Im Reaktorbetrieb stellt die Überwachung der Funktionalität aller Bauteile der Steuerstabantriebe eine Herausforderung dar und erfordert Material- und Verlässlichkeitsuntersuchungen unter Realbedingungen (Druck-, Temperatur- und Strahlungsbedingungen). Darüber hinaus sind Durchführungen elektrischer Leitungen zur Steuerung und Überwachung der Steuerstabantriebe notwendig. Dies erfordert Zuverlässigkeitsuntersuchungen ebenso wie Untersuchungen zu Langzeiteffekten, wie einer möglichen Zersetzung der Kabelisolierung – diese Fehlerquelle kann einen Einfluss auf die Ergebnisse einer PSA haben. Mögliche Fehler müssen immer in einen sicheren und vorhersagbaren Zustand führen. Die Verwendung von integrierten Steuerstabantrieben sind in den Konzepten von Westinghouse und dem Reaktor des Konsortiums Generation mPower geplant.

Integrierter Druckhalter

Der integrierte Druckhalter ist oberhalb des RDB angeordnet. Im Vergleich zu bisherigen Druckwasserreaktoren ist der integrierte Druckhalter breit und von geringerer Höhe. Dies erschwert die Überwachung von Druck- und Inventaränderndem Transienten. Schnelle Druck- und Inventaränderungen erfordern empfindlichere und schnellere Sensorik. Druckschwankungen im RDB wirken sich zeitnah auf den Druckhalter aus; dies muss

entweder in der Auslegung von Regelkreisen oder durch Einsatz von Dämpfungselemente berücksichtigt werden, um zyklische Rückwirkungseffekte zu vermeiden. Aufgrund des schlechteren Zugangs zum Druckhalter für Wartungs- und Revisionsarbeiten muss der Druckhalter stabiler und für längere Betriebsphasen ausgelegt sein.

Primärkühlmitteldurchflussmessung

Eine große Herausforderung für integrierte Druckwasserreaktoren ist die Messung der Durchflussraten in den komplexen Durchflusspfaden. Ohne die Verfügbarkeit langer gerader Rohrleitungen oder die Möglichkeiten zum Einbau von Durchflusseinschränkungen oder Venturi-Düsen ist der Einsatz von konventioneller Messtechnik für die Durchflussmessung schwierig. Alternative Messungen über die Leistungsaufnahme möglicher Primärpumpen oder ähnliches müssen bzgl. Genauigkeit, Unsicherheitsbereichen und Handhabbarkeit überprüft werden.

Messtechnische Erfassung eines Naturumlaufes: Niedrige Durchflüsse und Niederdruckanfahrbedingungen

Einige integrierte Druckwasserkonzepte verwenden eine Naturkonvektion im Primärkühlkreislauf (z. B. CAREM, NuScale und AB6-M). Diese Konzepte benötigen eine Anfahrroutine, um Neutronen- und thermohydraulische Instabilitäten im Niederdruckbereich zu verhindern. Messinstrumente zur Überwachung verschiedener Arten von Instabilitäten (z. B. Geysir-Effekt, Dichte- oder Druckwellen) sind notwendig. Der einzige mit Naturkonvektion betriebene Reaktor ist der Dodewaard Reaktor in den Niederlanden. Die einzigen zugelassenen Reaktoren mit Naturkonvektion sind der Economic SBWR (*S*implified Boiling *W*ater *R*eactor) und CAREM.

Überwachung der Kühlmittelfüllstände im Unfallverlauf

Zusätzlich zu konventionellen Messmethoden könnten Ultraschallsensoren oder thermische Sensoren zur Füllstandüberwachung verwendet werden. Diese Messsensorik könnte ein Bestandteil des gestaffelten Reaktorschutzes (Sicherheitsebenen bzw. defence in depth) zur Risikoabschätzung im Unfallverlauf sein. Thermische Füllstandsmessungen basieren auf Detektoren mit temperaturabhängigen Widerständen oder Thermoelementen.

Direkt verbundene Hauptkühlmittelpumpen: Durchfluss- und Vibrationsmessungen

Viele SMR-Konzepte verwenden integrierte Hauptkühlmittelpumpen, welche sich innerhalb des RDB befinden oder mit diesem direkt verbunden sind. Dadurch kann auf externe Rohrleitungen verzichtet und das Risiko für große Kühlmittelverluststörfälle vermieden werden. Aus Sicht der Instrumentierung und Reaktorkontrolle reduzieren sich die Möglichkeiten zum Einbau von Überwachungssensoren. Durchflussmessungen müssen direkt hinter der Pumpe durchgeführt werden, wo wichtige Schweißnähte verlaufen. Darüber hinaus ergeben sich auch Platzprobleme bezüglich der Temperatur- und Vibrationsüberwachung. Insbesondere bei horizontalen Pumpen ist die Vibrationsmessung aufgrund erhöhter Belastung der Lagerung besonders wichtig. Diese Herausforderungen erfordern eine Instrumentierungsauslegung, die den verfügbaren Platz um die Pumpe gut ausnutzt und dabei alle notwendigen Messungen abdeckt.

Westinghouse hat beispielsweise ein integriertes Überwachungssystem für die Hauptkühlmittelpumpen des AP 1000 entwickelt, welches so viele nützliche Daten wie möglich trotz Platzeinschränkungen erhebt. Ähnliche Konzepte können auch für integrierte Druckwasserreaktoren nützlich sein.

Kernüberwachung im unteren Plenum

Viele Druckwasserreaktoren verwenden Durchführungen im unteren Plenum zur Temperatur- und Neutronenflussmessung. Für integrierte Druckwasserreaktoren müssten in diesem Zusammenhang zwei technische Herausforderungen betrachtet werden:

- Der Platz für Durchführungen im unteren Plenum ist geringer; möglicherweise müssten die Durchführungen von mehreren Messinstrumenten gemeinsam verwendet werden.
- Der Abstand zwischen dem unteren Plenum und der Kerngitterplatte ist größer als in herkömmlichen Druckwasserreaktoren.

Die Kerninstrumentierung muss somit nicht nur dünner, sondern auch länger sein. Die Instrumentierung könnte sich unter Belastung zur Seite hin verformen und müssen entsprechend stabiler ausgelegt sein. Darüber hinaus müssen die Sensoren durch kleinere Öffnungen passen.

Weitere grundsätzliche Herausforderungen für die SMR-Konzepte ergeben sich bei Anlagen mit mehreren Reaktoren. Hier können Anlagenteile von mehreren Reaktoren gemeinsam verwendet werden. So gibt es z. B. Konzepte mit einer Turbine für mehrere Reaktoren oder einer gemeinsam verwendeten Warte und eine Betriebsmannschaft, die für mehrere Reaktoren verantwortlich ist. Gründe für den Einsatz einer einzigen Betriebsmannschaft für mehrere Reaktoren sind häufig wirtschaftlicher Natur: Geschäftsmodelle, einige Reaktorkonzepte generieren nicht genügend Umsatz aus der Stromerzeugung, um ein große Betriebsmannschaft zu finanzieren. Dieses Argument ist für Aufsichtsbehörden nicht relevant. Ein weiterer Grund für den Einsatz von nur einer Betriebsmannschaft für mehrere Reaktormodule sind Behauptungen, dass diese Reaktoren wesentlich einfacher zu bedienen sind, aufgrund

- vorhersehbarer und bedienerfreundlicher Fahrweisen (inhärente Kernstabilität, langsame Verfahrzeiten und Einschluss des Brennstoffs in der Folge eines Ereignisses),
- weniger Strukturen, die im Betrieb überwacht und bewegt werden müssen,
- passiver Sicherheitssysteme, die autonom die Anlage steuern und bei einem Unfallszenario lange ohne Eingriffe der Betriebsmannschaft auskommen,
- verbesserter Automatisierung,
- verbesserter Schnittstellen zum Reaktorfahrer, welche die Aufmerksamkeit für die Situation verbessern und die Notwendigkeit für Eingriffe reduzieren.

Für SMR-Anlagenkonzepte mit nur einer Betriebsmannschaft für mehrere Reaktormodule ist ein größeres Maß an Automatisierung der Anlage und der einzelnen Reaktoren erforderlich. Die Automatisierung beinhaltet einerseits den Routinebetrieb, andererseits jedoch auch die Identifizierung von Betriebsstörungen und dem Versagen von Komponenten (es ist dabei davon auszugehen, dass diese Komponenten größtenteils nicht zugänglich sind). Die Maßnahmen zur Störfallbeherrschung und ein anomaler Betrieb müssen vom Reaktorschutz automatisch durchgeführt werden. Eine entsprechende Automatisierung kommt in Kernkraftwerken bisher nicht vor. Der Nachweis für ein entsprechend reibungslos arbeitendes Schutzsystem für mehrere Reaktoren mit höherem Automatisierungsgrad und einer Aufsichtsfunktion muss noch erbracht werden.

Für einen zuverlässigen und wirtschaftlichen Betrieb von SMRs ist es notwendig, eine dauerhafte Überwachung kritischer Komponenten zur entwickeln und bereits in der Aus-

legungsphase zu berücksichtigen /UPA 13/. Auslegungsüberlegungen beinhalten folgende Aspekte:

- Verlängerte Brennstoffzyklen verlängern die Zeitabstände zwischen den Wartungs- und Inspektionsarbeiten. Kritische Komponenten sollten deshalb direkt im Betrieb überwacht werden (online monitoring).
- Die Ausfallsicherheit von Systemen ist im Hinblick auf Standorte mit schlechter nuklearer Infrastruktur besonders wichtig. Ausfallsicherheit setzt typischerweise neben einer robusten Auslegung auch eine Fehlererkennung und -analyse voraus.
- Bei einem Anlagenfernbetrieb könnten halbautomatische Eingriffe vorgenommen werden, die ein verlässliches Wissen über den aktuellen Anlagenzustand erfordern, um von außerhalb regelnd eingreifen zu können.
- Ökonomische Überlegungen führen zu einer fortschrittlichen Zustandsüberwachung und Funktionskontrolle. Weniger Wartungsarbeiten erfordern eine zuverlässige und fortschrittliche Zustandsüberwachung, um die Sicherheit und Zuverlässigkeit zu verbessern.
- Neue Kraftwerkstypen, Komponenten und Instrumentierungsmethoden können auch von einer fortschrittlichen Zustandsüberwachung profitieren.
- Einige Komponenten, wie die internen Komponenten in einem integrierten Primärkühlsystem, könnten für eine konventionelle Überwachungs- und Wartungstechnik nicht zugänglich sein. Hier sind automatisierte online Überwachungsmethoden notwendig.

2.3 Untersuchungen zur Zuverlässigkeit passiver Systeme

Eine detaillierte Untersuchung der Veröffentlichungen zur Zuverlässigkeit passiver Systeme, insbesondere mit Naturumlauf, wurde von der GRS /BEC 17/ durchgeführt. Mögliche Mechanismen, die zu einem funktionalen Versagen des Naturumlaufes führen können, sind u. a.

- eine thermische Schichtung in einem großen Volumen, welches einen Einfluss auf die Konvektion hat,
- Carryover und Carryunder, das Mitreißen von Flüssigkeit in einem Gas bzw. das Mitreißen von Gasbläschen in einer Flüssigkeit,

- Kondensation in der Gegenwart von nicht-kondensierbarem Gas, alle anderen Pl
- Vortex-Bildung an einem Abfluss,
- begrenzter Durchfluss durch Ausbildung einer der Fließrichtung entgegengesetzten Gasphasenströmung,
- Strömungsinstabilitäten, im Leistungsbetrieb können auch gekoppelte Leistungsschwankungen auftreten,
- Formverlustfaktoren durch Ablagerungen (z. B. an Sieben oder Rohrleitungen des Wärmetauschers) oder zunehmende Rohrrauhigkeiten.

Für eine Zuverlässigkeitsbestimmung der passiven Systeme, insbesondere der ausreichenden Wärmeabfuhr über ein System mit Naturkonvektion, ist eine Systemanalyse unerlässlich. In diesem Zusammenhang ist es wichtig, zunächst die Mindestanforderungen an das System zu kennen. d. h., welche Kühlleistung das Nachzerfallswärmeabfuhrsystem mindestens leisten muss und welche physikalischen Randbedingungen sind dazu mindestens erforderlich. Beispielsweise könnten nach einem Leckstörfall im Sekundärkühlkreis die Wassermenge und der Systemdruck niedriger im Vergleich zu einer Transiente (z. B. Ausfall der Hauptwärmesenke). sein Im Fall von durch Wärmeübertragung abhängigen Naturumlaufsystemen, z. B. Naturumläufe im Primär- und Sekundärkühlsystem, sind die Anfangs- und Randbedingungen gekoppelt. In diesen Fällen liegt es nahe, beide Naturumläufe gemeinsam zu analysieren.

Die Systemanalyse zur Zuverlässigkeitsbewertungen passiver Systeme (ausgenommen aktive Komponenten wie Ventile, die separat betrachtet werden) basiert in der Regel einerseits auf Zuverlässigkeitsanalysen, die eine Bewertung über eine Kombination aus Thermohydraulikanalysen (zur Bestimmung der Versagensoberfläche) und Wahrscheinlichkeitsverteilungen des Systemzustandes ermöglichen. Andererseits sollte auch das funktionelle Versagen des passiven Systems betrachtet werden, z. B. Unsicherheiten in den physikalischen Modellen, die den Versagensanalysen zugrunde liegen. Beispielhaft für die Zuverlässigkeitsanalyse kann die Studie von Nayak et al. /NAY 09/ angeführt werden. In dieser Studie wird die Zuverlässigkeit des Isolationskühlsystems (Isolation Condensor System) des indischen Schwerwasser-SMR AHWR (Advanced Heavy Water Reactor) über die APSRA-Methode (*A*ssessment of *P*assive System *R*eliability): Untersuchung der Zuverlässigkeit passiver Systeme) bestimmt. Unter anderem wurden folgende Ausfallgründe und physikalische Effekte in Betracht gezogen:

- zu niedrige Naturumlaufrate,
- Instabilität des Naturumlaufs,
- kritische Wärmestromdichte während Oszillationsvorgängen,
- Kondensationsverhalten bei vorhandenen, nicht-kondensierbaren Gasen,
- thermische Schichtung im Wasserbecken.

Ein erster Teil der Analyse ist die Bewertung der Systemparameter in Bezug auf einen möglichen Einfluss auf die Funktion der Nachzerfallswärmeabfuhr. Diese Bewertung basiert auf Experteneinschätzungen bzgl. zweier Aspekte:

- der Wahrscheinlichkeitsverteilung der Parameter sowie
- dem möglichen Einfluss der Parameter innerhalb der Wahrscheinlichkeitsverteilung auf die Funktion der Nachzerfallswärmeabfuhr.

Für eine entsprechende Parameteranalyse kommen Parameter der folgenden Bereiche in Betracht /IAE 14/:

- Prozessparameter, wie beispielsweise Durchflussrate, Temperatur, Leistung, Druck, Wärmestrom, thermische Energie und Gesamtmenge an Kühlmittel im System,
- geometrische Parameter, wie beispielsweise die Wärmeübergangsfläche, Rohrlängen und Rohrdurchmesser,
- Materialparameter, wie beispielsweise Wärmeleitfähigkeiten, Oberflächenrauhigkeiten oder auch Oxidschichten,
- thermohydraulische Parameter, wie beispielsweise Modellparameter, Parameter zur Bestimmung der Reynolds- oder Nusseltzahlen.

Die Analyse führte zu folgenden Ergebnissen bzgl. der identifizierten kritischen Parameter:

- Der Anteil an nicht-kondensierbaren Gasen im Nachzerfallswärmeabfuhrsystem führt zu einer wesentlichen Verschlechterung der Kondensation. In den Zeiten zwischen den regelmäßigen Entlüftungen können sich kleine Mengen an nicht-kondensierbaren Gasen im System sammeln.

- Im Kühlbecken kann es zu einer thermischen Schichtung mit höheren Temperaturen im oberen Bereich des Kühlbeckens kommen. Bei niedrigen Kühlbeckenfüllstände liegen die Wärmetauscher im oberen Bereich und sind von der höheren Temperatur (im Vergleich zur mittleren Kühltemperatur im Kühlbecken) auf der Sekundärseite betroffen. Neben der mittleren Kühlmitteltemperatur des Kühlbeckens sind daher auch die Parameter Füllstand und Temperaturschichtung in der Analyse zu betrachten. Bei sehr geringen Füllständen ist es darüber hinaus möglich, dass die Sekundärseite der Wärmetauscher nicht vollständig benetzt ist. Die verwendeten Parameter sind:
  - Wassertemperatur der Wärmesenke und
  - Füllstand der Wärmesenke.

Explizit nicht als kritischer Parameter wurde der Grad der Verschmutzung der Oberflächen des Wärmeübergangs betrachtet. Dieser Parameter könnte einen großen Einfluss auf die Funktion der Nachzerfallswärmeabfuhr haben, allerdings sind Verschmutzungen aufgrund der Reinhaltung durch das Kühlmittelaufbereitungssystem und der verwendeten Materialien gering, zudem wurde dieser Parameter bereits in der Systemauslegung berücksichtigt. In der weiteren Analyse konnte mit Hilfe thermohydraulischer Rechnungen eine Versagensoberfläche entsprechend Abb. 2.1 ermittelt werden. Diese trennt das Gebiet der erfolgreichen Durchführung der Maßnahme (success region) von dem Gebiet eines Versagens der Maßnahme (failure region) im Parameterraum. Aus Darstellungsgründen ergibt sich eine Beschränkung der Darstellung der Versagensoberfläche auf maximal drei Parameter; in diesem Fall sind alle kritischen Parameter im Diagramm berücksichtigt, der Anteil nicht-kondensierbarer Gase im System, der Anteil frei liegender Wärmeübergangsflächen (aufgrund eines niedrigen Beckenfüllstandes) und die Beckentemperatur.

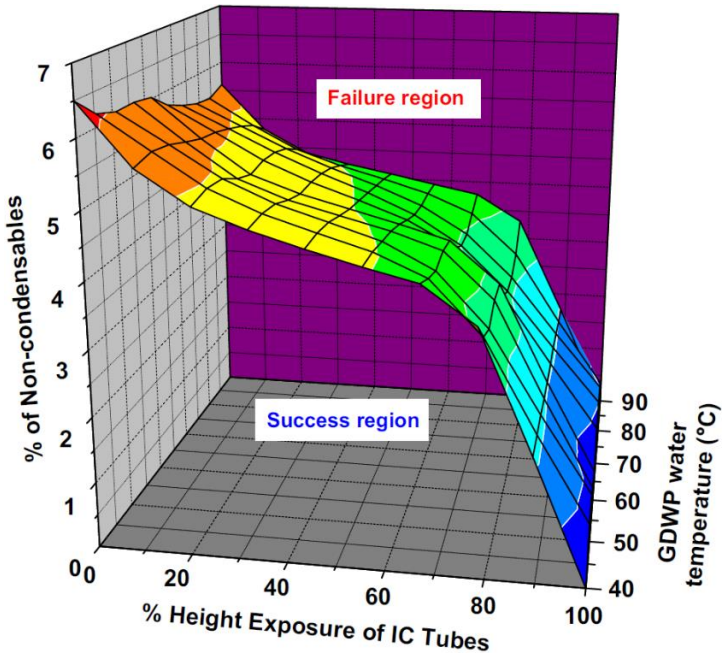


Abb. 2.1 Versagensoberfläche bzgl. der Parameter „Anteil nicht-kondensierbarer Gase im System“, „Anteil frei liegender Wärmeübergangsflächen“ und „Beckentemperatur“ /NAY 09/

Ein weiteres Beispiel für die Untersuchung funktionaler Zuverlässigkeiten ergibt sich in der Studie von Mezio et al. /IAE 14/, /NAY 07/. Hier wurden die Zuverlässigkeitsmethoden für passive Sicherheitsfunktionen (RMPS) auf die passiven Systeme (den Isolationskondensator und die Mitteldruckeinspeisung) eines CAREM-ähnlichen integralen Reaktors angewendet. Die Methode ist in Abb. 2.2 skizziert. Zwei Unfallabläufe wurden untersucht, ein Station Blackout (SBO) und ein kleines Leck unter SBO-Bedingungen.

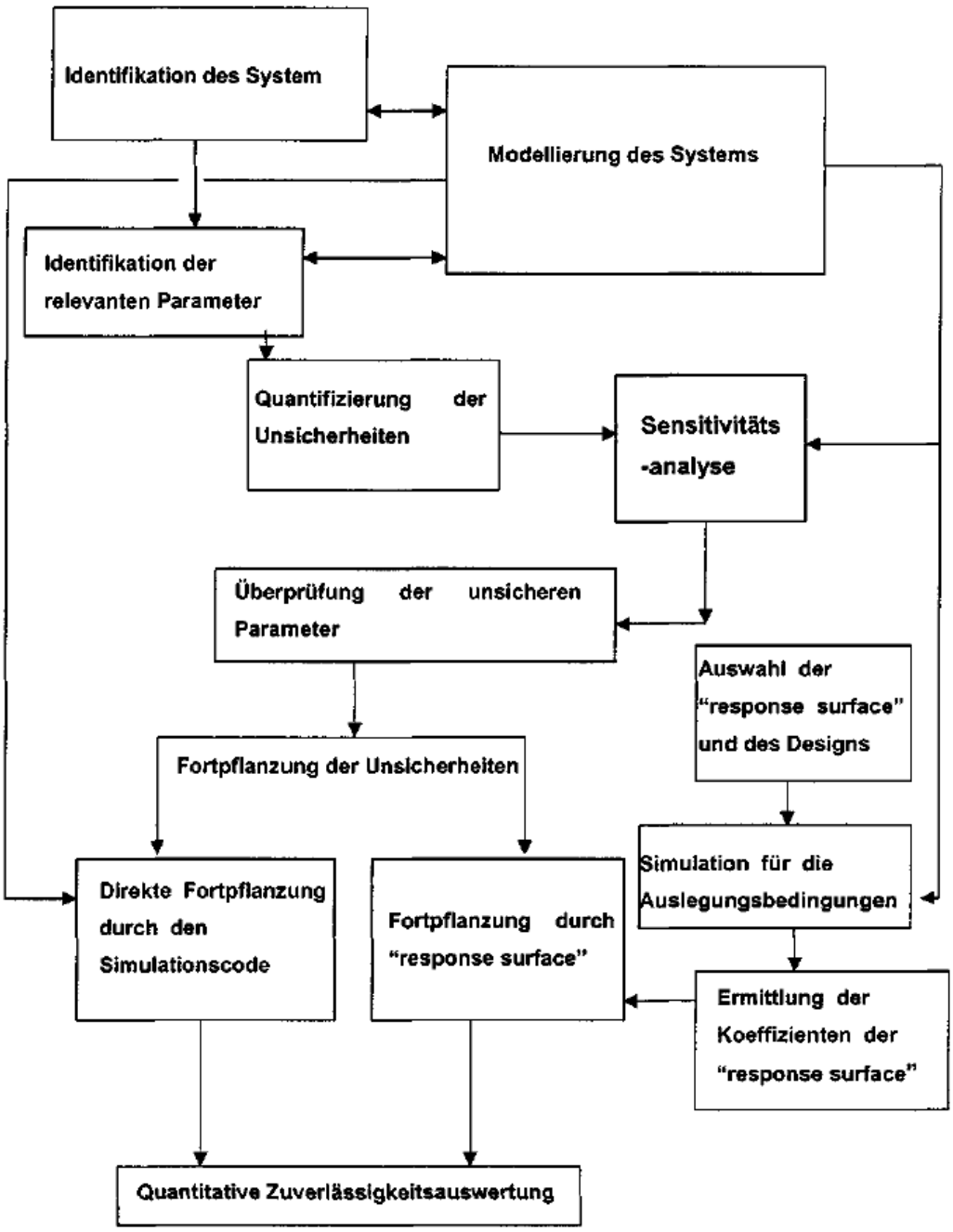


Abb. 2.2 Vorgehen bei der Durchführung einer RMPS nach /MUE 04/

Für den SBO konnten insgesamt 17 Parameter (siehe Tab. 2.2) identifiziert werden, für das kleine Leck ergaben sich 24 Parameter /MEZ 14/.

Tab. 2.2 Kritische Parameter für die thermohydraulischen Untersuchungen zur Zuverlässigkeit des Nachzerfallswärmeabfuhrsystems aus /IAE 14/

Parameters		Normalized Nominal value	Range		Distribution
1	Reactor power	1	0.95	1.05	TNORMAL
2	SCRAM delay	1	0.68	1.6	TLOGNORMAL
3	SCRAM: safety rods total drop time	2	1.2	4	TLOGNORMAL
4	Decay power factor (ANS79-3)	1	0.85	1.2	TLOGNORMAL
5	Reactor nominal pressure	1	0.99	1.01	TNORMAL
6	SCRAM: pressure set point	1.06	1.05	1.07	TNORMAL
7	IC: pressure set point	1.11	1.1	1.12	TNORMAL
8	RPV dome water level	1	0.75	1.25	TNORMAL
9	Primary circuit mass flow rate	1	0.96	1.04	TNORMAL
10	IC pool temperature	1	0.55	2.38	TLOGNORMAL
11	IC tube thickness	1	0.89	1.11	TNORMAL
12	IC fouling	5.71 10-3	0	5.71 10-2	TLOGNORMAL
13	RPV dome (steam zone) heat losses	1.00 10-3	5.00 10-4	1.50 10-3	TNORMAL
14	Safety Valves Set-Point	1.14	1.13	1.15	TNORMAL
15	IC pool's boiling heat transfer coefficient	1	0.5	1.5	TNORMAL
16	IC tube's condensation heat transfer coefficient	1	0.5	1.5	TNORMAL
17	Feedback reactivity coefficients	1	0	1.05	UNIFORM

Darüber hinaus wurde der Einfluss der Nodalisierung des Primärkühlsystems untersucht. Drei unterschiedlich detaillierte Modelle der RDB-Kuppel (Englisch: dome) wurden in den Analysen gerechnet. Eine Darstellung der entsprechenden Nodalisierungen findet sich in der nachfolgenden Abb. 2.3.

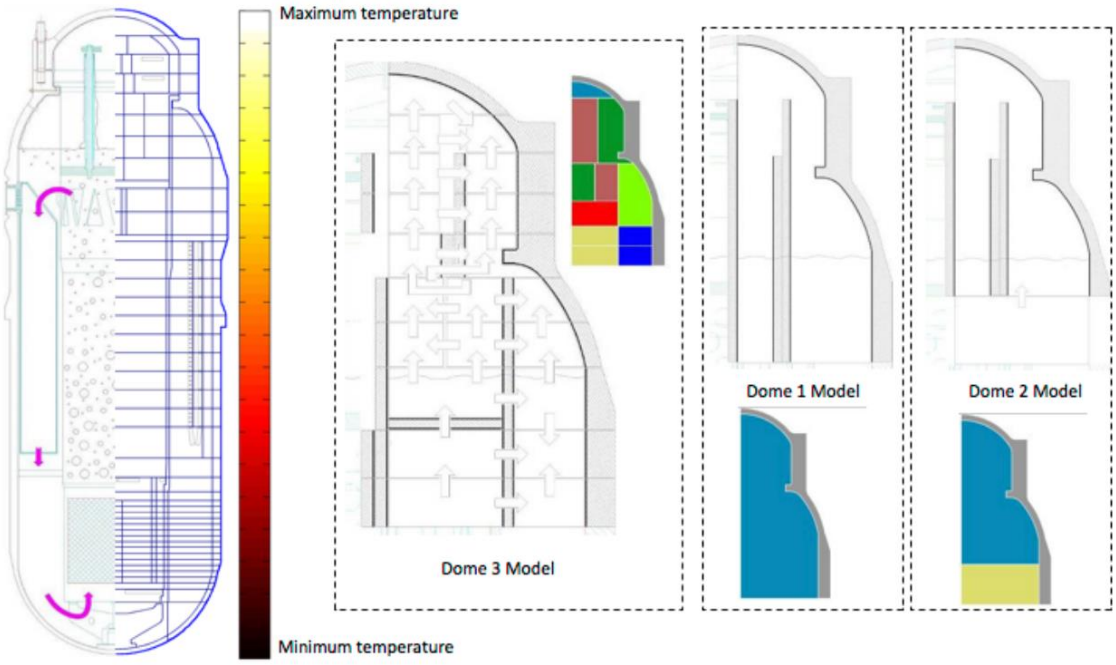


Abb. 2.3 Nodalisierung des Primärkühlsystems mit der höhenabhängigen Temperaturverteilung links und den Kuppel-Modellen rechts /MEZ 14/

In einer Sensitivitätsanalyse ergaben sich als einflussreiche Parameter auf die Kühlleistung der Isolationskühlung (siehe Abb. 2.4):

- die Nachzerfallswärme,
- die Ablagerungen an den Wärmeübergangsflächen und
- die Wärmeübergangskoeffizienten.

Die Versagenswahrscheinlichkeit konnte mit einem Konfidenzniveau von 0,99 bestimmt werden. In der einfachsten Nodalisierung des Druckhalterbereichs im oberen Plenum mit einem Kontrollvolumen (Kuppel 1) liegt die Versagenswahrscheinlichkeit bei 1,5 E-03, mit zwei vertikalen Kontrollvolumina (Kuppel 2) bei 8.8 E-04 und in der detaillierten Nodalisierung (Kuppel 3) bei einem wesentlich niedrigeren Wert von 1 E-05.

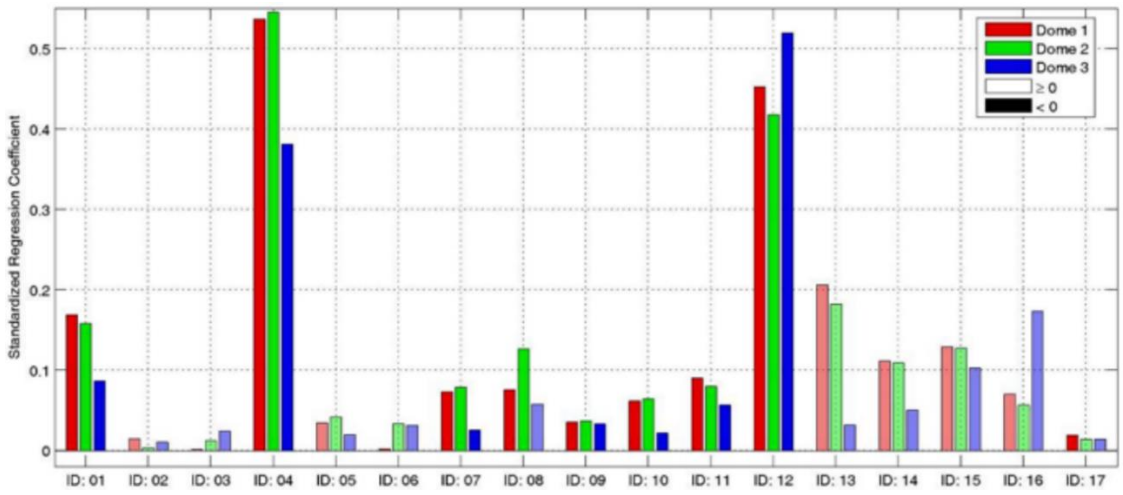


Abb. 2.4 Sensitivitätsanalysen für drei unterschiedliche Nodalisierungen des oberen Plenums (unterschiedliche Farben), von einem Model mit einem Knoten (Dome 1) über zwei vertikale Knoten (Dome 2) bis zu einer detaillierten Modellierung (Dome 3) /MEZ 14/

Eine ähnliche Liste kritischer Parameter wurde bei der Analyse eines möglichen Nachzerfallswärmeabfuhrsystems für ein 900 MW-Druckwasserreaktors nach /IAE 14/ und /MAR 05/ gefunden; das Ergebnis findet sich in Tab. 2.3. Eine Sensitivitätsanalyse zeigt eine große Abhängigkeit der Kühlleistung des Systems von der Menge an nicht-kondensierbaren Gasen im System, der Kühlbeckentemperatur und der Nachzerfallsleistung.

Tab. 2.3 Kritische Parameter eines DWR-Nachzerfallswärmeabfuhrsystems, aus /IAE 14/

Parameter	Type of distribution	Distribution parameters	Estimated range	Typical system application	Basis	Reference
$I_{i=1,2,3}$ Instant at which the isolation valve opens	Composed			RP2	RMPS/Expert judgement	Journal publication Ref. [6]
$X_{i=1,2,3}$ Rate of non-condensable at the inlet of the exchanger	Exponential	$\lambda = 182$ $\mu = 0$		RP2	RMPS/Expert judgement	Journal publication Ref. [6]
$L_{i=1,2,3}$ Initial pool water level	Truncated normal	$\mu = 4.5$ $\sigma = 0.6$		RP2	RMPS/Expert judgement	Journal publication Ref. [6]
$T_{i=1,2,3}$ Initial pool water temperature	Truncated normal	$\mu = 303$ $\sigma = 20$	280-368	RP2	RMPS/Expert judgement	Journal publication Ref. [6]
$C_{i=1,2,3}$ Fouling of exchanger tubes	Truncated normal	$\mu = 15$ $\sigma = 5$	0-30	RP2	RMPS/Expert judgement	Journal publication (III)
$R_{i=1,2,3}$ Number of broken tubes in the exchanger	Exponential	$\lambda = 7$ $\mu = 0$		RP2	RMPS/Expert judgement	Journal publication Ref. [6]
PUI Percentage of nominal core power	Truncated normal	$\mu = 100$ $\sigma = 1$	98-102	RP2	RMPS/Expert judgement	Journal publication Ref. [6]
PP Pressure in the pressurizer	Truncated normal	$\mu = 155$ $\sigma = 4$	153-166	RP2	RMPS/Expert judgement	Journal publication Ref. [6]
ANS Decay of residual power (ANS law)	Truncated normal	$\mu = 10$ $\sigma = 5$	0-20	RP2	RMPS/Expert judgement	Journal publication Ref. [6]
$NGV_{i=1,2,3}$ Real secondary level in the three steam generators	Truncated normal	$\mu = 12.78$ $\sigma = 0.30$	12.08-13.91	RP2	RMPS/Expert judgement	Journal publication Ref. [6]

Der IAEA-Bericht „Natural Circulation Phenomena and Modelling for Advanced Water Cooled Reactors“ /IAE 12/ ordnet die Phänomene im Zusammenhang mit einem Naturumlauf in zwei Kategorien ein:

- Phänomene aufgrund einer Wechselwirkung zwischen Primärkühlkreislauf und Sicherheitsbehälter sowie

– Phänomene aufgrund einer speziellen Reaktorkonfiguration oder dem Einbau neuer Komponenten.

Eine Liste der in /IAE 12/ beschriebenen Phänomene findet sich in Tab. 2.4. Für eine Validierung von Rechencodes zur Quantifizierung der Phänomene kann auf die gleiche Quelle zurückgegriffen werden. Dort sind Testeinrichtungen und Experimente beschrieben, die Daten zu den Phänomenen liefern.

Tab. 2.4 Liste von Naturumlaufphänomenen

Phänomen	Charakteristische thermohydraulische Einflüsse
Dynamik in großen Flüssigkeitsbecken	Thermische Schichtung Natürliche oder angetriebene Umwälzströmungen und Kreisläufe Dampfkondensation Wärme und Massentransport an die Oberfläche (z. B. Verdampfung) Flüssigkeitsverluste durch kleine Öffnungen
Einfluss nicht-kondensierbarer Gase auf den Kondensationswärmeübergang	Auswirkung des Gemischs auf den Wandwärmeübergang Gemisch in der Wasserphase Gemisch in der Dampfphase Schichtung in großen Behältern bei sehr niedrigen Geschwindigkeiten
Kondensation an Sicherheitsbehälterstrukturen	Kopplung an die Wärmeleitfähigkeit der großen Strukturen
Verhalten der Sicherheitsbehälter-Notfallsysteme	Wechselwirkung mit Primärkühlkreisläufen
Thermofluid-Strömung und Druckverluste in unterschiedlichen geometrischen Anordnungen	Lange Strömungspfade und Strömungspfade am Übergang von großen Rohrleitungen mit Wasserbecken Trennung der Phasen bei niedrigen Reynoldszahlen und laminarer Strömung Lokale Druckabfälle
Naturkonvektion in geschlossenen Kreisläufen	Wechselwirkungen zwischen parallelen Kühlkreisen, innerhalb und außerhalb des RDB Einfluss von nicht-kondensierbaren Gasen Stabilität Rücklauf-Kondensation
Dampf-Flüssigkeits-Wechselwirkung	Direkte Kondensation Druckwellen ausgelöst durch Kondensation
Schwerkraftgetriebene Kühlung und Druckspeicherverhalten	Kernkühlung und Kernflutung
Temperaturschichtung von Flüssigkeiten	Unteres Plenum des RDB Rückströmraum des RDB Horizontale oder vertikale Rohrleitungen

Phänomen	Charakteristische thermohydraulische Einflüsse
Verhalten der Notwärmetauscher und Isolationskondensatoren	Niedrigdruckphänomene
Schichtung und Durchmischung der Borsäure	Wechselwirkung von chemischen und thermo-hydraulischen Eigenschaften Zeitverzögerung bis zur Wirksamkeit der Borsäure
Verhalten im Kernaufbereitungsbehälter (System zur Nachzerfallswärmeabfuhr)	Thermische Schichtung Naturumlauf

Die Phänomene werden nachfolgend kurz zusammengefasst und /IAE 12/ folgend näher erläutert.

Dynamik in großen Flüssigkeitsbecken

Als Beispiel sei auf den Notfallkondensator im SWR-1000 in Abb. 2.5 (rechte Seite) verwiesen. Im Notfall sinkt der Füllstand im RDB, und die U-Rohre im Flutungsbecken füllen sich mit Dampf. Durch Kondensation überträgt sich die Wärme in das Flutbecken.

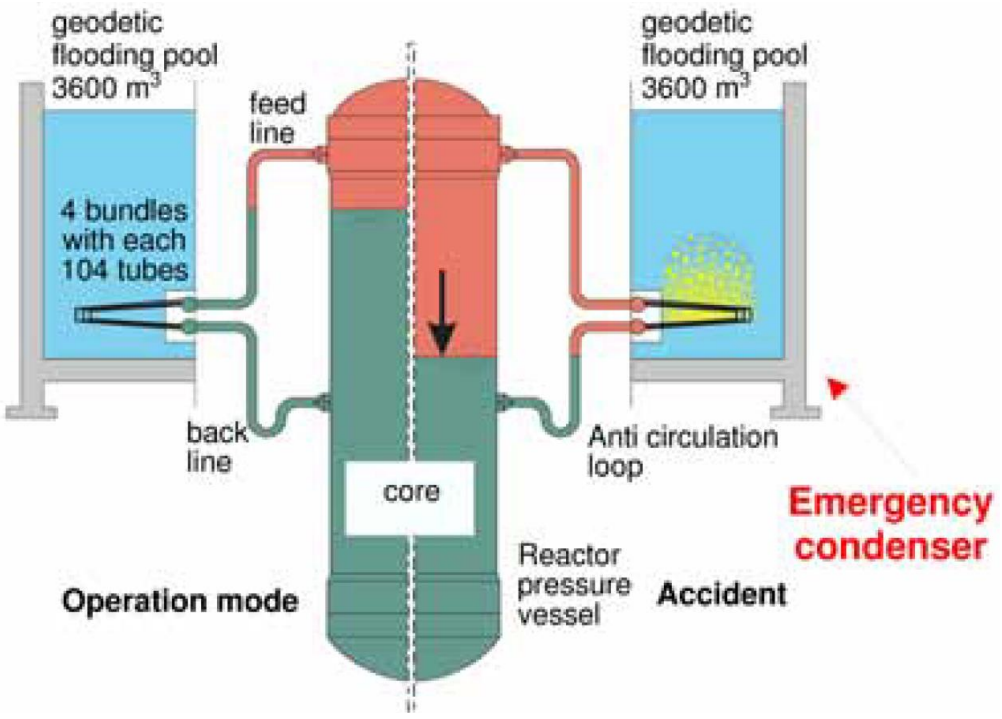


Abb. 2.5 Betriebsschema des eines Notfallkondensators des SWR-1000 /IAE 12/

Einfluss nicht-kondensierbarer Gase auf den Kondensationswärmeübergang

Eine wichtige Größe zur Beschreibung der Kondensation unter einer Atmosphäre mit nicht-kondensierbaren Gasen ist der Massenanteil an nicht-kondensierbaren Gasen. Ein Anteil von 1 % kann den Wärmeübergang der Kondensation um 50 % reduzieren. Dies liegt daran, dass die nicht-kondensierbaren Gase, wie in Abb. 2.6 veranschaulicht, eine Barriere zwischen Kondensatfilm und Dampf bilden. Die Konzentration der nicht-kondensierbaren Gase nimmt zum Film hin deutlich zu, der Dampfanteil entsprechend ab.

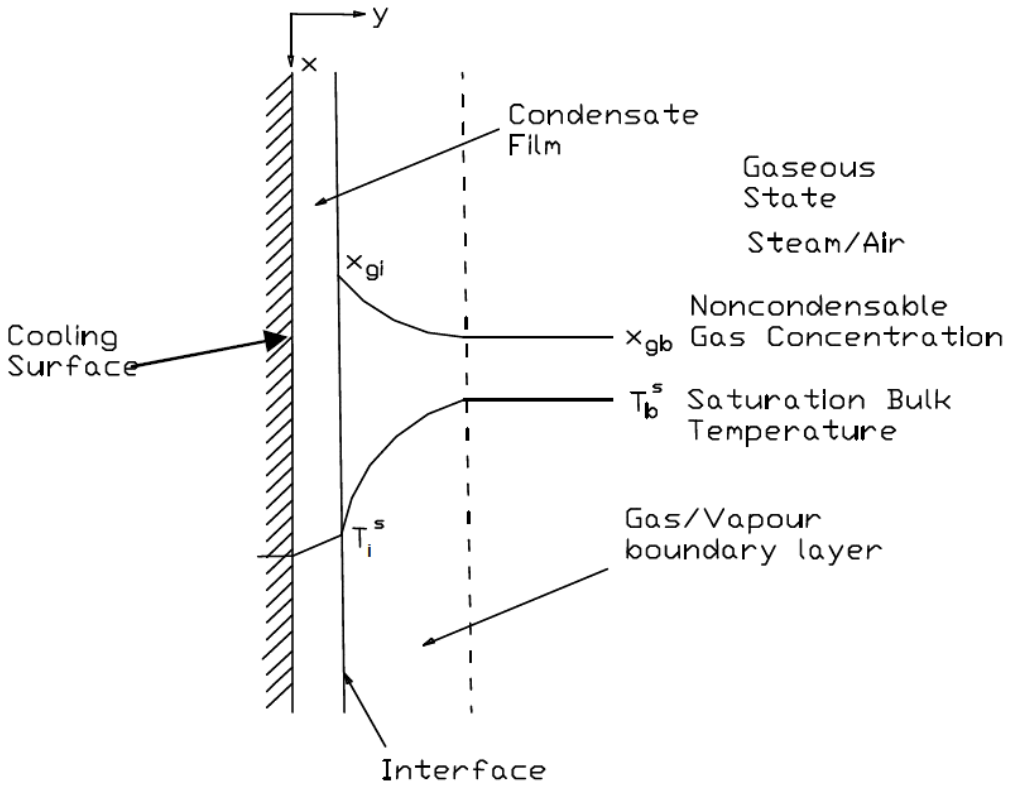


Abb. 2.6 Schematische Darstellung der Kondensation an einer benetzten Oberfläche /IAE 12/

Kondensation an Sicherheitsbehälter-Strukturen

Dieses Phänomen tritt in bestehenden Anlagen bei Fällen von Kühlmittelaustritt in den Sicherheitsbehälter auf. Insbesondere bei Anlagen mit extern gekühltem Sicherheitsbehälter, z. B. in Anlagen vom Type Westinghouse AP, dort wird der Sicherheitsbehälter aus Stahl extern durch einen Wasserstrom aus einem Behälter oberhalb des Sicherheitsbehälters gekühlt.

Verhalten der Sicherheitsbehälter-Notfallsysteme

Ein Beispiel für ein Sicherheitsbehälter-Notfallsystem ist das passive Sicherheitsbehälter-Kühlsystem (PCCS) des General Electric (GE) SBWR. Es handelt sich dabei um ein passives Wärmetauschersystem, welches Wärme aus dem Sicherheitsbehälter in das PCCS-Becken durch Kondensation überträgt (siehe Abb. 2.7). Das über Gravitation funktionierende Kühlsystem (GDCS) liefert Kondensat zur Kernkühlung. Nicht-kondensierbare Gase werden an den Suppression Pool (SP) abgegeben.

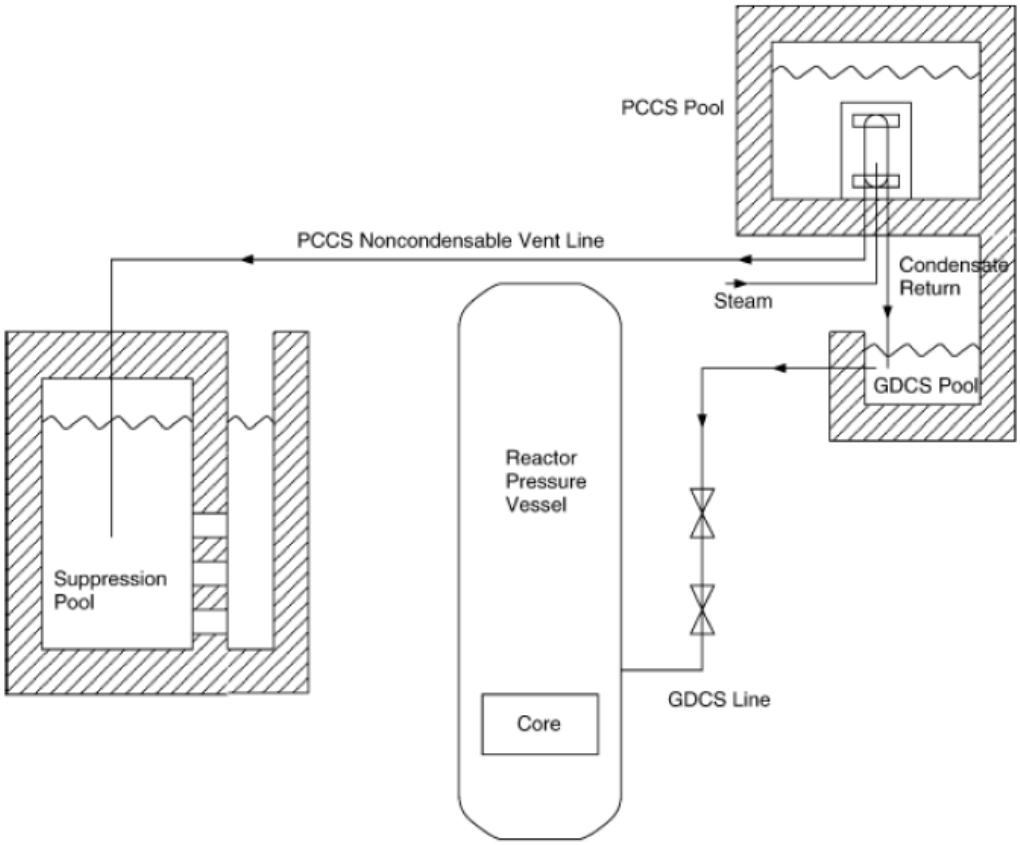


Abb. 2.7 Sicherheitseinrichtungen des GE SBWR /IAE 12/

Thermofluid-Strömung und Druckverluste in unterschiedlichen geometrischen Anordnungen

Ein Druckverlust ist der Druckunterschied zweier Stellen im Kühlsystem. Grundsätzlich kommt es zu Druckverlusten aufgrund von Durchflusswiderständen, Höhenunterschieden, Dichteunterschieden, Änderungen am Strömungsquerschnitt oder Änderungen der Strömungsrichtung. Druckverluste im Naturumlauf spielen eine wichtige Rolle für die Gleichgewichtsströmungsbedingungen, das Verhalten bei transienten Verläufen und die

Stabilitätseigenschaften. In realen Anlagen gibt es verschiedene Komponenten mit unterschiedlichen geometrischen Formen (runde Rohre, Öffnungen/Blenden usw.) und Querschnitten, die unterschiedliche Druckverluste bewirken. Darüber hinaus unterscheidet sich potenziell das Verhalten eines einphasigen Durchflusses von zweiphasigen Durchflüssen. Auch pumpengetriebene Durchflusseigenschaften können von Naturumläufen abweichen. Auch für große Rohrquerschnitte und Objekte, wie das obere und untere Plenum, können die Druckverluste bisher nicht verlässlich vorhergesagt werden.

Naturkonvektion in geschlossenen Kreisläufen

Naturumläufe werden in vielen wassergekühlten Reaktoren möglich und werden zur Störfallbeherrschung genutzt, darunter sind Anlagen vom Typ DWR, VVER-440, WWR-1000, CANDU, SWR und RBMK. Ein Naturumlauf benötigt im einfachsten Fall eine Wärmequelle und eine Wärmesenke, die über Rohrleitungen und einem Transportmedium miteinander verbunden sind. Prinzipiell kann das Kühlmittel auch zeitweise die Rolle der Wärmesenke übernehmen. Externe mechanische Antriebe oder andere treibende Kräfte sind nicht vorhanden. Folgende Naturumlauf-Anordnungen werden in /IAE 12/ näher beschrieben:

- Wärmequelle und Wärmesenke befinden sich im Primärkühlkreislauf. Wärmequelle ist der Kern, er befindet sich auf niedrigerer Höhe als die Wärmesenke, der Dampferzeuger oder die Primärseite des Wärmetauschers.
- Wärmequelle, Kern und Wärmesenke sowie ringförmiger Rückströmraum befinden sich im RDB.
- Die Kühlung der Sicherheitsbehälter-Luft erfolgt durch einen geschlossenen Kreislauf.

Naturumläufe sind bereits in mehreren Anlagen vorgesehen (z. B. nach einem Stromausfall ohne Eigenversorgung). Hier kann zwischen einem nominalen Betrieb ohne Kühlmittelverlust und einem off-nominalen Betrieb mit Kühlmittelverlust[1] unterschieden werden (siehe Tab. 2.5).

[1] Für einen Kühlmittelverluststörfall (KMV) können je nach Größe und Position des Lecks u. a. die Druckverteilung, die Druckverlustbeiwerte und die Umlaufraten variieren.

Tab. 2.5 Bisherige Einsatzbereiche für Naturumläufe in Kernreaktoren /IAE 12/

Reference condition / Reference system	Nominal		Off-nominal	
	1Φ	2Φ	LBLOCA (end phase)	SBLOCA, MCP trip, Other
BWR & RBMK		x	x	x
SG (secondary side)		x		x
PWR, VVER, CANDU (primary system)	x		x	x

Je nach Kühlmittelinventar können folgende Naturumläufe unterschieden werden:

- einphasig (1Φ),
- zweiphasig (2Φ)
- Rückflusskondensation (im Fall eines Wärmesenke, die den höchsten Punkt im Kreislauf einnimmt).

Die unterschiedlichen Naturumlauftypen sind in Abb. 2.8 dargestellt. In der Bildfolge von oben nach unten nimmt die Kühlmittelmenge im Kühlkreislauf ab. Ein einphasiger und wird durch die Auftriebskraft des erwärmten Kühlmittels (temperaturbedingte Dichteänderung) angetrieben. Im zweiphasigen Naturumlauf bewegen sich das Kühlmittel und der Dampf. Für den einphasigen und zweiphasigen Betrieb eines Naturumlaufs sind die Massendurchflussraten der wichtigste Parameter. Bei Rückflusskondensation ist der wichtigste Effekt die Dampfkondensation.

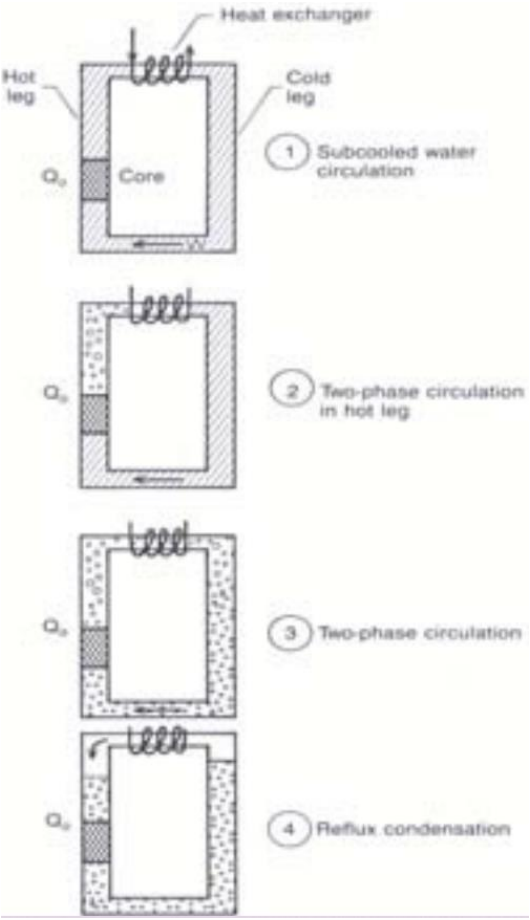


Abb. 2.8 Naturumlauftypen in Abhängigkeit des Kühlmittelinventars /IAE 05/

Zur Beschreibung und Charakterisierung von Naturumläufen sind folgende Schritte wichtig:

- die Untersuchung der Bedingungen, unter welchen sich ein Naturumlauf ausprägt,
- die Leistungsfähigkeit, mit der der Naturumlauf die Kernnachzerfallswärme abführen kann, sowie
- die Untersuchung der Einflüsse von äußeren Parametern auf den Naturumlauf.

Experimentelle Daten zur Abhängigkeit des Kühlmittelinventars und den unterschiedlichen Naturumlaufmoden sind in Abb. 2.9 gezeigt. Auf der x-Achse ist das Kühlmittelinventar aufgetragen und auf der y-Achse zum einen die Nachzerfallsleistung und zum anderen für die Trendkurve der Kühlmittelmassendurchsatz. Für den Massendurchsatzrate ergibt sich typischerweise im zweiphasigen Umlauf das globale Maximum.

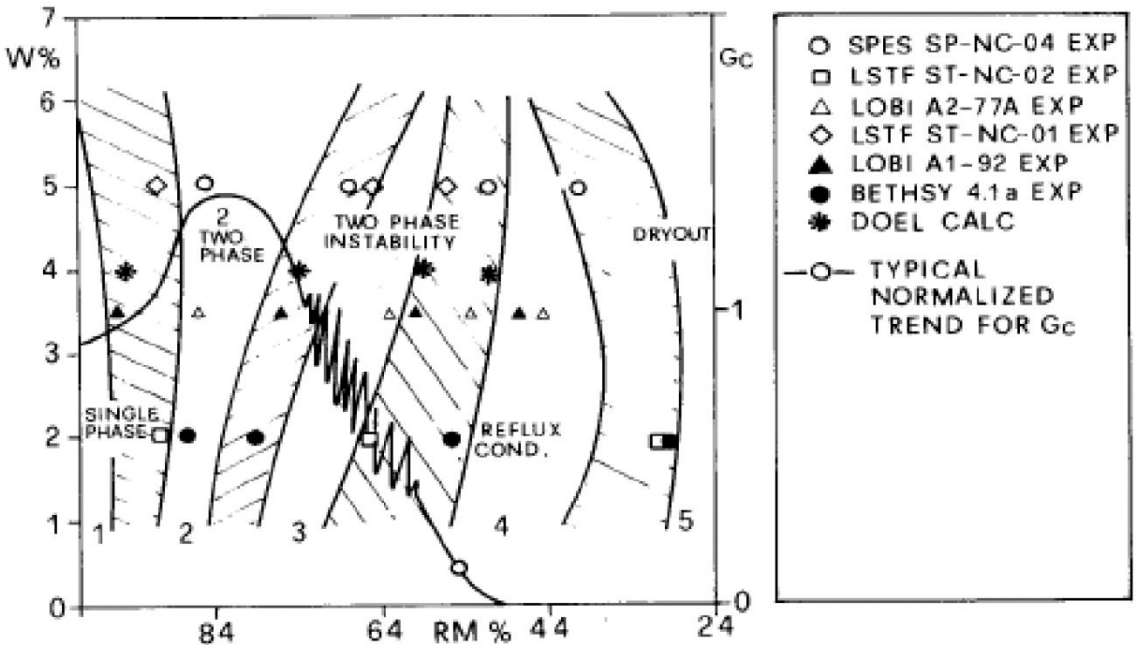


Abb. 2.9 Experimentelle Daten und Berechnungen zu verschiedenen Naturumlauf-Modi /IAE 12/

Ein zusätzlicher Aspekt des Naturumlaufes unter Leckbedingungen ist die Möglichkeit einer Verdünnung der Borsäurekonzentration in Druckwasserreaktoren. Sinkt aufgrund des ausströmenden Kühlmittels der Füllstand im Primärkühlsystem, so ergibt sich eine Energieübertragung in den Dampferzeuger im Reflux-Condenser-Modus. Das erzeugte Kondensat bleibt dabei weitgehend entboriert. Dieses Phänomen wird u. a. in /DAU 05/ und /UMM 10/ diskutiert.

Bekannte Ursachen und Auswirkungen von Strömungsinstabilitäten sind in Tab. 2.6 aufgeführt. Dazu zählt unter anderem die Ledinegg-Instabilität. Dabei handelt es sich Instabilität, die sich in Kühlkanälen beim Übergang von einer Zweiphasen- in eine Einphasenströmung bemerkbar macht. Im Zweiphasenbereich erfährt die Strömung höhere Druckverlust als im Einphasenbereich, der durch eine quadratische Abhängigkeit des Druckverlustes von der Durchflussrate geprägt ist.

Tab. 2.6 Klassifizierung von Strömungsinstabilitäten

Typ der Instabilität	Mechanismus	Charakteristik
Ausschlag in der Durchflussrate oder Ledinegg-Instabilität	Die Änderung der Druckverluste mit Änderung der Durchflussrate im System sind kleiner oder gleich des entsprechenden aufgeprägten Gradienten	Die Durchflussmenge steigt plötzlich stark an und stabilisiert sich dann auf einem neuen Wert

Typ der Instabilität	Mechanismus	Charakteristik
Übergang ins Filmsieden	Schlechter Wärmeübergang und schlechte Wärmeabfuhr	Anstieg der Wandtemperatur und Ausbildung von Durchflussschwankungen
Instabilität beim Übergang zwischen Strömungsmustern	Blasenströmung besitzt weniger Dampf, aber höhere Druck-verluste als eine ringförmige Strömung	Wiederkehrende Strömungsmuster und Schwankungen der Durchflussrate
Geysir-Effekt	Zyklische Anpassung während eines Metastabilen Zustands, typischerweise aufgrund fehlender Verdampfungskeime (z. B. überhitzter Dampf)	Wiederkehrender Prozess von Überhitzung und plötzlicher Verdampfung mit möglichem Ausstoß und Wiederbefüllung
Akustische Schwingungen	Resonanzen von Dichtewellen, die in einem Abblasevorgang zur Druckentlastung in Bereichen mit unterkühltem Sieden, Blasen- oder Filmsieden angeregt werden können	Hohe Frequenzen im Bereich von 10 bis 100 Hz abhängig von der Durchlaufzeit der Druckwellen im System
Dichtewellen	Verzögerungs- und Rückwirkungseffekte zwischen Durchflussrate, Dichte und Druckverlusten	Niedrige Frequenz im Bereich von 1 Hz abhängig von der Durchlaufzeit einer dauerhaften Welle
Thermische Schwankungen	Wechselwirkung zwischen Wärmeübergangskoeffizient und Durchflussänderungen	Entsteht bei Filmsieden
Siedewasserreaktor (SWR)-Instabilität	Wechselwirkungen zwischen Voidrückkopplung (Kern kritisch), den Durchflussbedingungen und dem Wärmeübergang	Einflussreich für kleine Verzögerungszeiten im Wärmeübergang vom Brennstoff zum Kühlmittel, variiert mit dem Abbrand und den Betriebs-parametern (z. B. besonders wahrscheinlich im Anfahrbetrieb)
Instabilität paralleler Kanäle	Wechselwirkung zwischen wenigen parallelen Kanälen	Verschiedene Möglichkeiten der Änderung des Strömungsmusters
Druckverlust-schwankungen	Ausschläge in der Durchflussmenge erzeugen eine dynamische Wechselwirkung zwischen Strömungskanal und komprimierbaren Volumen	Sehr niedrige Frequenzen, 0,1 Hz, periodischer Vorgang

Dampf-Flüssigkeits-Wechselwirkung

Der Massen- und Energieübertrag einer Dampfströmung in ein Wasserbecken ist ein dreidimensionales Phänomen und hängt von dem exakten Strömungspfad des Dampfes ab. Zunächst kann der Typ der Kondensation anhand des Diagrammes Abb. 2.10 abgelesen werden (Typen für seitliche Einströmungen hängen zusätzlich wesentlich vom Rohrdurchmesser ab). Er reicht von Kondensation im direkten Kontakt zwischen Dampf

und Beckenwasser über Blasenbildung und Bildung von Blasenwolken bis zu Mitreißfontänen. Ist der Kondensationstyp bestimmt, so kann die Kontaktfläche zwischen Dampf und Wasser und der Wärmeübergangskoeffizient näher bestimmt werden.

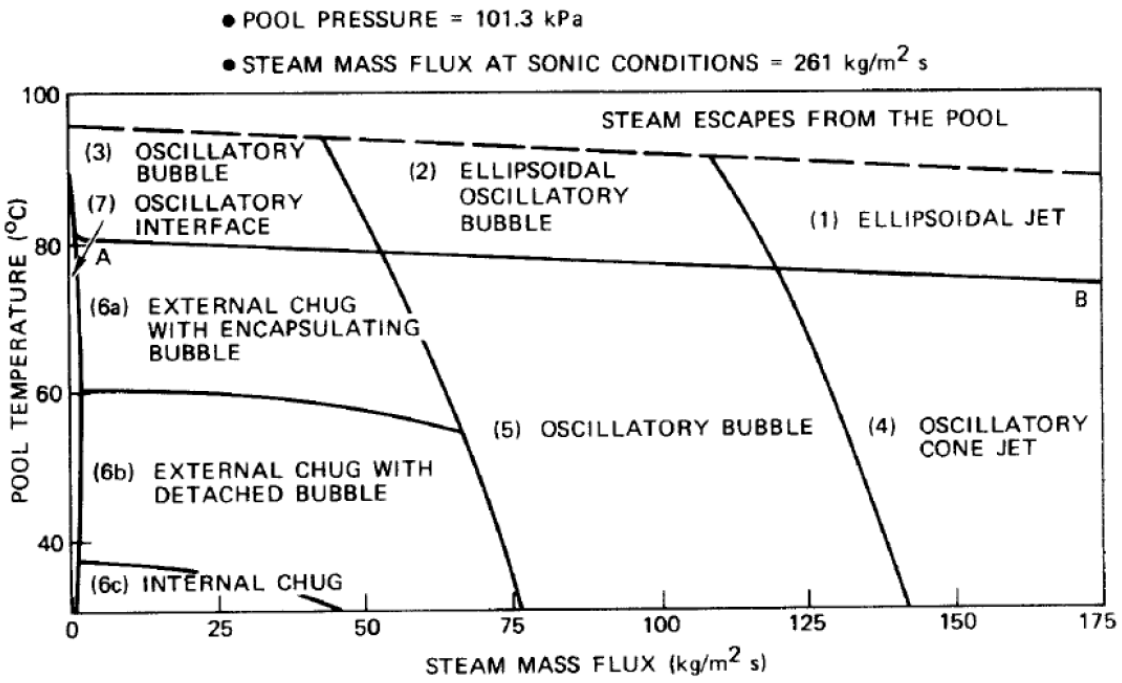


Abb. 2.10 Kondensation aus einer abwärts gerichteten Druckentlastungsleitung /IAE 21a/

Schwerkraftgetriebene Kühlung und Druckspeicherverhalten

Eine schwerkraftgetriebene Kühlung ist eine passive Komponente, die den Ausfluss aus höhergelegenen Wasserspeichern zur Kernkühlung verwendet. Im Fall von Leckagen im Kühlkreislauf sind große Kühlmittelmengen entsprechend vorzuhalten. Als Beispiel ist das gravitationsgetriebene Kühlsystem (GDCS) des vereinfachten SWR in Abb. 2.11 gezeigt. Zur Einspeisung der GDCS-Wasserbecken sind keine Pumpen erforderlich, allerdings eine Druckentlastung des Primärkühlsystems. Alternativ können auch druckbeaufschlagte Wasserspeicher zur Kernkühlung ohne Pumpen eingesetzt werden. Zur Einspeisung über Druckspeicher ist je nach Leckagegröße keine primärseitige Druckentlastung notwendig.

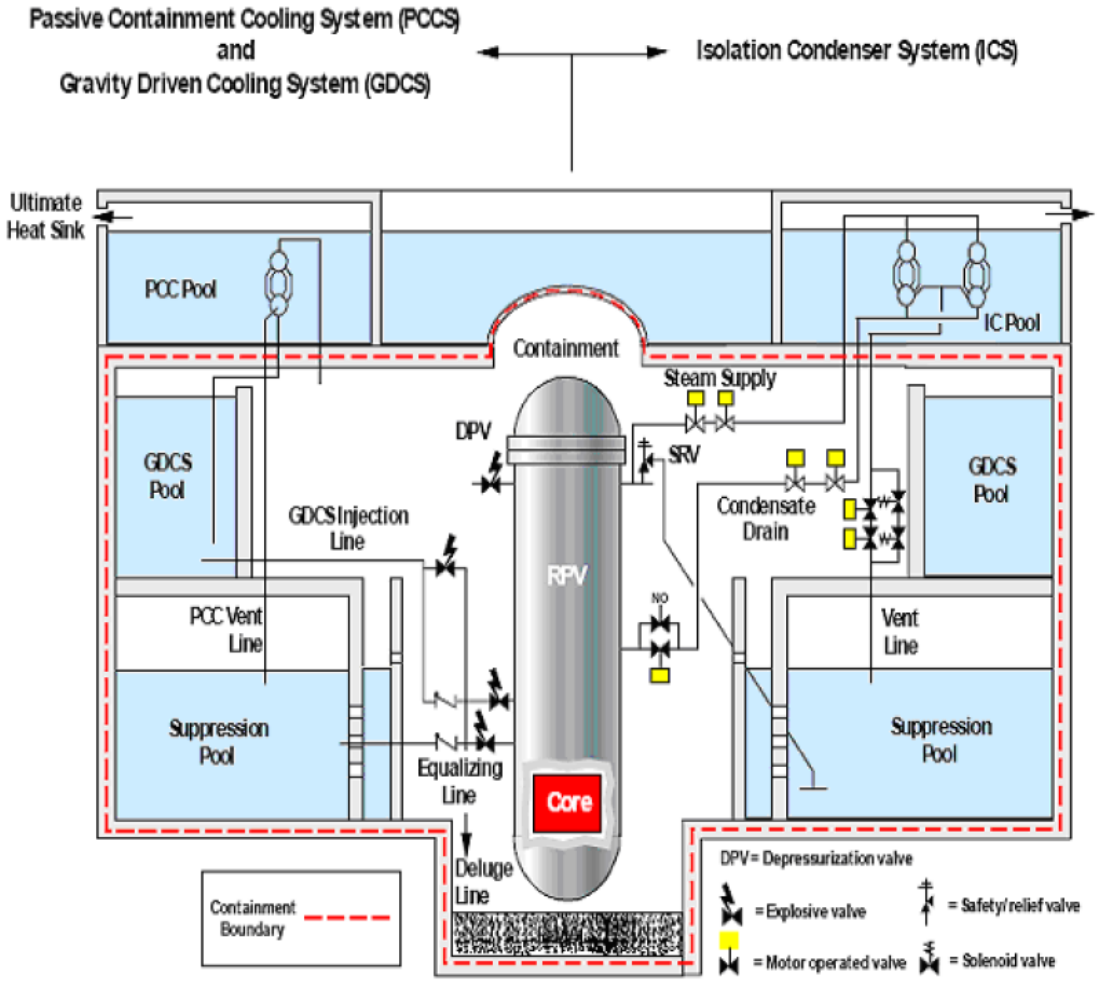


Abb. 2.11 Sicherheitssysteme des Vereinfachten SWR /IAE 12/

Temperaturschichtung von Flüssigkeiten

Die Einspeisung von Notkühlsystemen in horizontale Rohre, die teilweise mit Dampf gefüllt sind, kann zur Entstehung von kondensationsverursachten Wasserschlägen führen. Diese Schläge gefährden die Systemintegrität. Darüber hinaus kann sich eine Temperaturschichtung in großen Behältern mit großen Temperaturgradienten ausbilden.

Verhalten der Notwärmetauscher und Isolationskondensatoren

In einigen modernen Leichtwasserreaktoren wird die Nachzerfallswärme über einen passiven Kühlkreislauf abgeführt, so beispielsweise im SWR-1000, siehe Abb. 2.5. Typischerweise werden diese Notkühlkreisläufe als Naturumläufe ausgelegt und über Auftriebskräfte angetrieben. Die Wärmesenke wird entsprechend erhöht im Vergleich zur Position des Kerns angebracht.

Schichtung und Durchmischung der Borsäure

Die Hauptprobleme mit der Borsäuredurchmischung im Primärkühlkreislauf sind

- die Bildung von Bereichen mit niedrigerer Borsäurekonzentration,
- die plötzliche Ablösung solcher Bereiche sowie
- die Vermischung und der Transport von verdünnten Borsäurebereichen.

Bereiche mit niedriger Borsäurekonzentration können sich u. a. durch externe Verdünnung während niedriger Durchflussraten im Primärkühlkreislauf bilden oder durch Rückfluss von der Sekundärseite nach einem Kühlmittelverlust (KMV) (im Reflux Condenser Mode).

Verhalten im Hochdruckeinspeisebehälter (Make-up Tank, Behälter unter Primärkühlsystemdruck)

Der Hochdruckeinspeisebehälter, z. B. beim AP1000, ist mit kaltem, borierten Wasser gefüllt, mit dem Primärkühlsystem verbunden und dient der Noteinspeisung bei einem Kühlmittelverlust. Die Einspeisung erfolgt über die Schwerkraft. Im Unterschied zu bereits beschriebenen schwerkraftgetriebenen Kühlsystemen strömt in diesem System das Kühlmittel aus dem kalten Strang zurück in den Hochdruckeinspeisebehälter. Der Druck im Primärkühlsystem muss nicht bis auf Sicherheitsbehälterdruck abgefallen sein, um das System in Betrieb zu nehmen. Es entwickelt sich ein Naturumlauf mit kontinuierlich fallendem Kühlmittelinventar (als Folge des KMV). Strömt nur noch Dampf in den Hochdruckeinspeisebehälter, so dient das restliche Inventar nur noch der Einspeisung.

In /IAE 12/ wird außerdem eine Methode zur Untersuchung der Ausfallsicherheit von passiven Systemen vorgestellt, die Zuverlässigkeitsmethode für passive Sicherheitsfunktionen (Englisch: reliability methods for passive safety functions, RMPS). Die Methode findet in folgenden Problemstellungen Anwendung:

- Bestimmung und Quantifizierung von Unsicherheiten sowie Ermittlung wichtiger Einflussparameter,
- Durchführung von Unsicherheitsanalysen über thermohydraulische Modelle und Untersuchung von Systemausfällen des passiven Systems,
- Berücksichtigung des Ausfalls des passiven Systems in Ereignisablaufanalysen.

Entsprechend dem Verfahren werden die folgenden Schritte durchgeführt:

1. Systemanalyse und Modellierung
2. Erkennung der relevanten Parameter
3. Bestimmung der Unsicherheitsbereiche aller relevanten Parameter
4. Sensitivitätsanalysen
5. Quantitative Zuverlässigkeitsanalyse mit den einflussreichsten Parametern

Das Ablaufschema ist in Abb. 2.2 dargestellt.

Die Methode wurde für einen CAREM-ähnlichen Reaktor angewendet und ergab eine konservative obere Grenze für die Ausfallwahrscheinlichkeit des passiven Systems zur Wärmeabfuhr von 3 E-06.

Die Durchführung der Unsicherheitsanalysen über thermohydraulische Modelle und Simulationscodes kann u. a. mit GRS-Werkzeugen, wie SUSA und ATHLET, erfolgen. Als Referenz kann die Arbeit von Buchholz et al. in /BUC 15/ bzw. /BUC 16/ herangezogen werden.

2.4 Arbeiten zur PSA für Anlagen mit mehreren Reaktorblöcken gleichen Typs

Die blockübergreifenden Risiken, die in einer Mehrblock- oder Standort-PSA berücksichtigt werden müssen, sind u. a. (siehe /NUS 20/ und /HAG 21/):

a. der Ausfall gemeinsam genutzter Anlagenteile (z. B. gemeinsam genutzte Leitungen) oder die begrenzte Verfügbarkeit gemeinsam genutzter Systeme für mehrere betroffene Reaktorblöcke (z. B. das Feuerlöschsystem, elektrische Versorgungseinrichtungen oder mobile Notfalleinrichtungen, wie mobile Einspeisepumpen und Notstromaggregate),
b. gemeinsam verursachte Ausfälle (GVA) von Systemen mit gleichartigem Aufbau, Funktionsweise, Umgebungsbedingungen oder identischen Komponenten, die in den unterschiedlichen Reaktorblöcken genutzt werden,

c. gemeinsame auslösende Ereignisse (u. a. durch übergreifende Einwirkungen, wie Überflutung oder Brand) oder der Ausfall der externen Stromversorgung, oder GVA, wie beispielsweise Produktionsfehler,

d. eine verringerte Personalverfügbarkeit (z. B. der Werkfeuerwehr oder des Personals in der Warte) für jeden betroffenen Reaktorblock und ein erhöhtes Risiko für Fehlhandlungen des Betriebspersonals aufgrund erhöhter Anforderungen und Zeitmangel sowie

e. systematische Fehler bei Wartungs- und Inspektionsarbeiten in mehreren Reaktorblöcken, die zu einem gemeinsamen Ausfall führen können (dieser Punkt kann auch in b mitberücksichtigt werden).

Für einen Kernkraftwerksstandort mit SMR(s) sind grundsätzlich alle genannten reaktorübergreifenden Risiken für eine Mehrblock- oder Standort-PSA relevant.

2.4.1 Aufbau einer Mehrblock-PSA

Der IAEA-Bericht „Multi-unit Probabilistic Safety Assessment“ /IAE 21/ beinhaltet Empfehlungen der IAEA zur PSA von Kernkraftwerkstandorten mit mehreren Reaktoren, auch als Mehrblockanlagen bezeichnet. Eine schematische Darstellung des methodischen Vorgehens für die Erstellung einer Mehrblock-PSA Englisch: Multi-Unit PSA, MUPSA) findet sich in der nachfolgenden Abb. 2.12.

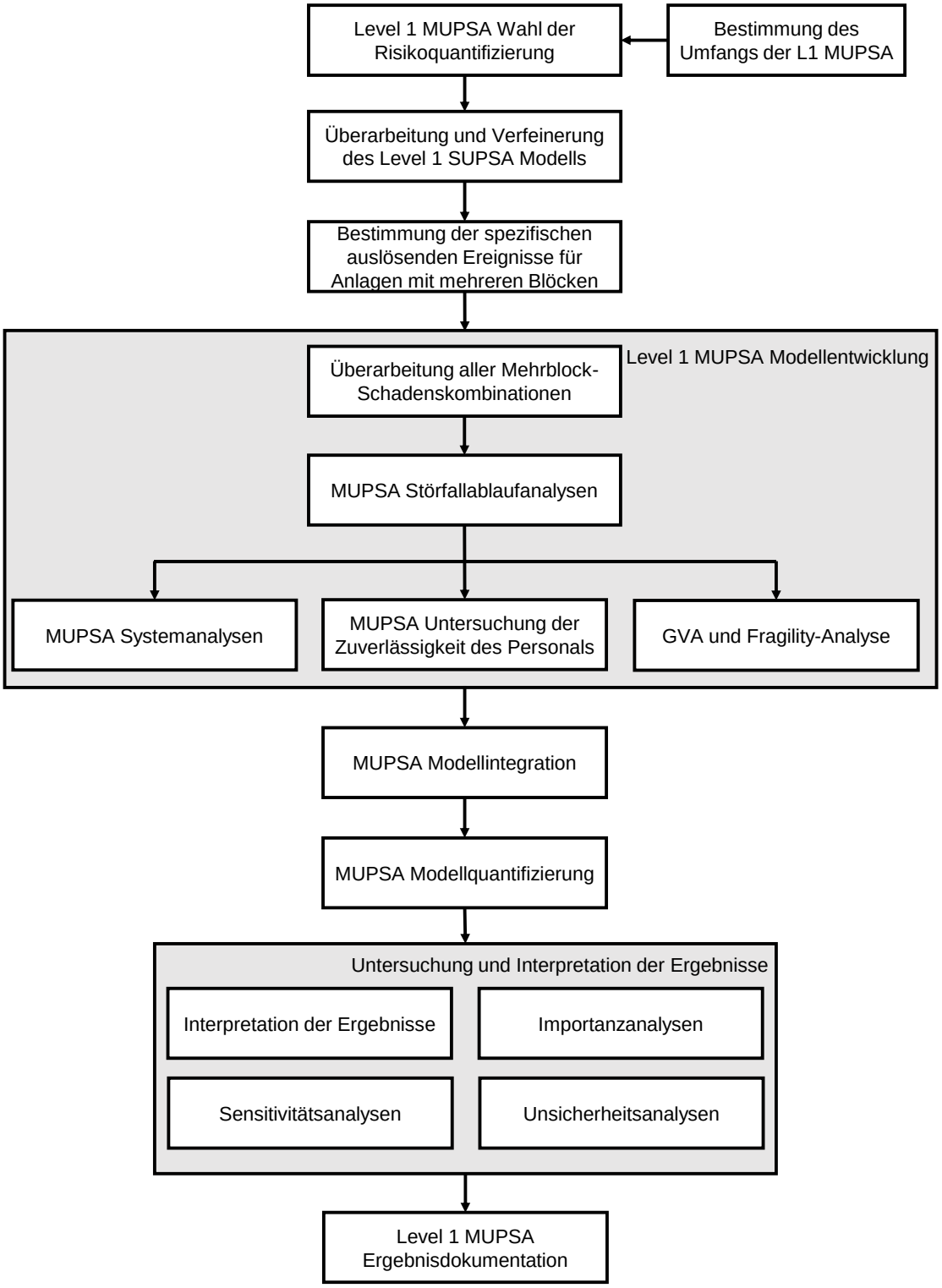


Abb. 2.12 Methodisches Vorgehen zur Erstellung einer Multi-Unit PSA der Stufe 1 entsprechend /IAE 21/

Im ersten Schritt wird der Umfang der MUPSA entsprechend dem Umfang der PSA für einen einzelnen Reaktorblock (Single-Unit PSA, SUPSA) festgelegt. Hierzu zählt die Auswahl der auslösenden Ereignisse aufgrund von anlageninternen Ereignissen und

übergreifenden Einwirkungen von innen, die in der MUPSA berücksichtigt werden sollen. Einwirkungen und auslösende Ereignisse, die nur wenig zum Gesamtrisiko beitragen, können hier bereits ausgeschlossen werden.

Für die Risikoquantifizierung kommen sowohl Einzelblock- als auch Mehrblock-Risikomaße zum Einsatz. Mehrblock-Risikoquantifizierungen können beispielsweise auch mögliche Schäden an gemeinsam genutzten Anlagenteilen, wie dem Brennelementlagerbecken, beinhalten. Außerdem sind andere Risikomaße, wie die Kernschadenshäufigkeit für einen beliebigen einzelnen Reaktor (single unit core damage frequency, SUCDF) und für mehrerer Reaktoren (multi-unit core damage frequency, MUCDF), von Interesse /IAE 19/[2].

Im nächsten Schritt werden alle SUPSA-Modelle in einem MUPSA-Modell zusammengeführt. Im Rahmen einer Überarbeitung werden zunächst die SUPSA-Modelle vereinfacht. Darin bleiben jedoch die risikorelevanten auslösenden Ereignisse aufgrund anlageninterner Ereignisse sowie aufgrund übergreifender Einwirkungen von innen und außen und Einwirkungskombinationen, die in mehreren Reaktorblöcken ein auslösendes Ereignis bewirken können, berücksichtigt. Folgende Kriterien können für eine qualitative Auswahl herangezogen werden:

- Führt das Ereignis direkt zu einer Reaktorschnellabschaltung (RESA) in mehreren oder allen Reaktorblöcken?
- Führt das Ereignis zu einer sofortigen RESA in einem Reaktorblock, und wird ein anderer Block in einen veränderten Zustand versetzt, der möglicherweise zu einer RESA führt?
- Führt das Ereignis zu veränderten Zuständen in mehreren Reaktorblöcken, die möglicherweise eine RESA zur Folge haben?

Lässt sich eine dieser Fragen mit ja beantworten, so sollte das Ereignis in einer MUPSA berücksichtigt werden. Auch ein quantitatives Kriterium für den Ausschluss von Unfallszenarien kann in der Durchsicht geprüft werden. Eine Einwirkung von innen oder außen oder ein internes auslösendes Ereignis wird beispielsweise vernachlässigt, wenn

[2] In diesem Positionspapier werden die verschiedenen Aspekte behandelt, in denen sich die sicherheitstechnische Bewertung von SMR von derjenigen von großen Leistungsreaktoren unterscheidet. Insbesondere wird auf die Unterschiede der Begriffe „multi-unit“, wie er bei der Bewertung großer Leistungsreaktoren verwendet wird, und „multi-module“ für SMR eingegangen.

sich unter Verwendung konservativer Annahmen für alle möglichen Freisetzungskategorien ein Beitrag zur Gesamteintrittshäufigkeit dieser Freisetzungskategorien von weniger als α (ein typischer Wert für α ist 0,1 % /IAE 21/) möglich ist. Hier müssen allerdings mögliche Einflussfaktoren auf den Unfallablauf, wie GVA oder der Ausfall gemeinsam genutzter Hilfssysteme, in das Modell der MUPSA eingebaut und in der Überarbeitung berücksichtigt werden. In der Überarbeitung kann alternativ auch das Auswahlkriterium α angepasst werden. Es ist auch zu prüfen, ob Ersatzteile und Personal bei auslösenden Ereignissen in mehreren Reaktoren in vollem Umfang für jeden einzelnen Reaktorblock zur Verfügung stehen, wie dies möglicherweise in der SUPSA angenommen wurde. Abhängigkeiten zwischen mehreren Reaktorblöcken können u. a. sein:

- gemeinsam von mehreren Reaktorblöcken genutzte bauliche Anlagenteile, Systeme und Komponenten (Englisch: structures, systems and components, SSC) und Infrastruktur, wie gemeinsam genutzte Gebäude und bauliche Anlagenteile, externe Stromversorgung, Pumpstationen, Kühlwassereinrichtungen, Notstromversorgung, Zufahrtsstraßen, Löschwasserversorgung etc.,
- gemeinsame Lagertanks für Wasser, Treibstoff etc.,
- Systeme zur Begrenzung von Unfallfolgen, die von mehreren Reaktoren benötigt werden könnten, z. B. mobile Dieselgeneratoren,
- übergreifende einzelne Einwirkungen oder Einwirkungskombinationen (von innen wie außen) oder auch GVA, z. B. das Versagen vergleichbarer SSC durch Einwirkungen von außen, wie Erdbeben oder Tsunami,
- räumliche Einschränkungen, wie beispielsweise eine gemeinsam von mehreren Reaktoren genutzte Warte,
- Abhängigkeiten im Betriebsablauf der Betriebsmannschaft (aufgrund eingeschränkter Personalverfügbarkeiten) oder der Unfallmanagementroutinen,
- der Einfluss eines betroffenen Reaktorblocks auf andere Einrichtungen, beispielsweise durch eine radioaktive Freisetzung oder eine Ausbreitung des Unfalls auf andere Reaktorblöcke.

Darüber hinaus können Vereinfachungen in der SUPSA eine Überarbeitung erfordern. Grundsätzlich besteht die Möglichkeit, dass Szenarien in der MUPSA in Kernschäden in mehreren Blöcken führen, die in einer SUPSA zu keinem Kernschaden führten.

Die modifizierten SUPSA-Modelle werden gemeinsam in das MUPSA-Model überführt. Dabei ist zu beachten, dass die Einträge auch namentlich unterscheidbar sind, z. B., dass die Ereignisse des Ausfalls der Hauptkühlmittelpumpe 1 im Reaktor 1 und der Hauptkühlmittelpumpe 1 im Reaktor 2 nicht beide mit HKP1“ benannt sind, sondern möglicherweise mit HKP1R1 und HKP1R2.

Der nächste Schritt in der Erstellung des MUPSA-Modells besteht in einer Prüfung und Überarbeitung der auslösenden Ereignisse. Hier liegt ein besonderer Fokus in der Auswertung der Betriebserfahrung hinsichtlich möglicher Lücken in den SUPSA-Modellen mit Blick auf die Gefährdung anderer Reaktorblöcke. Es zeigt sich, dass die Betrachtungen der IAEA keine GVA der Hilfssysteme durch eine übergreifende Einwirkung berücksichtigen, was beispielsweise in der PSA von NuScale für eine SMR-Anlage explizit berücksichtigt wird, wie in Tab. 2.7[3] dargestellt. Des Weiteren wird jedes auslösende Ereignis hinsichtlich eines möglichen Einflusses auf andere Blöcke geprüft. Hier gelten erneut die oben genannten drei qualitativen Ausschlusskriterien. Am Ende dieses Analyseschritts werden die auslösenden Ereignisse neu gruppiert und die Eintrittshäufigkeiten aller MUPSA-relevanten auslösenden Ereignisse bestimmt.

[3] Die Angaben zu verwendeten Wahrscheinlichkeiten in Tab. 2.7 entsprechend der NuScale-PSA sollen eine Orientierungshilfe darstellen. Es muss beachtet werden, dass diese Werte Experteneinschätzungen darstellen, die auf konservativen Annahmen beruhen.

Tab. 2.7 Betrachtungen zu verschiedenen auslösenden Ereignissen im Hinblick auf eine Mehrblock-PSA

Gruppierung auslösender Ereignisse (SUPSA)	Bewertung nach IAEA MUPSA /IAE 21/	Multi-Modul-PSA für SMR nach /NUS 20/, Faktoren, ob Einzelmodul oder mehrere Module betroffen sind	Neugruppierung der auslösenden Ereignisse (MUPSA) in auslösende Ereignisse für einen oder mehrere Reaktoren etc.
KMV innerhalb des Sicherheits-behälters	Ein KMV in einem Reaktorblock kann nicht zu einer RESA oder veränderten Bedingungen in einem anderen Block führen.	90 % im Fall von Fehlöffnungen von Ventilen oder ande-ren Fehlfunktionen, 99 % im Fall von Leitungsbrüchen	KMV innerhalb des Sicherheitsbehälters ausschließlich eines Moduls/Blocks
		1 % bis 10 %	Gemeinsam verursachter KMV innerhalb des Sicherheitsbehälters
KMV in angeschlossene Systeme	Nur die Auswirkungen einer möglichen resultierenden anlageninternen Überflutung werden berücksichtigt.	99 %	KMV in angeschlossene Systeme ausschließlich eines Moduls/Blocks
		1 %	Gemeinsam verursachter KMV in angeschlossene Systeme
Transienten	Sekundäre Effekte, z. B. über veränderte Temperatur-, Druck- oder Dampf-bedingungen in Systemen, die sich in unmittelbarer Nähe zu Systemen eines anderen Blocks befinden (z. B. in einem gemeinsamen Maschinenhaus)	90 %	Transiente nur eines Moduls/Blocks
		10 %	Transiente in mehreren Modulen/Blöcken
Ausfall der externen Stromversorgung	Dies ist in der MUPSA nicht zu berücksichtigen	0%	Modul-/blockspezifisch
	Dies hängt davon ab, ob mehrere Blöcke das gleiche Umspannwerk verwenden.	100 %	Fehler im Umspannwerk
	In der MUPSA ist zu berücksichtigen, dass alle Reaktorblöcke betroffen sein können.		Netz- und wetterbezogen

Gruppierung auslösender Ereignisse (SUPSA)	Bewertung nach IAEA MUPSA /IAE 21/	Multi-Modul-PSA für SMR nach /NUS 20/, Faktoren, ob Einzelmodul oder mehrere Module betroffen sind	Neugruppierung der auslösenden Ereignisse (MUPSA) in auslösende Ereignisse für einen oder mehrere Reaktoren etc.
Ausfall von Hilfssystemen	Das Vorgehen hängt davon ab, ob die Hilfssysteme gemeinsam von mehreren Blöcken verwendet werden.	70 % für Verlust der Gleichspannungs-stromversorgung	Ausfall eines Hilfssystems ausschließlich eines Moduls/Blocks
		30 %	GVA der Hilfssysteme
Interner Brand	Die Möglichkeit für ein Übertreten des Brandes auf andere Reaktorblöcke sollte geprüft werden.	Ein Übergreifen des internen Brandes oder einer internen Überflutung auf andere Module wird nicht quantitativ analysiert, obwohl eine RESA in mehreren Modulen möglich ist und ein Ausfall gemeinsam genutzter Systeme droht, u. a. des Volumenregel-systems und des Systems zur Flutung des Sicherheits-behälters.	Interner Brand mit ausschließlich einem betroffenen Modul/Block
			Modul-/blockübergreifender interner Brand
Interne Überflutung	Die Möglichkeit einer Ausweitung der Überflutung zu angrenzenden Reaktorblöcken ist zu prüfen.		Interne Überflutung mit ausschließlich einem betroffenen Modul/Block
			Modul-/blockü-ber-greifende interne Überflutung
	Im Fall eines KMV in angeschlossene Systeme ist die Möglichkeit einer internen Überflutung eines anderen Blocks zu prüfen.		Interne Überflutung nach KMV an einem ange-schlossenen System
Erdbeben	Alle Blöcke sind gleich aufgebaut mit gleichen erdbeben-bedingten Ausfällen.	Für starke Erdbeben wird eine Beschä-digung aller Module angenommen, bei schwächeren Erdbeben nicht.	Erdbebenschäden an allen Modulen/Blöcken gleichermaßen
	Der Ausfall gemein-sam verwendeter Systeme führt direkt in ein auslösendes Ereignis in der MUPSA.	Das Versagen des Krans, der eine Schwachstelle dar-stellt und mehrere Module beschädigen könnte, wird ausge-schlossen.	Erdbebenschäden an gemeinsam verwendeten Systemen

Ein weiterer Schritt bei der Erstellung einer MUPSA (siehe Abb. 2.12) ist die Überarbeitung aller Mehrblock-Schadenskombinationen. Entsprechend dem quantitativen Kriterium können Endzustandskombinationen (z. B. Kernschaden in einem Reaktor und Freisetzung aus dem Brennelementlagerbecken) mit geringer Relevanz aus dem MUPSA-Modell entfernt werden.

Der nächste Schritt in der Erstellung der MUPSA ist die Durchführung der Ereignisablaufanalysen. Ereignisablaufanalysen mit Berücksichtigung aller möglicher Abläufe werden bei Anlagenstandorten mit mehr als zwei Reaktorblöcken[4] schnell unübersichtlich und aufwändig. Nur in sehr spezifischen Fällen, wenn baugleiche Blöcke gleichermaßen betroffen sind, kann vereinfacht angenommen werden, dass der Ereignisablauf für alle Blöcke identisch ist. Sind keine wesentlichen Vereinfachungen der Ereignisablaufanalysen möglich, so ist häufig eine Vereinfachung der Darstellung der Analysen erforderlich, um eine übersichtliche Darstellung über die möglichen Ereignisabläufe zu erhalten. Folgende Darstellungsmöglichkeiten für Ereignisablaufanalysen sind verbreitet:

- Gesamtereignisablauf-Ansatz (Master Event Tree Approach): Jedes auslösende Ereignis wird separat in einem Ereignisbaum modelliert und ausgewertet. In diesem Ereignisbaum werden alle Reaktorblöcke berücksichtigt. Grundsätzlich werden die Ereignisabläufe aus den PSA für die einzelnen Reaktorblöcke zu Gesamtereignisablaufdiagrammen (separat für jedes auslösende Ereignis bzw. jede übergreifende Einwirkung) zusammengeführt, ein Beispiel ist in Abb. 2.13 gezeigt.

- Einzelfehlerbaum-Ansatz (Single Fault Tree Approach): Alle Blöcke und Gefahren werden gemeinsam in einem Fehlerbaum bzgl. einer Bestimmungsgröße (z. B. die Mehrblock-Kernschadenshäufigkeit) beschrieben. Die Modelle der einzelnen Reaktorblöcke können in diesem Ansatz bzgl. der Risikomaße gemeinsam ausgewertet werden. Die Fehlerbäume eignen sich gut zur Unterteilung in kleinere Einheiten und die beispielhafte Darstellung und Erklärung der Funktionsweise einer kleineren Fehlerbaumeinheit reicht mitunter aus, um auch die Funktionsweise von analogen oder ähnlichen Fehlerbäumen verständlich zu machen. Ein Beispiel ist Abb. 2.14 zu entnehmen.

- Gemischter Ansatz (Hybrid Approach): Der gemischte Ansatz verwendet sowohl den Gesamtereignisablauf- als auch den Einzelfehlerbaum-Ansatz. Die Kernschadenshäufigkeiten für jeden einzelnen Reaktorblock werden dabei in einzelnen Fehlerbäumen abgebildet und stellen die Basis für die Ereignisse der Gesamtereignis-Ablaufanalyse dar. Insbesondere für baugleiche Blöcke ergeben sich die erforderlichen

[4] Insbesondere für Kraftwerksstandorte mit unterschiedlichen Reaktorblöcken oder nach auslösenden Ereignissen, welche die einzelnen Blöcke unterschiedlich beeinträchtigen und mit hoher Wahrscheinlichkeit zu unterschiedlichen Abläufen führen wie z. B. der Unfall in Fukushima Dai-ichi, der zu unterschiedlichen Abläufen in den Reaktorblöcken 1 bis 3 führte)

Einzelfehlerbäume für die unterschiedlichen Reaktorblöcke analog. Darüber hinaus kann die Komplexität der Gesamtereignisablaufdiagramme niedrig gehalten werden.

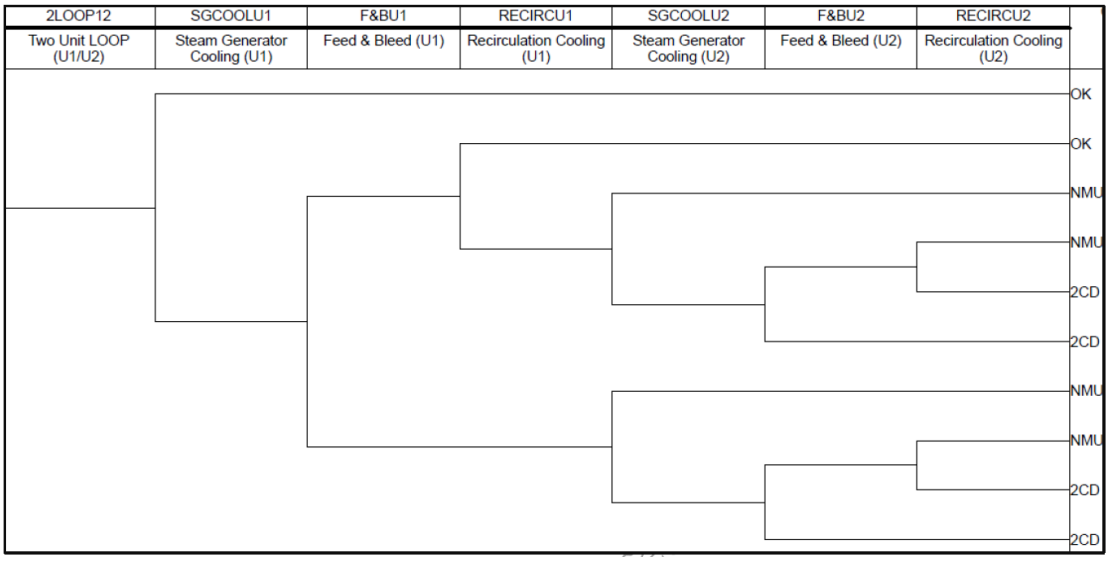


Abb. 2.13 Beispiel für einen Gesamtereignisablauf-Ansatz /IAE 21/

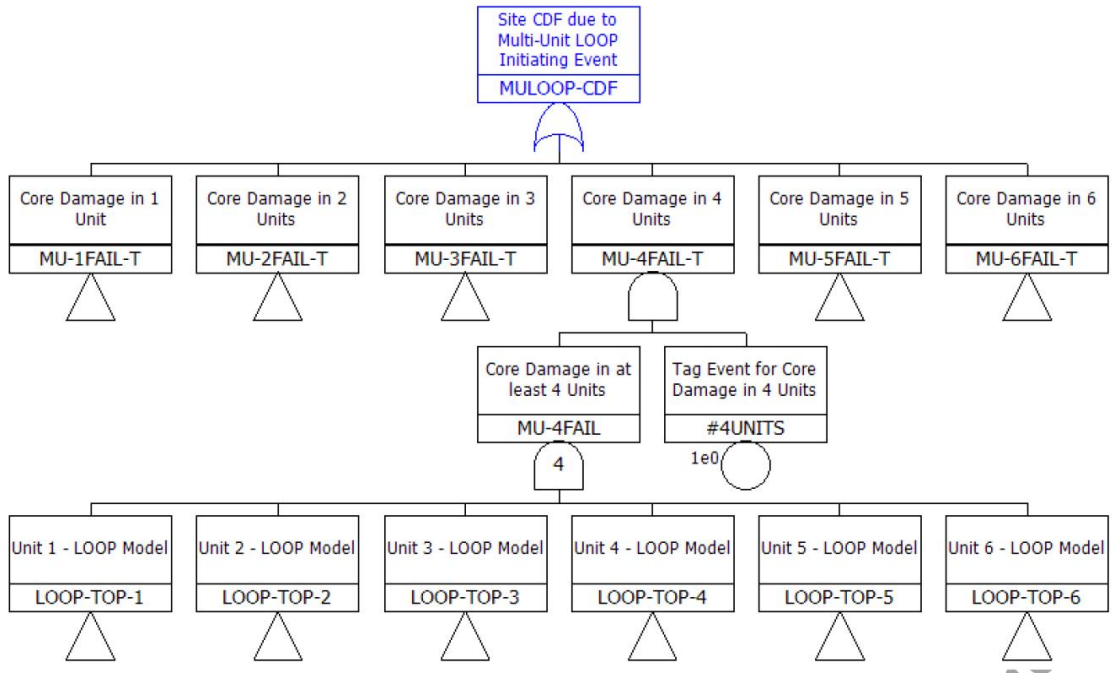


Abb. 2.14 Beispiel für einen Einzelfehlerbaum-Ansatz /IAE 21/

Im folgenden Schritt werden drei MUPSA Modelluntersuchungen, die Systemanalyse, die Personalzuverlässigkeitsanalyse und die Untersuchungen zu GVA und zu erbeben-bedingten Ausfällen (Fragility), aufgezeigt. Die Modelluntersuchungen beziehen sich im

Wesentlichen auf die reaktorübergreifenden Risiken (vgl. Punkte a bis e zu Beginn des Abschnitts 2.4).

Gemeinsam genutzte Systeme

In der Systemanalyse werden gemeinsam von mehreren Reaktorblöcken genutzte Systeme untersucht und modelliert. Wichtig für die Modellierung ist unter anderem, ob und unter welchen Umständen das System dauerhaft für ein einzelnes Modul benötigt wird, ob die einzelnen Blöcke bei Systemanforderungen mit kurzen Einsatzzeiten das System im Wechsel zwischen den Blöcken betreiben können oder ob das System von mehreren Blöcken gleichzeitig angefordert wird. Wird ein System beispielsweise von mehreren Reaktorblöcken angefordert, können verschiedene Modellierungen notwendig sein:

- eine dynamische Modellierung der Fehlerbäume, welche die Umschaltung des Systems im Unfallablauf erlaubt,
- eine Priorisierung bzgl. des Reaktorblocks, des Reaktorblockzustands oder des Anforderungsfalls, für welchen das System bevorzugt eingesetzt wird,
- Anpassung von Systemverfügbarkeitswahrscheinlichkeiten für die einzelnen Reaktorblöcke in Abhängigkeit von der Anzahl der Anforderungsfälle und der notwendigen Nutzungsdauer.

Personalzuverlässigkeit

In der Untersuchung zur Zuverlässigkeit des Personals werden bestimmte Aspekte, wie der Einfluss mehrerer betroffener Reaktorblöcke oder der Einfluss gemeinsam genutzter Räumlichkeiten, wie eine gemeinsam genutzte Warte, auf die Entscheidungen und Handlungen des Personals näher betrachtet. Wichtige Aspekte dabei sind u. a.

- das Personal, welches für mehrere Blöcke zuständig ist,
- gemeinsam genutzte Warten,
- erhöhter Stress durch die Unfallbedingungen in mehreren Reaktorblöcken,
- Personalkapazität und -verfügbarkeit, da mehrere Reaktorblöcke betroffen sein können,

- Einschränkungen und zusätzliche Gefahren für das Personal durch die Unfallbedingungen in einem anderen Reaktorblock (z. B. Freisetzung von Radioaktivität oder Möglichkeit von Wasserstoffexplosionen).

Generell sind die üblichen Methoden zur Untersuchung und Quantifizierung der Personalzuverlässigkeit auch in einer Mehrblock-PSA anwendbar. Ein erheblicher Einfluss der Personalzuverlässigkeit auf den Unfallverlauf ist für den Fall, dass Personal für mehrere Blöcke zuständig ist und blockübergreifende GVA wenig zum Ereignisablauf beitragen (das bedeutet, in jedem Block ist ein unterschiedlicher Ereignisablauf anzunehmen), zu erwarten. Im Fall übergreifender Einwirkungen bzw. Einwirkungskombinationen auf baugleiche Reaktorblöcke ergeben sich folgende vereinfachende Annahmen für das Personal:

- gleiche Abläufe der erforderlichen Maßnahmen für alle betroffenen Reaktorblöcke bei gleichen Betriebszuständen,
- keine frühzeitige Freisetzung aus einem Reaktorblock, der länger andauernde Arbeiten (z. B. Reparaturen) an anderen Blöcken erschwert,
- Konzentration auf einen Störfall, keine Verwechslungsgefahren bei der Durchführung der Maßnahmen.

Reaktorblockübergreifende GVA

Die Berücksichtigung der blockübergreifenden GVA in einer Mehrblock-PSA kann konservativ vereinfacht oder detailliert erfolgen. Für GVA, die in den Kernschadenshäufigkeiten dominieren, wird eine Überarbeitung vom vereinfachten auf das detaillierte Modell empfohlen. Dazu sind folgende Schritte durchzuführen:

1. Vereinfachte Modellierung: Ein GVA-Basisereignis wird den Fehlerbäumen des MUPSA-Modells an den entsprechenden Stellen hinzugefügt.

2. Das Basisereignis der vereinfachten Modellierung wird durch ein detailliertes Modell der GVA (dieses Modell berücksichtigt alle Ausfallkombinationen, wie „3 von 4“ oder „5 von 7“, mit entsprechend unterschiedlichen Wahrscheinlichkeiten) ersetzt.

3. Sind die GVA in der detaillierten Modellierung noch immer besonders einflussreich, so können die Modellparameter durch spezifischere Analysen der betroffenen baulichen Anlagenteile, Systeme und Komponenten feiner abgestimmt werden.

Für eine Mehrblock-PSA sind folgende spezifische Faktoren für GVA relevant:

- Für unterschiedliche Reaktortypen und unterschiedliche Komponenten werden in der Regel keine reaktorblockübergreifenden GVA modelliert.
- GVA für unterschiedliche Modellvarianten eines Bauteils z. B. Ventile mit unterschiedlichen Durchmessern (auch vom gleichen Hersteller) werden üblicherweise nicht berücksichtigt.
- Bauteile des gleichen Typs aus unterschiedlichen Herstellungsjahren oder nach einer Designüberarbeitung sind weniger anfällig für GVA.
- GVA passiver Komponenten werden anders berücksichtigt als solche aktiver Komponenten. GVA passiver Systeme können auch umweltbedingte Einflüsse beinhalten, z. B. durch Korrosion und Verschleiß. Hier können die Bedingungen in den Reaktoren unterschiedlich sein, z. B. durch unterschiedliche Fahrweisen. GVA in einem Reaktor sind deshalb nicht direkt auf GVA in mehreren Reaktoren übertragbar.
- Sind mehrere Reaktoren den gleichen materialbeanspruchenden Bedingungen ausgesetzt (z. B. extremer Kälte, kann die Möglichkeit eines GVA auch für sich unterscheidende Komponenten der einzelnen Reaktoren berücksichtigt werden.

Einwirkungsbedingte Ausfallanalyse (Fragility Analysis)

In der einwirkungsbedingten Ausfallanalyse werden die Einflüsse einiger Einwirkungen von außen (wie Erdbeben oder Überflutung) untersucht. Eine vollständige Korrelation mit einer Wahrscheinlichkeit nahe 1 ergibt sich nur für die vorgenannten Einwirkungen und nur für Reaktorblöcke im gleichen Gebäude, auf gleicher Höhe, gleicher Bauart, gleicher Ausrichtung und im gleichen Betriebszustand. Die Berücksichtigung der Korrelationen bzgl. entsprechender Einwirkungen von außen im Modell für eine Mehrblock-PSA erfolgt analog zu den Betrachtungen der GVA.

Die nächsten Schritte in der Durchführung einer Mehrblock-PSA entsprechend Abb. 2.12 erfolgen in der gleichen Weise wie für eine PSA der Stufe 1 für einen einzelnen Reak-

torblock: An dieser Stelle wird auf die entsprechende Fachliteratur /BMU 05/, /IAE 21/ und /IAE 24/ verwiesen.

Ergebnisgrößen einer Mehrblock-PSA

Als Ergebnis einer PSA der Stufe 1 für eine Mehrblockanlage ergeben sich zusätzliche Risikomaße, u. a. die relative Bedeutung der Mehrblock-Kernschadenshäufigkeit, die nach /IAE 19/ wie folgt bestimmt werden können:

- Kernschadenshäufigkeit eines bestimmten Reaktorblocks am Anlagenstandort (CDF_1): Szenarien, die zu Kernschäden in mehreren Reaktorblöcken am Standort führen, werden dabei nicht berücksichtigt[5],
- Kernschadenshäufigkeit genau eines beliebigen Blocks am Standort mit *N* Blöcken ($SUCDF_1$):
  $SUCDF_1 = N \cdot CDF_1$
- Kernschadenshäufigkeit aus Störfällen mit Kernschadensendzuständen in x Reaktorblöcken (CDF_x),
- Gesamthäufigkeit von Kernschäden in einem oder mehreren Reaktorblöcken (*CDF*):
  $CDF = \sum_{x=0}^{N-1} \binom{N-1}{x} CDF_{1+x}$,
- Gesamtkernschadenshäufigkeit für Kernschäden in mehreren Reaktorblöcken:
  $MUCDF = \sum_{x=1}^{N-1} \binom{N-1}{x} CDF_{1+x}$,
- Standort- bzw. Anlagenkernschadenshäufigkeit (*SCDF*):
  $SCDF = SUCDF + MUCDF$,
- Relative Bedeutung der Mehrblock-Kernschadenshäufigkeiten im Vergleich zur Kernschadenshäufigkeit eines Reaktorblocks (*CPMA*):
  $CPMA = (CDF - CDF_1)/CDF$.

[5] Es ist zu beachten, dass die PSA für einen (hypothetischen) einzelnen Reaktorblock am Standort in diesem Zusammenhang nicht ausreicht, da Wechselwirkungen mit anderen Reaktorblöcken bestehen und im Störfallverlauf berücksichtigt werden müssen. Darüber hinaus können in der Regel die Ergebnisse von Standorten mit einer anderen Anzahl von Reaktorblöcken, aber ansonsten gleichen Verhältnissen nicht direkt verwendet werden.

2.4.2 Konservative Abschätzungen des Gesamtrisikos (Scoping Approach)

GE-Hitachi hat u. a. einen qualitativen Ansatz für eine konservative Abschätzung des Gesamtrisikos eines Kernkraftwerksstandort (für den Standort Wylfa Newydd, Großbritannien) entwickelt. Dieser ist zusammenfassend in /IAE 21/, Annex VI beschrieben. Die Abschätzung enthält u. a. folgende Einschränkungen:

- Die Abschätzung berücksichtigt kein Risiko für Reaktorblöcke in unterschiedlichen Betriebszuständen oder für weitere Radionuklidquellen, wie dem Brennelementlagerbecken.
- Die Abschätzung berücksichtigt keine besonderen baulichen Aspekte, wie beispielsweise Reaktoren, die sich einen Sicherheitsbehälter teilen.

Auf Basis der Ergebnisse in /HEN 19/ gelten folgende konservative Annahmen:

- Anlageninterne auslösende Ereignisse und Einwirkungen von innen in mehreren Reaktorblöcken machen 10 % des gesamten Einzelblock-Risikos aus, wenn sich mehrere Reaktorblöcke nur nicht-risikorelevante Systeme teilen. Sofern wichtige Systeme von mehreren Reaktorblöcken genutzt werden, ist das Mehrblock-Risiko ebenso hoch wie das Risiko für einen einzelnen Reaktorblock.
- Das Risiko durch Einwirkungen von außen, wie Erdbeben, wird für Mehrblockanlagen gleich betrachtet wie das Einzelblock-Risiko. Die Reaktorblöcke werden in diesem Fall als maximal korreliert angesehen.

Für Reaktorblöcke mit einem geringen Anteil an gemeinsam genutzten Systemen[6] (z. B. Dieselgeneratoren) gilt darüber hinaus für die Mehrblock-Kernschadenshäufigkeit und die Standort-Kernschadenshäufigkeit:

$$\begin{matrix} MUCDF \leq CDF_{\mathrm{MUEAE}} + 0{,}1 \cdot CDF_{\mathrm{MUIAE}} \\ SCDF \leq CDF_{\mathrm{MUEAE}} + n \cdot CDF_{\mathrm{MUIAE}} + n \cdot CDF_{\mathrm{SUAE}} \end{matrix} \text{ mit:} \qquad \textbf{(}2.1)$$

n: Anzahl der Reaktorblöcke,

MUEAE: auslösende Ereignisse infolge übergreifender Einwirkungen von außen für Mehrblockanlagen und

[6] Hier werden nur von gemeinsam genutzten Systemen betrachtet und keine gemeinsam genutzten Strukturen oder Gebäude.

MUIAE: auslösende Ereignisse infolge übergreifender Einwirkungen von innen für Mehrblockanlagen.

Für Reaktoren mit einer wesentlichen gemeinsamen Nutzung von Systemen und Komponenten ergeben sich die folgenden Beziehungen:

$$MUCDF \leq CDF_{\text{MUEAE}} + 1{,}0 \cdot CDF_{\text{MUIAE}} + 0{,}1 \cdot CDF_{\text{SUAE-MUI}} \quad \text{mit:} \qquad (2.2)$$
$$SCDF \leq CDF_{\text{MUEAE}} + n \cdot CDF_{\text{MUIAE}} + n \cdot CDF_{\text{SUAE}}$$

SUAE-MRI: auslösendes Ereignis in einem Reaktorblock mit einer möglichen Auswirkung auf alle Reaktorblöcke.

Zeigt sich in einer konservativen Abschätzung nach /HEN 19/, dass das Standortsicherheitsziel (z. B. die Kernschadenshäufigkeiten unterhalb eines geforderten Grenzwerts) erreicht wird, ist eine detaillierte Mehrblock-PSA nicht erforderlich /IAE 21/.

Multi-Modul -Risikoanalyse von NuScale

NuScale betrachtet in den PSA-Unterlagen /NUS 20/ das Risiko mehrerer betroffener Reaktormodule anhand der PSA für nur ein Modul. Die Methode geht zunächst von einem betroffenen Modul aus. Anhand der Störfallcharakteristik ergibt sich daraus das Risiko für die anderen Module. Das in /NUS 20/ dargestellte Vorgehen findet sich in der nachfolgenden Abb. 2.15.

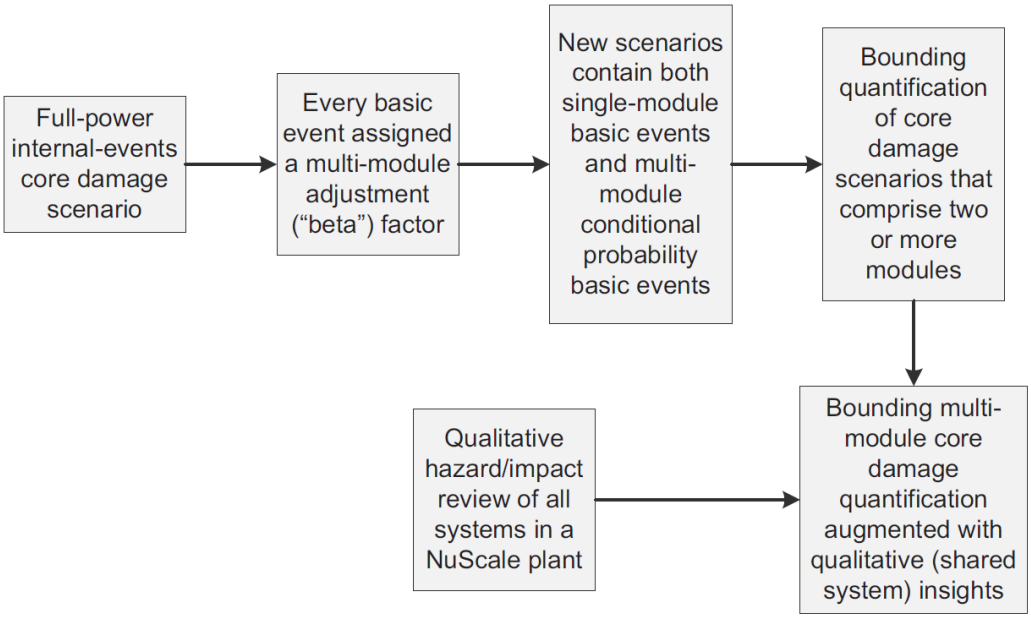


Abb. 2.15 Konzept von NuScale zur Abschätzung des Risikos mehrerer Reaktormodule eines SMR /NUS 20/

Das Risiko für alle Reaktormodule wird dabei über Multi-Modul-Anpassungsfaktoren quantifiziert. Die Anpassungsfaktoren basieren auf Experteneinschätzungen und liegen bei Werten zwischen 0,01 (sehr geringe Wahrscheinlichkeit für Ausfälle in mehreren Modulen) bis 1,0 (hohe Wahrscheinlichkeit für Ausfälle in mehreren Modulen). Neben den Unfallszenarien werden auch die Basisereignisse, u. a. Ausfallwahrscheinlichkeiten von Komponenten, GVA, die Zuverlässigkeit passiver Systeme, Wartungs- und Testarbeiten sowie Handlungen der Betriebsmannschaft mit Multi-Modul-Anpassungsfaktoren bewertet. Die Werte reichen von 0,1 bis 10. Damit werden alle oben aufgeführten reaktorblock- bzw. -modulübergreifenden Risiken in der PSA berücksichtigt.

2.4.3 Modellierung in einer Mehrblock-PSA

Grundlegende Überlegungen und Ansätze zur Modellierung einer Mehrblock-PSA sind in /LIM 18/ zu finden. Die verschiedenen Aspekte der Durchführung einer solchen PSA sind in Tab. 2.8 vergleichend zu einer PSA für einen einzelnen Reaktorblock beschrieben. In Tab. 2.9 findet sich eine Spezifikation aller auslösenden Ereignisse, die als Ereignisse in einer Mehrblock-PSA berücksichtigt werden könnten.

Tab. 2.8 Vergleich der Charakteristika von PSA für einen Einzelblock- und einen Mehrblockanlagenstandort

Charakteristik	SUPSA	MUPSA
Umfang der Analyse	Ein Leistungsreaktor	Zwei oder mehr Blöcke am Standort, welche gleichzeitig das gleiche auslösende Ereignis erfahren
Auslösendes Ereignis	Ein Ereignis, das zu einem Kernschaden oder einer Freisetzung von radioaktivem Material aus einer Anlage bzw. einem Kernreaktor führen kann	Ein Ereignis, dass zu einem Kernschaden oder einer Freisetzung von radioaktivem Material aus zwei oder mehr Anlagen/Kernreaktoren führen kann. Drei Hauptkategorien können unterschieden werden: 1. Zeitgleiches[7] Eintreten unabhängiger auslösender Ereignisse in mehr als einem Kernreaktor • Eintrittshäufigkeiten normalerweise gering 2. Übergreifendes Mehrblock-Ereignis (z. B. radioaktive Freisetzung in einen Nachbarreaktor) 3. Übergreifende Einwirkung (z. B. Erdbeben, Überflutung, Brand)
Modellierung der Systemausfälle	Ereignisablauf- und Fehlerbaumanalysen	Ereignisablauf- und Fehlerbaumanalysen
Zuverlässigkeitskenngrößen	• Zuverlässigkeit von SSC • Zuverlässigkeit menschlicher Handlungen • Eintrittshäufigkeiten der auslösenden Ereignisse	• Zuverlässigkeit von SSC • Zuverlässigkeit menschlicher Handlungen • Eintrittshäufigkeiten der auslösenden Ereignisse • Ausfallwahrscheinlichkeiten gemeinsam genutzter SSC (z. B. Notfalldieselgeneratoren) • Wahrscheinlichkeiten für blockübergreifende GVA • Blockübergreifende, korrelierte Empfindlichkeit von SSC • Leistung der Betriebsmannschaft im Fall eines Mehrblock-Störfalls mit Berücksichtigung organisatorischer Faktoren
Methode zur Quantifizierung	• Auswertung aller Minimalschnitte	• Fehlerbaumanalysen • Monte-Carlo Stichprobenanalysen (wenn Fehlerbäume aufgrund der Größe oder der Näherung seltener Ereignisse nicht handhabbar sind)

[7] innerhalb der Missionszeit, typischerweise 72 Stunden

Tab. 2.9 Mögliche auslösende Ereignisse, die in einer Mehrblock-PSA berücksichtigt werden könnten

Kategorie für auslösende Ereignisse bei Mehrblockanlagen	Mögliche auslösende Ereignisse, die zu berücksichtigen sind
Zeitgleiches[7] Eintreten unabhängiger auslösender Ereignisse in mehr als einem Reaktorblock	• Anlageninterne auslösende Ereignisse • Einwirkungen von innen (z. B. anlageninterne Überflutung oder Brand), falls keine Ausbreitung zu anderen Reaktorblöcken stattfindet
Übergreifendes Mehrblock-Ereignis	• Alle anlageninternen auslösenden Ereignisse
Gemeinsames auslösendes Ereignis	• Alle Einwirkungen von außen (z. B. Erdbeben, Tsunami, Tornado, Flugzugabsturz), die die mehr als einen Reaktorblock betreffen • Anlageninterne Ereignisse, die mehr als einen Reaktorblock betreffen

Zwei Faktoren machen das PSA-Modell für eine Mehrblockanlage vergleichsweise kompliziert und aufwändig. Ein Faktor betrifft die unterschiedlichen Reaktorbetriebszustände; typischerweise werden bis zu zehn Anlagenbetriebszustände (ABZ, Englisch: *p*lant *o*perational *s*tate, POS) eines Reaktors (wie Leistungsbetrieb oder die unterschiedlichen Zustände des Nichtleistungsbetriebs, wie Mitte-Loop mit oder ohne Reaktordeckel etc.) unterschieden. Die Reaktorblöcke an einem Standort können sich bei Eintritt des auslösenden Ereignisses in unterschiedlichen Anlagenbetriebszuständen befinden. Ein weiterer, ergebnisrelevanter Faktor ist durch die unterschiedlichen auslösenden Ereignisse, insbesondere die Modellierung aller Fälle für ein zeitgleiches Eintreten unabhängiger auslösender Ereignisse in unterschiedlichen Reaktorblöcken, gegeben.

Über die Vernachlässigung extrem unwahrscheinlicher Konstellationen für beide Faktoren kann versucht werden, das Mehrblock-PSA-Modell zu vereinfachen. Zum Beispiel können einige sehr unwahrscheinliche auslösende Ereignisse als exklusive Ereignisse modelliert werden, da diese nicht zeitgleich für unterschiedliche Reaktorblöcke zu unterstellen sind. Ein entsprechendes Beispiel könnte ein KMV durch ein großes Leck sein, welches nur für einen Reaktorblock unterstellt wird, sofern keine weiteren Reaktorblöcke im Ereignisablauf unzulässig beeinträchtigt werden können.

Ein großes Problem bei der Modellierung eines übergreifenden Mehrblock-Ereignisses ist die Kopplung zwischen der Stufe 1 und der Stufe 2 der PSA. Die freigesetzten Spaltprodukte aus den Ergebnissen der PSA der Stufe 2 für einen Reaktorblock können einen

Einfluss auf die PSA der Stufe 1 für einen anderen Reaktorblock in der Mehrblock-PSA haben. Ein Beispiel für die Berücksichtigung zusätzlicher Unverfügbarkeit von Eingriffen der Betriebsmannschaft durch die radioaktive Freisetzung aus einem anderen Reaktorblock ist in /IAE 21/, Appendix II gegeben.

Beispiele für die Mehrblock-PSA-Modellierung von drei Reaktorblöcken über Ereignisablaufanalysen und Fehlerbäume sind in Abb. 2.16 und Abb. 2.17 gegeben. Dabei steht U_x, x = 1,2,3 stehen für die unterschiedlichen Reaktorblöcke. Eine Linie über dem U symbolisiert einen intakten Block.

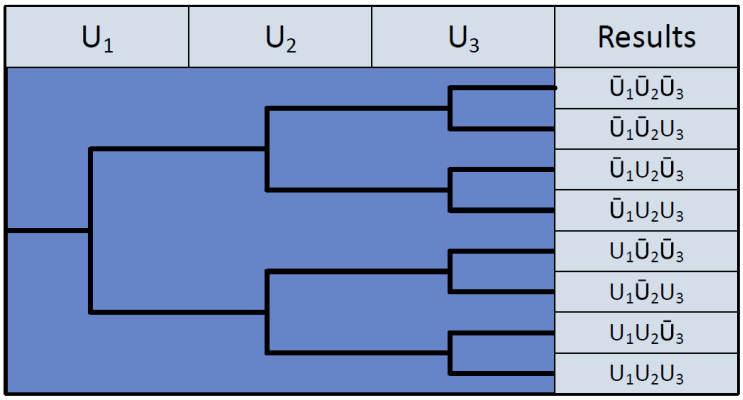


Abb. 2.16 Ereignisablaufanalyse für einen Standort mit drei Reaktorblöcken, aus /LIM 18/

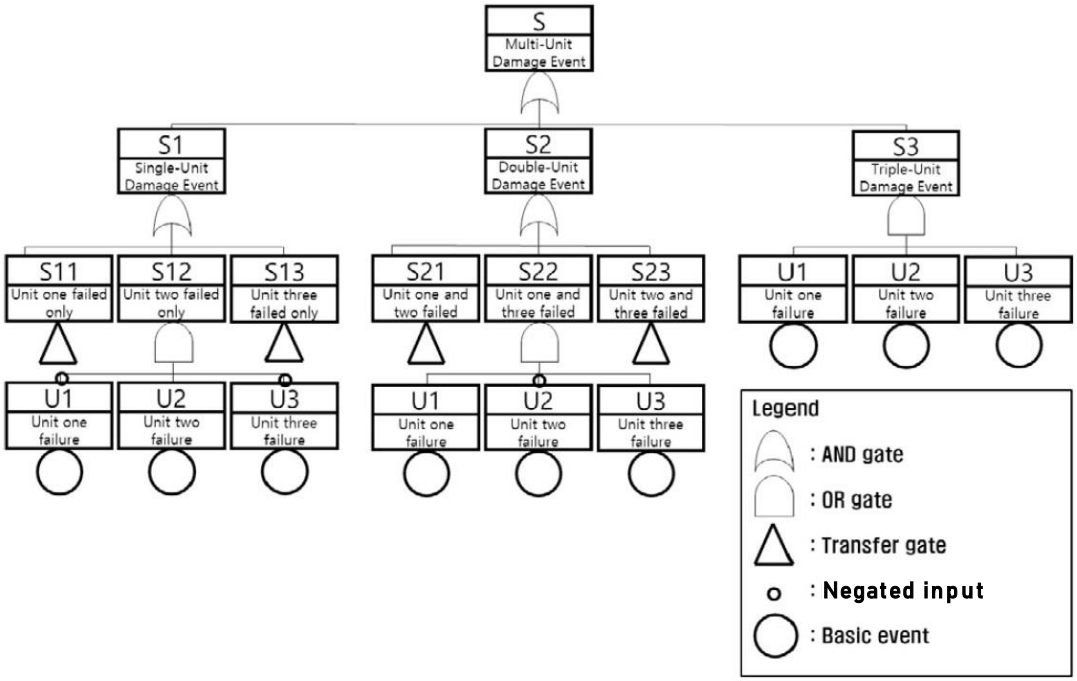


Abb. 2.17 Fehlerbaumanalyse für einen Standort mit drei Reaktorblöcken /LIM 18/

Zur Modellierung der GVA ist möglicherweise die Beta-Faktor-Methode zu einfach, da diese sehr konservativ eine hohe Wahrscheinlichkeit für den Ausfall gleicher Komponenten in mehreren Blöcken liefert. Die Alpha-Faktor-Methode hingegen hat den Nachteil, dass beispielsweise für 24 gleiche Komponenten (jeweils vier Komponenten in sechs Blöcken) $2^2 – 1$ Parameterwerte nötig sind. Eine hybride Methode könnte die Lösung zur Verringerung der Komplexität und zur Verhinderung einer zu hohen Konservativität sein.

In /KIM 18/ wird eine Mehrblock-PSA für einen koreanischen Kernkraftwerksstandort mit sechs Leistungsreaktoren durchgeführt. In einem ersten Schritt wird der Beitrag unabhängig auftretender auslösender Ereignisse in mehreren Reaktorblöcken auf die Standort-Kernschadenshäufigkeit untersucht. Die Untersuchungen basieren auf folgenden vereinfachenden Annahmen:

- Die sechs Blöcke sind baugleich und damit auch alle SSC. Nur die Betriebsmannschaften unterscheiden sich.
- Alle sechs Blöcke sind im Leistungsbetrieb bei maximaler Leistung. Andere Betriebsphasen werden nicht berücksichtigt.
- Alle auslösenden Ereignisse in den einzelnen Reaktorblöcken treten unabhängig voneinander auf. Es werden keine Abhängigkeiten zwischen den einzelnen Reaktorblöcken angenommen. Das Auftreten eines auslösenden Ereignisses in einem Block hat entsprechend der Modellierung keinen Einfluss auf das Auftreten eines auslösenden Ereignisses in einem anderen Block.
- Das „zeitgleiche“ Auftreten von mehr als einem auslösenden Ereignis in unterschiedlichen Reaktorblöcken bezieht sich auf eine Zeitspanne von 72 Stunden.

Zunächst werden für optimistische und pessimistische Annahmen die Kernschadenshäufigkeiten mehrerer Blöcke bestimmt. Der optimistische Fall beschreibt völlig unabhängige Blöcke (z. B. ohne GVA), der pessimistische Fall beschreibt eine komplette Abhängigkeit aller Blöcke mit Ausnahme der auslösenden Ereignisse.

Die Kernschadenshäufigkeiten f_k für k Blöcke eines Standortes mit m Reaktoren im optimistischen Fall ergeben sich über /KIM 18/

$$f_k = {}_mP_k \cdot \left[\sum_{i=1}^{n} f(IE_i) \cdot CCDP_i\right] \cdot \left[\sum_{i=1}^{n} Pr(IE_i) \cdot CCDP_i\right]^{k-1} \qquad (2.3)$$

Mit der Häufigkeit $f(IE_i)$ für ein spezifisches auslösendes Ereignis IE_i und der bedingten Wahrscheinlichkeit in einem anderen Block $Pr(IE_i)$. $CCDP_i$ ist die bedingte Kernschadenswahrscheinlichkeit bzgl. dem auslösenden Ereignis *i.* ${}_mP_k$ ist die Zahl der möglichen Kombinationen von Reaktorblöcken, *n* die Zahl der auslösenden Ereignisse, die in der Einzelblock-PSA untersucht werden. Für den pessimistischen Fall wird eine bedingte Kernschadenwahrscheinlichkeit von 1 angenommen, und es ergibt sich die Formel

$$f_k = {}_mP_k \cdot \left[\sum_{i=1}^{n} f(IE_i) \cdot CCDP_i\right] \cdot \left[\sum_{i=1}^{n} Pr(IE_i) \cdot 1\right]^{k-1} \qquad (2.4)$$

Die relativen Kernschadenshäufigkeiten für mehrere Blöcke des Standortes mit sechs Reaktorblöcken sind in Tab. 2.10 angegeben. Das Ergebnis verdeutlicht, dass sogar für den pessimistischen Fall das gleichzeitige Auftreten von Kernschadenszuständen in drei oder mehr Blöcken mit relativen Häufigkeiten von unter 0,1 % bei weiteren Betrachtungen vernachlässigt werden kann. Darüber hinaus zeigte sich, dass für auslösende Ereignisse mit vergleichsweise niedrigen Eintrittshäufigkeiten, z. B. auslösende Ereignisse infolge einer anlageninternen Überflutung oder eines internen Brandes, kein zeitgleiches Auftreten in zwei oder mehr Blöcken unterstellt werden muss, da im pessimistischen Fall relative Häufigkeiten von unter 1 % ermittelt werden konnten.

Tab. 2.10 Relative Kernschadenshäufigkeiten in mehreren Reaktorblöcken /KIM 18/

Anzahl der Reaktoren mit Kernschaden	Optimistischer Fall, Verhältnis zur Kernschadenshäufigkeit aus SUPSA für alle 6 Blöcke	Pessimistischer Fall, Verhältnis zur Kernschadenshäufigkeit aus SUPSA für alle 6 Blöcke
2	1,1 E-70	3,6 E-02
3	9,8 E-15	1,0 E-03
4	6,5 E-22	2,2 E-05
5	2,9 E-29	3,2 E-07
6	6,4 E-37	2,3 E-09

Des Weiteren wurde in /KIM 18/ ein MUPSA-Modell für die Berücksichtigung von zwei der sechs Blöcke erstellt. Entsprechend werden die Komponentengruppen zur Berücksichtigung von GVA nicht sehr groß, der zusätzliche Aufwand bleibt für zwei oder drei Komponenten in einem Block überschaubar. Im Fall von vier oder mehr Komponenten wird zur Beschreibung der GVA auf die einfachere Beta-Faktor-Methode zurückgegriffen. Dies stellt einen hybriden Ansatz in der Verwendung der Beta- und der Alpha-Faktor-Methoden dar.

Unter allen auslösenden Ereignissen in Folge von Einwirkungen von innen und außen wurden die folgenden vier Mehrblock-Auslöser auf Basis der koreanischen Kraftwerkspraxis ausgewählt:

- Ausfall der externen Stromversorgung in allen Reaktorblöcken,
- Ausfall der Not- und Nachwärmesenke in allen Reaktorblöcken,
- auslösendes Ereignis durch Erdbeben (insgesamt elf durch Erdbeben induzierte auslösende Ereignisse werden betrachtet, z. B. ein Ausfall der externen Stromversorgung als Folge eines Erdbebens),
- auslösendes Ereignis durch Tsunami.

Folgende Annahmen wurden getroffen:

- Die sechs Blöcke am Standort sind baugleich und damit auch alle SSC mit Ausnahme der Dieselgeneratoren.
- Die Betriebsmannschaften sind unterschiedlich, verwenden jedoch die gleichen Unterlagen, und die Störfallbeherrschung, Test- und Wartungsarbeiten werden in der gleichen Weise durchgeführt. Die Wahrscheinlichkeiten menschlicher Fehler sind in allen Reaktorblöcken gleich.
- Alle sechs Reaktorblöcke sind im Leistungsbetrieb unter Vollast. Andere Betriebsphasen werden nicht berücksichtigt.
- Alle sechs Reaktorblöcke sind gleichzeitig in gleichem Maße gleichzeitig vom auslösenden Ereignis betroffen.
- Beeinträchtigungen anderer Blöcke durch Kernschaden oder Spaltproduktfreisetzungen aus anderen Blöcken werden nicht berücksichtigt.
- Mitigative Maßnahmen werden nicht berücksichtigt.

Ein Beispiel für einen Fehlerbaum zur Bestimmung der Kernschadenshäufigkeit im Fall eines Ausfalls der externen Stromversorgung in mehreren Reaktorblöcken ist gegeben in Abb. 2.18.

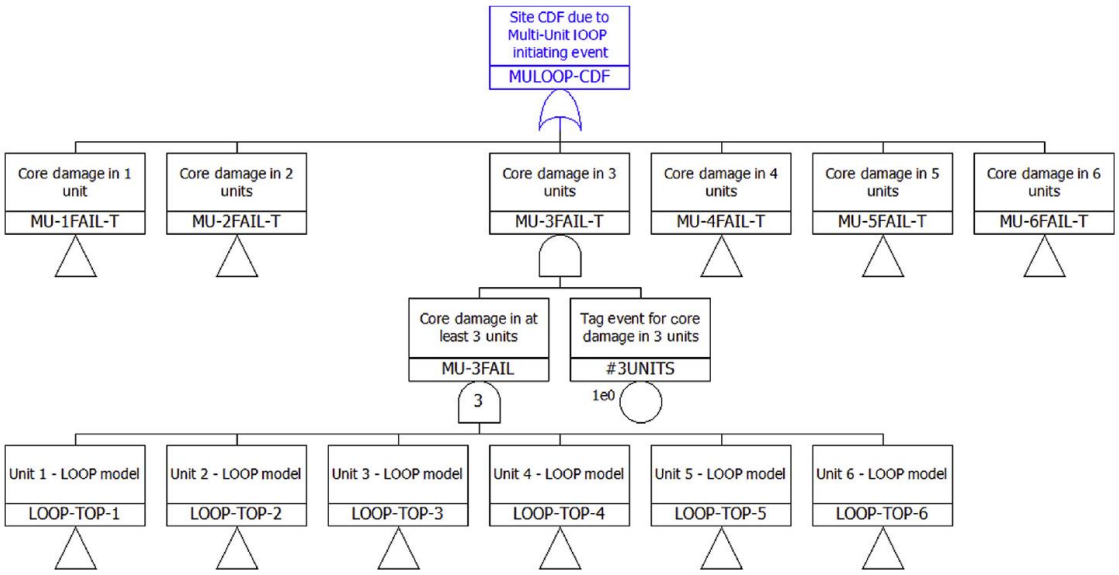


Abb. 2.18 Beispiel für einen Fehlerbaum zur Bestimmung der Standort-Kernschadenshäufigkeit nach Ausfall der externen Stromversorgung in mehreren Reaktorblöcken /KIM 18/

Mehrere Modellvereinfachungen wurden durchgeführt, um die gleichzeitige Handhabung von sechs SUPSA-Modellen in einem MUPSA-Modell zu erleichtern:

- Fehlerbäume, die nicht im Zusammenhang der MUPSA benötigt werden, wurden gelöscht.
- Die bedingten Kernschadenswahrscheinlichkeiten wurden für jedes auslösende Ereignis separat bestimmt.
- Die Namen aller Basisereignisse und Logikbausteine wurden um die Blocknummer des zugehörigen Reaktorblocks ergänzt, um voneinander zu unterscheiden zu sein.

Insgesamt wurden in der Mehrblock-PSA die folgenden fünf Abhängigkeiten zwischen den Reaktorblöcken modelliert:

1. Auslösende Ereignisse aus gemeinsamer Ursache
2. SSC, die von mehreren Reaktorblöcken genutzt werden
3. Abhängigkeiten menschlicher Fehler in mehreren Blöcken
4. GVA in mehreren Reaktorblöcken
5. Seismische Korrelationen in mehreren Reaktorblöcken

Die Ergebnisse der MUPSA-Analysen sind mit Ausnahme des Erdbebens in Tab. 2.11 zusammengefasst. Im Fall eines Tsunamis ist die Wahrscheinlichkeit für Kernschäden in allen Reaktorblöcken höher als die Wahrscheinlichkeit für einen Kernschaden in nur einem Reaktorblock. Nach einem Verlust der externen Stromversorgung oder der Not- und Nachwärmesenke in mehreren Blöcken dominieren die Kernschadenshäufigkeiten in einem oder zwei Blöcken.

Tab. 2.11 Ergebnisse der Mehrblock-PSA: Häufigkeiten für Kernschäden am betrachteten Standort, aus /KIM 18/

Anzahl der Blöcke mit Kernschaden	Verlust der externen Stromversorgung in mehreren Blöcken	Verlust der Not- und Nachwärmesenke in mehreren Blöcken	Tsunami
1	6,4 E-06	3,0 E-07	1,3 E-07
2	4,5 E-07	5,0 E-09	2,0 E-09
3	4,1 E-08	9,3 E-10	3,6 E-10
4	2,9 E-09	1,7 E-10	5,0 E-09
5	Gering	2,0 E-11	7,3 E-10
6	Gering	1,4 E-12	1,8 E-07

Die Modellierung des Erdbebens berücksichtigt elf Folgeereignisse (als Basisereignisse) modelliert, u. a. ein großes Leck oder den Ausfall der externen Stromversorgung. Für das gleiche auslösende Ereignis oder die gleiche Einwirkung von außen können entsprechend dieser Modellierung in den unterschiedlichen Reaktorblöcken unterschiedliche Folgeereignisse eintreten.

Darüber hinaus wurden in der Modellierung sechs Erdbebenstärken unterschieden. Aufgrund einer fehlenden Datenbasis werden die Erdbeben-induzierten GVA typischerweise vereinfacht binär modelliert mit vollständigen Korrelationen zwischen identischen und redundanten Komponenten und keinen Korrelationen für alle anderen Komponenten. Diese vereinfachte Annahme führt zur Überschätzung der Kernschadenshäufigkeiten, weshalb auch Korrelationskoeffizienten für Erdbeben-induzierte GVA von 0,0, 0,3, 0,5; 0,7 und 0,9 zusätzlich untersucht wurden. In Abb. 2.19 ist das Ergebnis der relativen Kernschadenshäufigkeiten für einem und für mehrere Reaktorblöcke dargestellt. Für größere Korrelationskoeffizienten steigt die Wahrscheinlichkeit für Kernschäden in mehreren Blöcken an.

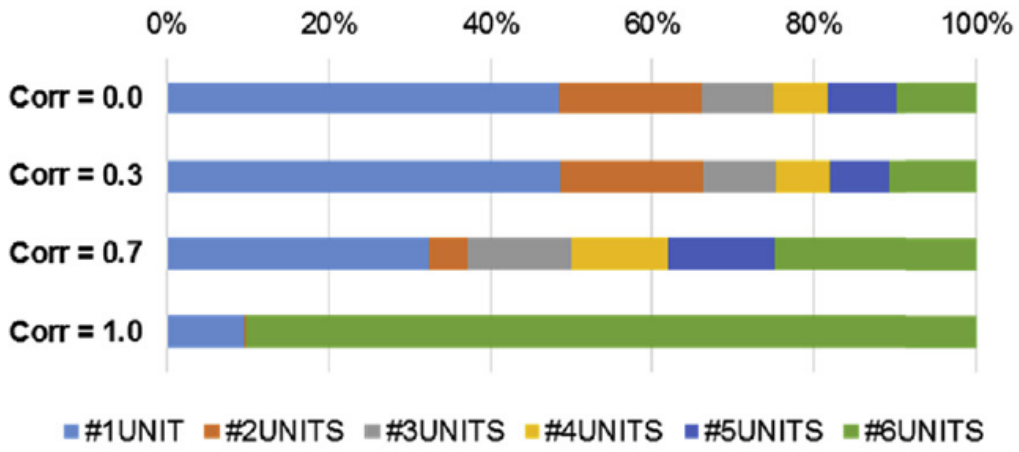


Abb. 2.19 Gesamtergebnisverteilung aller Erdbebenstärken für Erdbeben-induzierte Kernschadenshäufigkeiten in einem oder mehreren Reaktorblöcken für unterschiedliche Erdbebenkorrelationskoeffizienten /KIM 18/

Eine Software zur Modellierung und der Berücksichtigung von großen Fehlerbäumen im Rahmen einer Mehrblock-PSA ist in /HAN 18/ beschrieben. Die quantitative Auswertung einer MUPSA wird beschrieben über eine angepasste Methode zur Bestimmung der minimalen Schnitte oder alternativ über einen Monte-Carlo-Ansatz.

In der koreanischen Multi-Unit PSA werden Fälle von übergreifenden auslösenden Ereignissen explizit nicht betrachtet. In /STU 14/ werden diese auslösenden Ereignisse genauer analysiert und in drei Kategorien eingeteilt:

- Kaskadenverlauf: Das auslösende Ereignis in einem Block führt zu einem Kernschaden in diesem Block und in einem oder mehreren weiteren Blöcken.
- Ausbreitender Verlauf: Das auslösende Ereignis in einem Block führt zu Kernschäden in anderen Blöcken, jedoch nicht zu einem Kernschaden im Block mit dem auslösenden Ereignis.
- Beschränkter Verlauf: Es kommt nur in dem vom auslösenden Ereignis betroffenen Block zu einem Kernschaden.

Die Analysen führen über einen Scoping-Ansatz zu einer allgemeinen Abschätzung des Mehrblock-Risikos für Mehrblock-Standorte. Anhand eines realen Beispiels wird deutlich, dass das Risiko ausgehend aus dem gemeinsamen auslösenden Ereignis eines Erdbebens das Risiko von übergreifenden auslösenden Ereignissen sehr deutlich überwiegt.

Aus der Fachliteratur sind weitere Modelle zur Beschreibung von Mehrblock-Risiken bekannt, diese werden im Folgenden thematisch gegliedert vorgestellt.

Übergreifende Einwirkungen

Auslösende Ereignisse, welche mehrere Blöcke gleichzeitig beeinträchtigen, können in zwei Kategorien eingeteilt werden /HAG 21/:

- Definite Events – mehrere Reaktorblöcke sind unmittelbar betroffen. Entsprechende Ereignisse sind Netzstörungen, Ausfall der gemeinsamen Wärmesenke, naturbedingte Einwirkungen von außen, Erdbeben, Hochwasser, extreme Wetter- und Witterungseinflüsse, biologische Einwirkungen, anlagenexterne Brände und zivilisatorische Einwirkungen wie z B. ein unfallbedingter Flugabsturz.
- Conditional Events – Betriebsstörungen oder Störfälle in einem Block oder einer anderen Radionuklidquelle, welche einen benachbarten Reaktorblock beeinträchtigen.

Zu den Definite Events zählen auch die oben beschriebenen GVA-Ereignisse, die u. a. NuScale als mögliche auslösende Ereignisse berücksichtigt (siehe dazu /NUS 20/). Hierzu zählen das gleichzeitige Versagen identischer Komponenten in unterschiedlichen Blöcken, wie beispielsweise zwei gealterte Rohre, die in unterschiedlichen Reaktorblöcken in geringem Zeitabstand zueinander (innerhalb der Missionszeit von 72 h) gemeinsam versagen.

Gemeinsame Verwendung bzw. begrenzte Verfügbarkeit von Systemen oder gemeinsam genutzte Strukturen

Im SMR von NuScale werden folgende Systeme gemeinsam von mehreren Reaktormodulen verwendet /NUS 20/:

- das Reaktorbecken und dessen Systeme,
- das Flut- und Drainagesystem des Sicherheitsbehälters (Englisch: containment flooding and drain system, CFDS),
- die Reaktorhalle,
- die Betriebsmannschaft.

An koreanischen Kernkraftwerksstandorten werden folgende Systeme gemeinsam von mehreren Blöcken verwendet /KIM 18/:

- ein alternativer Wechselspannungsdieselgenerator, welcher von drei Reaktorblöcken gemeinsam genutzt wird,
- das Umspannwerk,
- das Meerwasser in der Nähe des Standorts als Not- und Nachwärmesenke.

Identische Komponenten – GVA

Identische Komponenten sind Komponenten mit derselben Auslegung, gleicher Betriebsweise und betrieblicher Umgebung /HAG 21/. Entsprechende Komponenten sind anfällig für Ausfälle aufgrund einer gemeinsamen Ursache (GVA). Bäckström et al. /BAE 18/ beschränken sich bei der Betrachtung der GVA in einem konservativen Modell auf die Berücksichtigung gemeinsamer blockübergreifender Ausfälle identischer Komponenten mit identischem Aufbau. Die anlagenweite GVA-Wahrscheinlichkeit wird konservativ über die Anzahl aller identischen Komponenten skaliert und basiert auf der GVA-Wahrscheinlichkeit aller identischen Komponenten eines Reaktorblocks.

Ein diesbezüglich erweiterter Ansatz wird in /KIM 20/ (und bezugnehmend in /IAE 21/) beschrieben. Das Baumdiagramm in Abb. 2.20 erlaubt die Bestimmung der Korrelationsfaktoren für Systeme oder Komponenten, die nicht komplett identisch sind. Alle ‘Faktoren‘ entlang des Baums werden aufsummiert. Es wird zwischen dem Aufbau des Systems, der Betriebsweise und den Umgebungsbedingungen unterschieden. Ein ähnliches Diagramm mit anderen Ergebniswerten und der zusätzlichen Berücksichtigung von Wartungsarbeiten ist in /JAN 18/ zu finden. Unter Berücksichtigung von Ausfällen aus gemeinsamer Ursache in mehreren Reaktorblöcken ergeben sich wesentlich höhere Werte für die Mehrblock-Kernschadenshäufigkeiten.

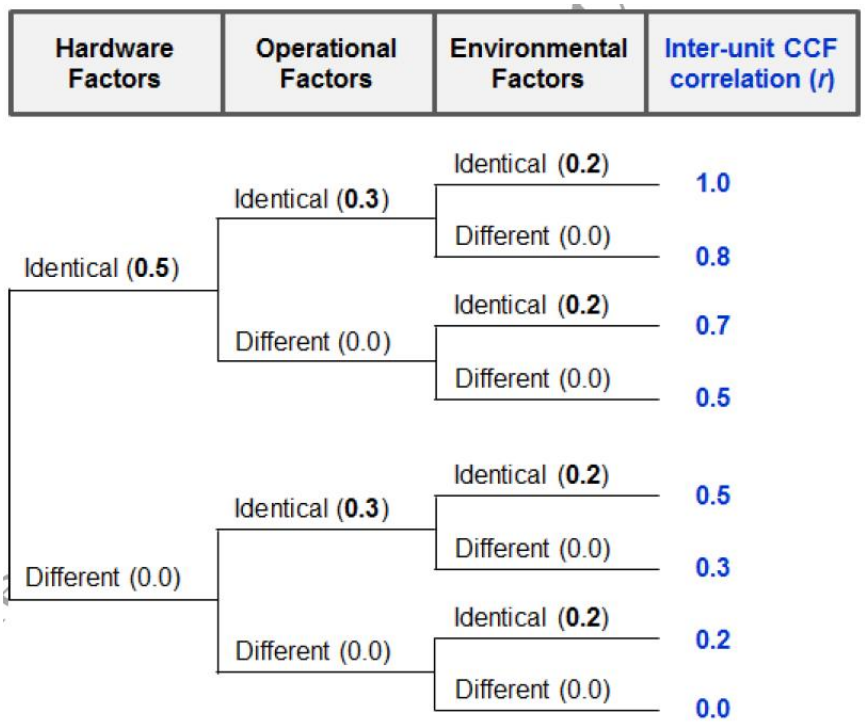


Abb. 2.20 Erweitertes Schema zur Bestimmung der Korrelationsfaktoren zwischen identischen und verschiedenen Systemen, aus /IAE 21/

Es gibt verschiedene vereinfachte Modelle zur implizierten Beschreibung von GVA /SCH 89/. Die wichtigsten werden nachfolgend kurz erläutert.

Beta-Faktor-Methode

Im Fall einer sehr beschränkten empirischen Datenbasis kann dieses einfache Modell angewendet werden. Die Wahrscheinlichkeit eines Ausfalls aller m Komponenten ergibt sich aus der Wahrscheinlichkeit eines Ausfalls einer Komponente Q_t und dem β-Faktor:

$$Q_k = \begin{cases} (1-\beta)\cdot Q_t & k = 1 \\ 0 & m > k > 1 \\ \beta \cdot Q_t & k = m \end{cases} \qquad (2.5)$$

Multiple-Greek-Letter-Methode

Diese Methode bildet auch Mehrfachausfälle, die nicht alle Komponenten betreffen ab. Entsprechend werden weitere Parameter benötigt. Beispielsweise ergibt sich für m = 3:

$$\begin{aligned} &\text{Einzelausfall } Q_1 = (1-\beta)\cdot Q_t \\ &\text{Doppelausfall } Q_2 = 0{,}5\cdot\beta\cdot(1-\gamma)\cdot Q_t \\ &\text{Tripelausfall } Q_3 = \beta\cdot\gamma\cdot Q_t \end{aligned} \qquad \textbf{(}2.6)$$

Alpha-Faktor-Methode

Im Unterschied zur Multiple-Greek-Letter-Methode werden bei der Alpha-Faktor-Methode die Schätzwerte für die Ausfallwahrscheinlichkeiten über Verhältnisse beobachteter Ein- und Mehrfachausfälle ermittelt, so ergibt sich für den Ausfall von *k* Komponenten:

$$\begin{aligned} Q_k &= {}^{k}\Big/\binom{m-1}{k-1}\cdot\frac{\alpha_k}{\alpha_t}\cdot Q_t \\ \alpha_t &= \sum_{k=1}^{m} k\cdot\alpha_k \end{aligned} \qquad (2.7)$$

Die Gesamtausfallwahrscheinlichkeit einer Komponente A ergibt sich dann als Summe von Einzelausfall- und Mehrfachausfällen, zum Beispiel für drei Komponenten *A, B, C* ergibt sich ein Gesamtausfall entsprechend der in der nachfolgenden Abb. 2.21 dargestellten Logik.

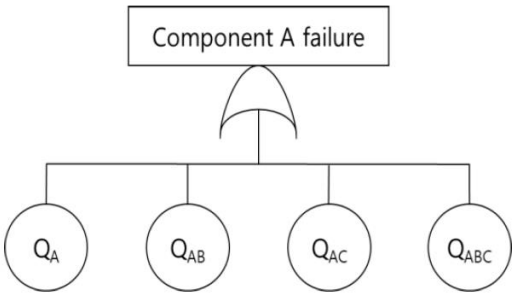


Abb. 2.21 Gesamtausfall einer Komponente A für ein dreifach redundantes System /JAN 18/

Personalverfügbarkeit, Personalzuverlässigkeit und organisatorische Faktoren

Diese Kategorie beschreibt Fehler der Betriebsmannschaft nach Eintritt eines auslösenden Ereignisses (post-event action). Entsprechende Fehler können sich zum einen auf

die Störfallbeherrschung des gestörten Reaktorblocks oder andererseits auf benachbarte Blöcke auswirken, z. B. durch eine fehlerhafte Rückschaltung nach einem Ausfall der Netzeinspeisung eines Blocks /HAG 21/. Eine weitere blockübergreifende Abhängigkeit ergibt sich durch die Bindung personeller Ressourcen, z. B. die Mitglieder der Werkfeuerwehr bei einem größeren Brand in einem Reaktorblock.

Bäckström et al. /BAE 18/ modellieren den personellen und organisatorischen Faktor der PSA über einen Erschwerungsgrad oder Mehraufwand (Penalty Factor). Der Grad der Erschwerung wird über eine Experteneinschätzung festgelegt. Folgende Multiplikatoren werden vorgeschlagen:

- keine wesentlichen übergreifenden Personalanforderungen, Erschwerungsfaktor = 1,
- niedriger Einfluss auf die Personalverfügbarkeit, Erschwerungsfaktor = 2,
- zusätzlich Herausforderungen, mittlerer Einfluss, Erschwerungsfaktor = 5,
- hoher Einfluss auf die Personalverfügbarkeit, Erschwerungsfaktor = 10.

Die Multiplikatoren werden auf die Ausfallwahrscheinlichkeiten für die Durchführung von Handlungen des Betriebspersonals angewendet. Sind die Anforderungen von der Betriebsmannschaft nahezu unmöglich zu leisten, so wird die Ausfallwahrscheinlichkeit mit 1 angenommen.

NuScale modelliert die Fehlerwahrscheinlichkeit der Betriebsmannschaft für die Fehlerdiagnose und Durchführung von Handmaßnahmen in einer PSA für ein einzelnes Reaktormodul in drei Stufen (siehe dazu NUS 20/):

- mindestens 30 Minuten für die Fehlerdiagnose und ausreichend Zeit für die Durchführung der Maßnahmen (Fehlerwahrscheinlichkeit = 4.0 E-03),
- minndestens 30 Minuten für die Fehlerdiagnose und wesentlich mehr Zeit für die Durchführung der Maßnahmen als notwendig (Fehlerwahrscheinlichkeit = 2.2 E-04),
- mehr als eine Stunde für die Fehlerdiagnose und wesentlich mehr Zeit für die Durchführung der Maßnahmen als notwendig, allerdings muss die Handmaßnahme lokal durchgeführt werden (Fehlerwahrscheinlichkeit = 1.4 E-03).

Die Modellierung fasst dabei die Fehlerdiagnose und die Maßnahmendurchführung in einem Fehlerbaumeintrag zusammen. Das gesamte Zeitbudget, das bis zur spätesten Durchführung der Maßnahme zur Verfügung steht, teilt sich in die beiden Unteraufgaben der Diagnose und der Maßnahmendurchführung auf. Darüber hinaus wird zwischen lokalen Maßnahmen im Bereich des betroffenen Moduls und der Durchführung von Maßnahmen aus der Warte heraus unterschieden. Die Fehlerdiagnose wird nominell mit einer Wahrscheinlichkeit von 1 % als fehlerhaft angenommen, die Maßnahmendurchführung mit 0,1 %. Innerhalb einzelner Ereignisabläufe wird für zwei untersuchte Handmaßnahmen der Betriebsmannschaft eine moderate Abhängigkeit modelliert, für die dritte Handmaßnahme eine starke Abhängigkeit und darüber hinaus eine komplette Abhängigkeit. Ein entsprechendes quantitatives Modell wird in /SWA 83/ als „Model positiver Abhängigkeiten“ vorgestellt, die bedingten Fehlerwahrscheinlichkeiten für unterschiedliche Abhängigkeit zwischen Ereignis *A* und Ereignis *B* berechnen sich über die Fehlerwahrscheinlichkeit *N* eines isolierten Ereignisses wie folgt:

- keine Abhängigkeit: $W[\mathrm{B}|\mathrm{A}] = \mathrm{N}$,
- schwache Abhängigkeit: $W[\mathrm{B}|\mathrm{A}] = \frac{1+19\cdot N}{20}$,
- mittlere Abhängigkeit: $W[\mathrm{B}|\mathrm{A}] = \frac{1+6\cdot N}{7}$,
- starke Abhängigkeit: $W[\mathrm{B}|\mathrm{A}] = \frac{1+N}{2}$,
- vollständige Abhängigkeit: $W[\mathrm{B}|\mathrm{A}] = 1{,}0$.

Für das NuScale-Modell könnte das bedeuten, dass für mehrere Handmaßnahmen mit Fehlerwahrscheinlichkeit von *N* = 2,2 E.04 während eines Ereignisablaufes gilt:

- 1. Handmaßnahme: $W_1 = N = 2{,}2 \cdot 10^{-4}$,
- 2. Handmaßnahme: $W_2 = \begin{cases} N = 2{,}2 \cdot 10^{-4}, \text{ falls 1. Handmaßnahme erfolgreich} \\ \frac{1+6\cdot N}{7} = 1{,}43 \cdot 10^{-1}, \text{ falls 1. Handmaßnahme fehlerhaft} \end{cases}$
- 3. Handmaßn.: $W_3 = \begin{cases} N = 2{,}2 \cdot 10^{-4}, \text{ falls 1. und 2. Handmaßnahme erfolgreich,} \\ \frac{1+6\cdot N}{7} = 1{,}43 \cdot 10^{-1}, \text{ falls 1. oder 2. Handmaßn. fehlerhaft,} \\ \frac{1+N}{2} = 5{,}00 \cdot 10^{-1}, \text{ falls 1. und 2. Handmaßnahme fehlerhaft} \end{cases}$,
- Weitere Handmaßnahmen: $W_n = 1{,}0$, falls 3 vorangegangene Handmaßnahmen fehlerhaft sind.

Die Reihenfolge, in der die Handmaßnahmen durchgeführt werden, ist für dieses Modell besonders wichtig, da Handmaßnahmen, die aufgrund von vorherigen Fehlern notwendig werden, mit erhöhter Wahrscheinlichkeit auch fehlerhaft sind.

Korrekturmaßnahmen für fehlerhafte Handlungen der Betriebsmannschaft werden in der PSA von NuScale nicht berücksichtigt. Fehlhandlungen, die den Ereignisablauf verschlechtern könnten, konnten nicht gefunden werden.

Die Modellierung des Multi-Modul-Risikos erfolgt über einen Faktor, der die Leistungsbeeinflussung der Betriebsmannschaft beschreibt. Der Leistungsbeeinflussungsfaktor liegt bei einem Wert von 10. Eine Einschränkung der lokalen Tätigkeiten durch eine Freisetzung eines anderen betroffenen Moduls wird nicht explizit modelliert. Abhängigkeiten zwischen Handmaßnahmen werden nur im Ereignisablauf eines Moduls berücksichtigt und nicht übergreifend für Transienten in mehreren Modulen. Die Betriebsmannschaft ist für bis zu zwölf Module zuständig.

Systematische Fehler bei Wartungs- und Inspektionsarbeiten

Diese Kategorie beinhaltet Personalfehler vor Eintritt des auslösenden Ereignisses (pre-event action). Systematische Fehler bei identischen Arbeitsabläufen können die Verfügbarkeit von Komponenten beeinträchtigen oder zu auslösenden Ereignissen in mehreren Anlagen führen /HAG 21/.

NuScale verwendet entsprechend Aussagen in /NUS 20/ für die Modellierung und Quantifizierung von systematischen Fehlern bei Wartungs- und Inspektionsarbeiten generische Daten. Sowohl präventive (geplante) als auch korrektive (z. B. Reparaturarbeiten) Maßnahmen (post-event) werden berücksichtigt. Mögliche Fehlerursachen aus Wartungs- und Inspektionsarbeiten können sein

- Fehler beim Zusammenbau, Wiedereinsetzen oder bei der Wiederinbetriebnahme,
- Kalibrierungsfehler von Komponenten oder
- eine fehlerhafte Wiederherstellung von Komponenten nach Überprüfungen der Funktionalität.

Nach Wartungsarbeiten werden Überprüfungen der Funktionalität der gewarteten Systeme durchgeführt. Da keine Wartungsarbeiten an mehreren parallelen Pumpen gleich-

zeitig ausgeführt werden, werden keine Abhängigkeiten der Fehlerwahrscheinlichkeiten für diesen Fall angenommen. Ansonsten wird konservativ von gleichzeitiger oder aufeinanderfolgender Durchführung von geplanten Wartungsarbeiten an unterschiedlichen Redundanzen ausgegangen. Diese Wartungsarbeiten finden typischerweise in einem sicheren Anlagenzustand während eines Brennelementwechsels unter passiver Abfuhr der Nachzerfallsleistung statt.

Die Modellierung des Multi-Modul-Risikos erfolgt über einen Faktor, der die Kopplung der Wartungs- und Inspektionsarbeiten modelliert. Dieser Faktor liegt zwischen und 0,1 für Komponenten, die in allen Modulen unabhängig vorhanden sind, und 1,0 (vollständige Kopplung) für Komponenten, die modulübergreifend arbeiten (z. B. Dieselgeneratoren).

Organisatorische Abhängigkeiten

In vielen Fällen besteht eine gemeinsame Organisation seitens eines gemeinsamen für mehrere Reaktorblöcke an einem Kraftwerksstandort. Für den Betriebs- und Störfallablauf werden Prozeduren erstellt. Als Beispiele für blockübergreifende organisatorische Abhängigkeiten sind eine mögliche Übertragung fehlerhafter Prozeduren aus bestehenden Reaktorblöcken hin zu neuen Blöcken oder fehlerhafte Auslegungsberechnungen, die auf andere Blöcke übertragen werden, zu nennen /HAG 21/.

Behandlung von Unsicherheiten

Unsicherheiten in den PSA-Ergebnissen sind grundsätzlich zu berücksichtigen, wenn aus den Ergebnissen Schlussfolgerungen und Entscheidungen abgeleitet werden sollen. Drei Gruppen von Unsicherheiten lassen sich entsprechend /HAG 21/ wie folgt unterscheiden:

- Unsicherheit bezüglich der Vollständigkeit der PSA,
- Unsicherheit bezüglich der Modellierung und dem Einfluss der verwendeten Modelle, Annahmen und Abschätzungen auf das Ergebnis, hier können Sensitivitätsanalysen dazu beitragen, diese Unsicherheit zu quantifizieren, sowie
- statistische Unsicherheit bzgl. der Zuverlässigkeitskenngrößen und Eintrittshäufigkeiten übergreifender Einwirkungen bzw. auslösender Ereignisse; diese Unsicher-

heiten werden typischerweise über Monte-Carlo-Simulationen im PSA-Ergebnis berücksichtigt bzw. im Ergebnis ausgewiesen.

Insbesondere die Unsicherheiten aus den ersten beiden Gruppen können aufgrund der höheren Komplexität einer Multi-Unit PSA höher ausfallen als bei einer Single-Unit PSA.

Darüber hinaus sind folgende Unsicherheiten besonders hervorzuheben /HAG 21/:

- Unsicherheit in Bezug auf die Modellierung und den Grad der Abhängigkeiten der menschlichen Handlungen zur Störfallbeherrschung in mehreren Reaktorblöcken,
- Berücksichtigung eines administrativen Abschaltens eines nicht betroffenen Reaktorblocks sowie
- Korrelationsgrad gleichartiger Komponenten in benachbarten Reaktorblöcken bei übergreifenden Einwirkungen von außen (insbesondere Erdbeben) und Einwirkungskombinationen.

2.5 Erweiterte PSA-Methoden für Small Modular Reactors

Die Arbeiten von C. Smith et al. vom Idaho National Laboratory (INL) /SMI 12/ befassen sich mit einer erweiterten und verbesserten Methodik der PSA, um SMRs in die PSA einzuschließen. Durch die Verwendung der entwickelten Methodik ergeben sich insbesondere die in Tab. 2.12 vorgestellten Verbesserungen.

Tab. 2.12 Verbesserungen einer erweiterten PSA

Potenzial im Bereich …	Bisherige PSA-Einschränkung	Vorteile einer erweiterten PSA
Simulation von Unfallabläufen	Eingeschränkte Berücksichtigung von dynamischem Ablaufverhalten	Möglichkeit zur Berücksichtigung von Zeitaspekten, welche einen Einfluss auf Sicherheitsmargen und andere physikalischen Phänomene haben
Bestimmung der Sicherheitsmargen	Sicherheitsmargen werden nicht bestimmt, sondern einzelne Endzustände ergeben sich aus der Modellentwicklung	Sicherheitsmargen werden durch die Kopplung von deterministischen und probabilistischen Rechnungen bestimmt

Potenzial im Bereich …	Bisherige PSA-Einschränkung	Vorteile einer erweiterten PSA
Räumliche Wechselwirkungen	Sehr eingeschränkte Berücksichtigung von räumlichen Wechselwirkungen, hauptsächlich beschränkt auf Überflutungs- und Brandmodelle	Die dreidimensionale Modellierung von Gebäudeteilen und Systemen mit Berücksichtigung physikalischer Gesetzmäßigkeiten ermöglicht die Simulation von räumlichen Wechselwirkungen während des Störfallablaufs
Darstellung des Ausfallgrundes	Spezifische Ausfallgründe werden in Fehlermodellen, wie „Fehler beim Start“ und „Fehler im Betrieb“, zusammengefasst	Eine sichere Datengrundlage von Ausfallgründen und -modellen wird in eine Komponentenbibliothek eingebaut und bei Bedarf wird der Ausfallgrund ausgewählt
Cloudbasierte Verfahren zur Erstellung, Auswertung und Speicherung der PSA-Modelle	Üblicherweise werden PSAs von einzelnen Experten oder kleinen Expertenteams mit eingeschränktem Austausch und eingeschränkter Rechenkapazität erstellt	Teams mit unterschiedlicher Expertise und Fokus können sowohl Modelle als auch Rechenkapazität teilen, um verbesserte Analysen durchzuführen

Eine vorgeschlagene Erweiterung der PSA besteht in der Verwendung probabilistischer Sicherheitsmargen in deterministischen Sicherheitsanalysen, d. h. die Sicherheitsmarge zwischen tatsächlichem Versagen einer Komponente und dem konservativen Versagenspunkt soll über eine Wahrscheinlichkeitsfunktion beschrieben werden. Bei Bedingungen zwischen tatsächlichem Versagen und konservativem Versagenspunkt besteht demnach nur eine bestimmte Wahrscheinlichkeit kleiner als 1, dass die Komponente versagt. Dazu sollen dynamisch bei der Simulation der probabilistischen Risiken die Zwischenergebnisse der deterministischen Analysen (wie beispielsweise Temperatur und Druck) ausgewertet und das Ergebnis in der weiteren deterministischen Rechnung berücksichtigt werden. Die Besonderheit dieser Erweiterung drückt sich in den Austauschpfeilen zwischen den Arbeitspunkten 2 und 3 in Abb. 2.22 aus.

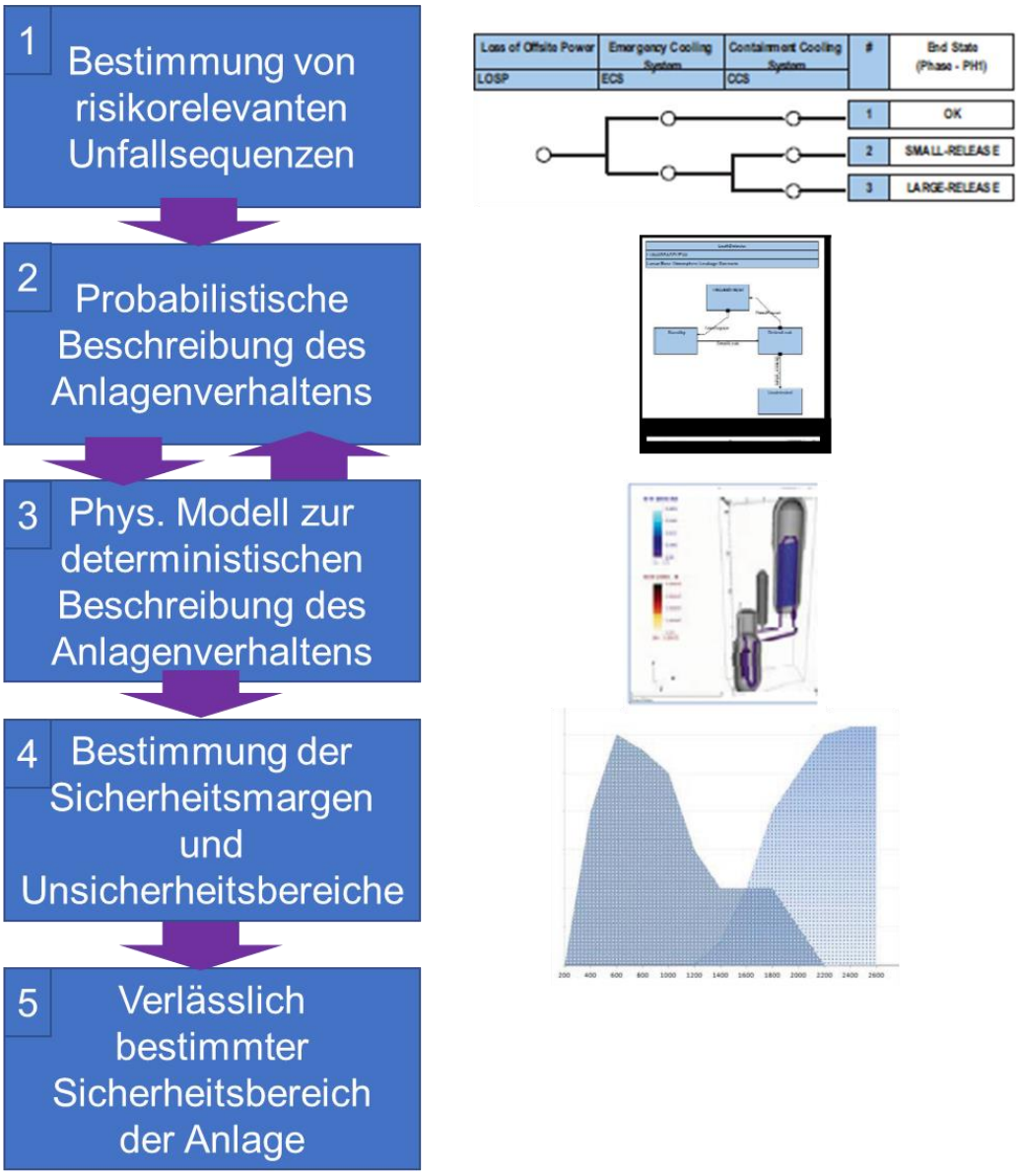


Abb. 2.22 Arbeitsablaufplan für die erweiterte PSA nach /SMI 12/

Neben den probabilistischen Sicherheitsmargen wird ein internet-cloud-basiertes PSA-System vorgeschlagen. Alle PSA-beteiligten Mitarbeiter profitieren von folgenden Verbesserungen:

- Nutzung aktueller Daten und Modelle mit einer speziellen Unterstützung durchdatenbasierte Suchanfragen,
- Verwendung zentral bereitgestellter (und browsergestützter) Programme zur Durchführung der Analysen und zum Teilen der Ergebnisse im Team,
- Erweiterung aktueller Software-Lösungen zur Überprüfung des probabilistischen Modells oder der probabilistischen Simulation,

- ein einfach zugängliches, sicheres Nachschlagwerk zur Unterstützung zukünftiger Expertengenerationen und als Referenz für eine vorbildliche PSA-Durchführung,
- integrierte Zusammenarbeit der Mitglieder des Teams,
- Anbindung an Rechenzentren, um die Einschränkungen der Rechenkapazität durch die Verwendung nur eines Desktop-Computers zu umgehen.

Darüber hinaus ist ein Modul angedacht, das räumliche Wechselwirkungen untersucht, beispielsweise das ausströmende Kühlmittel nach einem Rohrversagen (vgl. Abb. 2.23).

Abb. 2.23 Dreidimensionale Simulation des Beckens der Pumpstation, die zu einem Wasserschaden an einem naheliegenden Generator führt /SMI 14/

Weitere Ideen zur Optimierung von PSA werden in /SMI 13/ vorgestellt. Diese Publikation war die Grundlage für ein Treffen mit Interessensvertretern, um ein technisches Feedback zu den detaillierten technischen Rahmenspezifikation für die probabilistische Risikobewertung für SMR zu erhalten. Moderne Sicherheitsanalysen können von Fortschritten in folgenden Bereichen profitieren:

- parallele und verbesserte Rechenmethoden,
- dynamische Simulationen,
- Alterungsschädigungsmodelle für Materialien,

- integrierte Systeme und verbesserte Sensoren,
- virtuelle Umgebungen,
- Modellierung der menschlichen Wahrnehmung,
- Informationstechnik,
- Parameterdatenanalysen.

Für die Zulassung von SMRs werden folgende Untersuchungen erforderlich sein:

- Störfallabhängiger Nachweis der Kraftwerkstauglichkeit, was eine wohlüberlegte Auswahl der zu analysierenden Ereignisse und ein abgestuftes Vorgehen bei der Störfallanalyse impliziert,
- Berücksichtigung von Unsicherheiten (der Umgang mit Unsicherheiten in den Rechnungen statt der veralteten Praxis der Rechnung mit konservativen Werten),
- probabilistische Risikoanalyse (notwendig in heutigen Zulassungsverfahren in den meisten Ländern),
- Bearbeitung SMR-spezifischer technischer Fragestellungen (z. B. der Betrieb mehrerer Reaktormodule),
- Bearbeitung technologischer Fragestellungen (z. B. Zuverlässigkeit passiver Systeme).
- Die sorgfältige Bestimmung der Systemstruktur und Leistungsfähigkeit, welche im Betrieb gewartet werden muss.

Die Zulassungsvoraussetzungen in den USA wurden nach den Reaktorunfällen von Fukushima Dai-ichi angepasst, folgende Kategorisierung von Störfällen ist angedacht:

- Auslegungsereignisse:
  - ungestörter Betrieb,
  - Betriebsstörungen,
  - Auslegungsstörfälle (einschließlich Einwirkungen von innen),
  - Auslegungsstörfälle infolge Einwirkungen von außen,

- Auslegungsüberschreitende Ereignisse:
  - Ereignisse, die eine Erweiterung der Auslegung erfordern:
    - anlageninterne Ereignisse (einschließlich Einwirkungen von innen),
    - Einwirkungen von außen,
  - Szenarien im Restrisikobereich:
    - anlageninterne Ereignisse (einschließlich Einwirkungen von innen),
    - Einwirkungen von außen.

In /SMI 13/ wird eine Methode zur anpassungsfähigen Stichprobenerzeugung vorgestellt. Typischerweise ergeben sich bei Unsicherheitsanalysen zwei Probleme, die Anzahl der Unsicherheitsparameter ist sehr hoch und der Rechenaufwand ist sehr hoch. Daher kann der gesamte hochdimensionale Lösungsraum nur sehr punktuell analysiert werden. Eine anpassungsfähige Steuerung der Stichprobenerzeugung tastet den Lösungsraum systematischer ab. Dieser Prozess erfordert drei Schritte:

- Durchführung einiger anfänglicher Simulationen entsprechend der gegebenen Unsicherheitsintervalle mit Monte-Carlo-Stichprobenerzeugung;
- Erzeugung eines Ersatzmodells auf Grundlage der Ergebnisse der anfänglichen Simulationen (State Estimation);
- Auf Grundlage des neuen Modells werden die Stichproben nach Wichtigkeit gewichtet und die Stichproben mit höchster Gewichtung werden weiterverwendet (Action Selection).

Dann wiederholt sich der Ablauf mit den neuen Stichproben. Das Verfahren endet mit Erreichen einer Konvergenz.

Das Ablaufschema ist in Abb. 2.24 gezeigt.

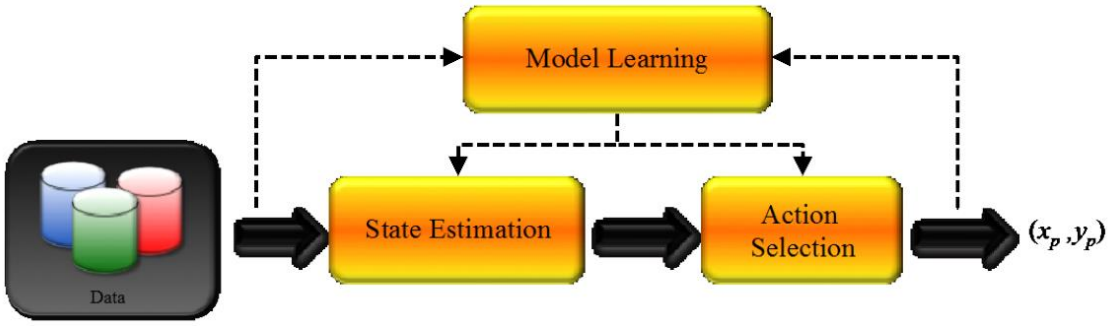


Abb. 2.24 Iteratives Verfahren zur anpassungsfähigen Stichprobenerzeugung /SMI 13/

2.6 Zusammenfassung

In einigen wesentlichen Punkten unterscheidet sich eine PSA für SMR von bisherigen PSA. Insbesondere kommen in einigen SMR-Konzepten mehr passive Systeme zum Einsatz. Die Zuverlässigkeit der passiven Systeme muss im Zusammenhang mit einer PSA bewertet werden. Hierfür wurden verschiedene Methoden entwickelt, z. B. die APSRA-Methode. Im Fall thermohydraulischer passiver Systeme, wie Naturumläufen, können mit Hilfe von Rechentools, z. B. ATHLET, RELAP oder MELCOR, mögliche Ausfallbedingungen bestimmt werden. Verschiedene Einflussfaktoren, insbesondere das Kühlmittelinventar und die Menge an nicht-kondensierbaren Gasen im System, können zu Ausfällen führen. Detaillierte Untersuchungen zu den Ausfallwahrscheinlichkeiten der Naturumläufe in bisherigen DWR konnten nicht gefunden werden. In DWR fallen die Hauptkühlmittelpumpen im Notstrombetrieb aus oder werden im Fall eines kleinen Lecks abgeschaltet, die weitere Kühlung erfolgt dann über Naturumläufe im Primärkühlsystem.

Die PSA für eine Anlage mit mehreren SMR-Modulen, ein Konzept, welches u. a. NuScale verwendet, kann grundsätzlich analog zur Mehrblock-PSA für einen Standort mit mehreren Leistungsreaktoren durchgeführt werden. Allerdings sind die methodischen Ansätze zur Durchführung einer Multi-Unit PSA weltweit noch nicht sehr weit entwickelt und verbreitet. Einige Datenlücken, z. B. bzgl. der Ausfallraten für GVA in unterschiedlichen Reaktoren, und methodische Lücken, z. B. zur Berücksichtigung von Personalunverfügbarkeiten nach Radionuklidfreisetzungen aus einem anderen Reaktor am Standort, sind noch nicht vollständig geschlossen. Insbesondere die Reaktorunfälle von Fukushima Dai-ichi werfen die Frage nach der Notwendigkeit für Mehrblock-PSA auf. Reaktorübergreifend sind gemeinsam genutzte Anlagenteile und Systeme, GVA, übergreifende Einwirkungen und Einwirkungskombinationen, die Zuverlässigkeit von

Personalhandlungen sowie Wartungs- und Inspektionsarbeiten zu modellieren. Alternativ kann auf konservative Abschätzungen zum Gesamtrisiko (scoping approach) zurückgegriffen werden.

Neben den passiven Systemen und der Multi-Unit PSA können die PSA-Methoden verbessert und erweitert werden. Insbesondere die Arbeiten von Smith et al. /SMI 12/, /SMI 13/ und /SMI 14/ beschäftigen sich mit einer Modernisierung und Erweiterung der PSA-Methoden mit Blick auf SMRs. Die dreidimensionale Modellierung von Gebäudeteilen und Systemen und die entsprechende Betrachtung räumlicher Wechselwirkungen ist beispielsweise im Hinblick auf die kompakte Bauweise von SMRs von besonderem Interesse.

Insgesamt hat sich bei der Aufarbeitung des Standes von Wissenschaft und Technik gezeigt, dass für die Durchführung von PSA für SMRs die bisherigen methodischen Ansätze zwingend erweitert werden müssen.

3 Beschreibung der Referenzanlage

Für die Erstellung einer PSA ist es zwingend erforderlich, detaillierte Kenntnisse über die Technik, Funktion und Betriebsweise der zu betrachtenden Anlage zu haben. Weltweit gibt es eine Vielzahl unterschiedlicher Konzepte für SMRs. Diese befinden sich in den unterschiedlichsten Stadien zwischen Konzepterstellung und lizensiertem Betrieb. Von den vielen Konzepten erscheint der SMR von NuScale hinsichtlich des Umfangs und der Qualität der frei zugänglichen anlagenspezifischen Unterlagen und des Fortschritts im Genehmigungsverfahren als ein geeignetes Referenzkonzept eines SMR. Die Anlagenbeschreibung, die bereits an anderer Stelle erfolgte /SCH 20/ und /SCH 21a/, ist nachfolgend kurz zusammengefasst. Die NuScale-Anlage besteht im Wesentlichen aus den Gebäuden und den Anlagenteilen entsprechend Abb. 3.1.

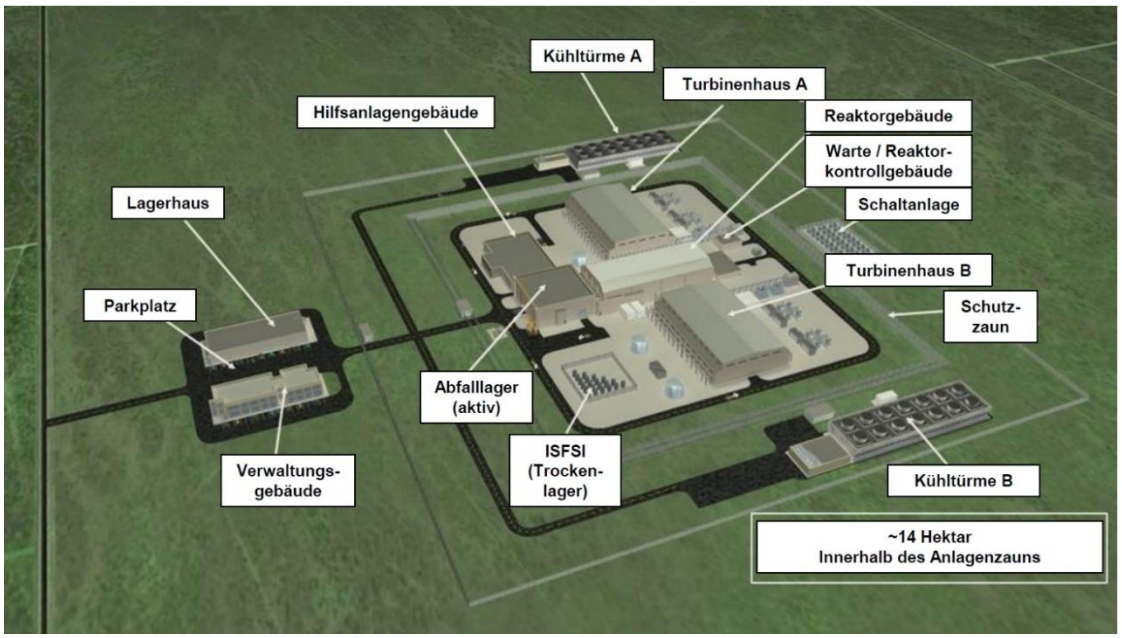


Abb. 3.1 Übersicht über ein Modul für den Anlagenstandort einer NuScale-Anlage

3.1 Anlagenkonzept und Reaktorgebäude

Das SMR-Konzept von NuScale besteht aus zwölf symmetrisch angeordneten, integralen DWR-Modulen, als NuScale Power Modules (NPM) bezeichnet, mit einer Leistung von 45 MW_e pro Modul. Als Grundlage wurde die Technologie herkömmlicher DWR verwendet und weiterentwickelt bzw. vereinfacht. Wesentliches Merkmal des Reaktorkonzepts sind die ausschließlich auf Naturumlauf basierenden Funktionsweisen des Energieübertragungsprozesses und der Sicherheitssysteme. Jedes Modul ist ein einfaches,

kompaktes System ohne jegliche aktiven Komponenten (z. B. Pumpen), das über jeweils eine Turbine, einen Kondensator, und einen Generator verfügt. Dadurch kann auch bei Ausfall eines Reaktormoduls oder bei Wartung/Brennelementwechsel die Gesamtanlage mit reduzierter Leistung weiterbetrieben werden. Ein Brennstoffzyklus beträgt etwa zwei Jahre, so dass bei einer Anlage mit zwölf Modulen alle zwei Monate bei einem Modul eine Revision vorgesehen ist. Der Brennelementwechsel findet in einem angrenzenden Bereich des Reaktorbeckens statt, die abgebrannten Brennelemente lagern in einem Lagerbecken, welches an das Reaktorbecken anschließt. Der Aufbau der Anlage und eine Übersicht des Reaktorgebäudes (100 m lang, 24 m breit und 23 m hoch) sind in den Abbildungen Abb. 3.2 und Abb. 3.3 dargestellt. Die Höhe des Reaktorbeckens beträgt 43 m mit einem Betriebsfüllstand von 21 m. Heiz- und Lüftungssysteme versorgen das Gebäude der Warte und das Reaktorgebäude mit dem Verbindungstunnel. Das Lüftungssystem ist in der Lage, freigesetzte Radionuklide in der Abluft des Reaktorgebäudes, des Abfalllagers und der Hilfsgebäude aus der Luft zu filtern.

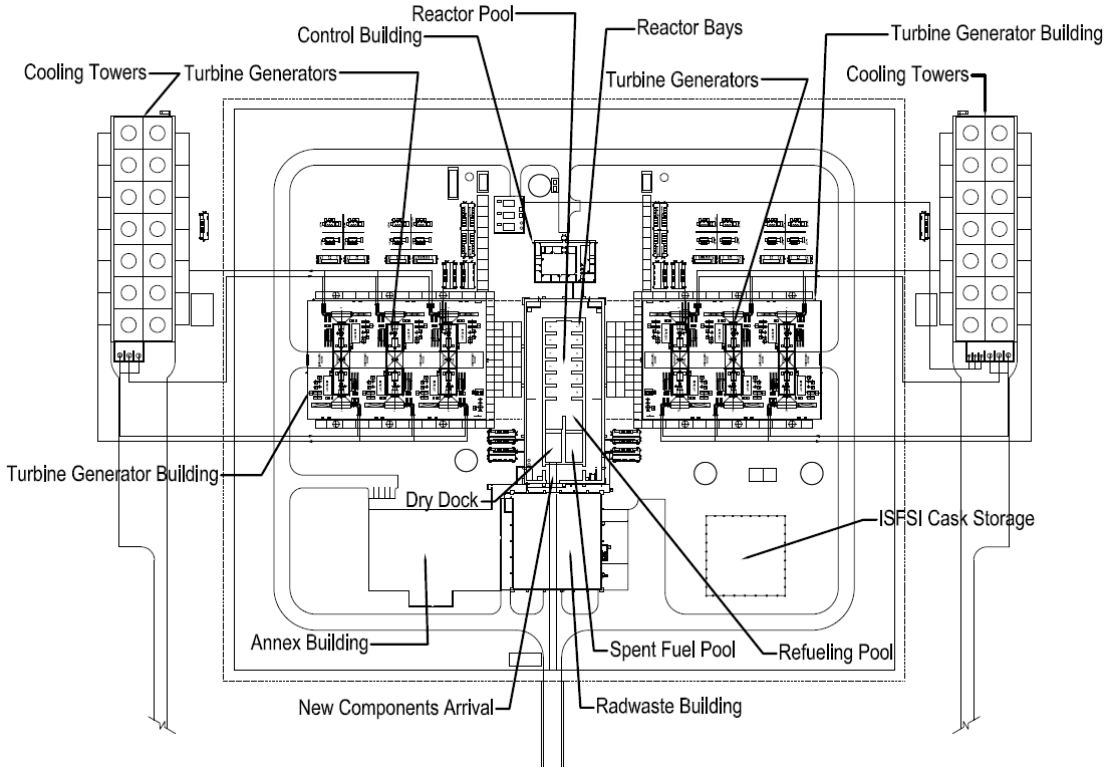


Abb. 3.2 Anlagenaufbau einer möglichen SMR-Anlage von NuScale mit zwölf Reaktormodulen /SCH 20/

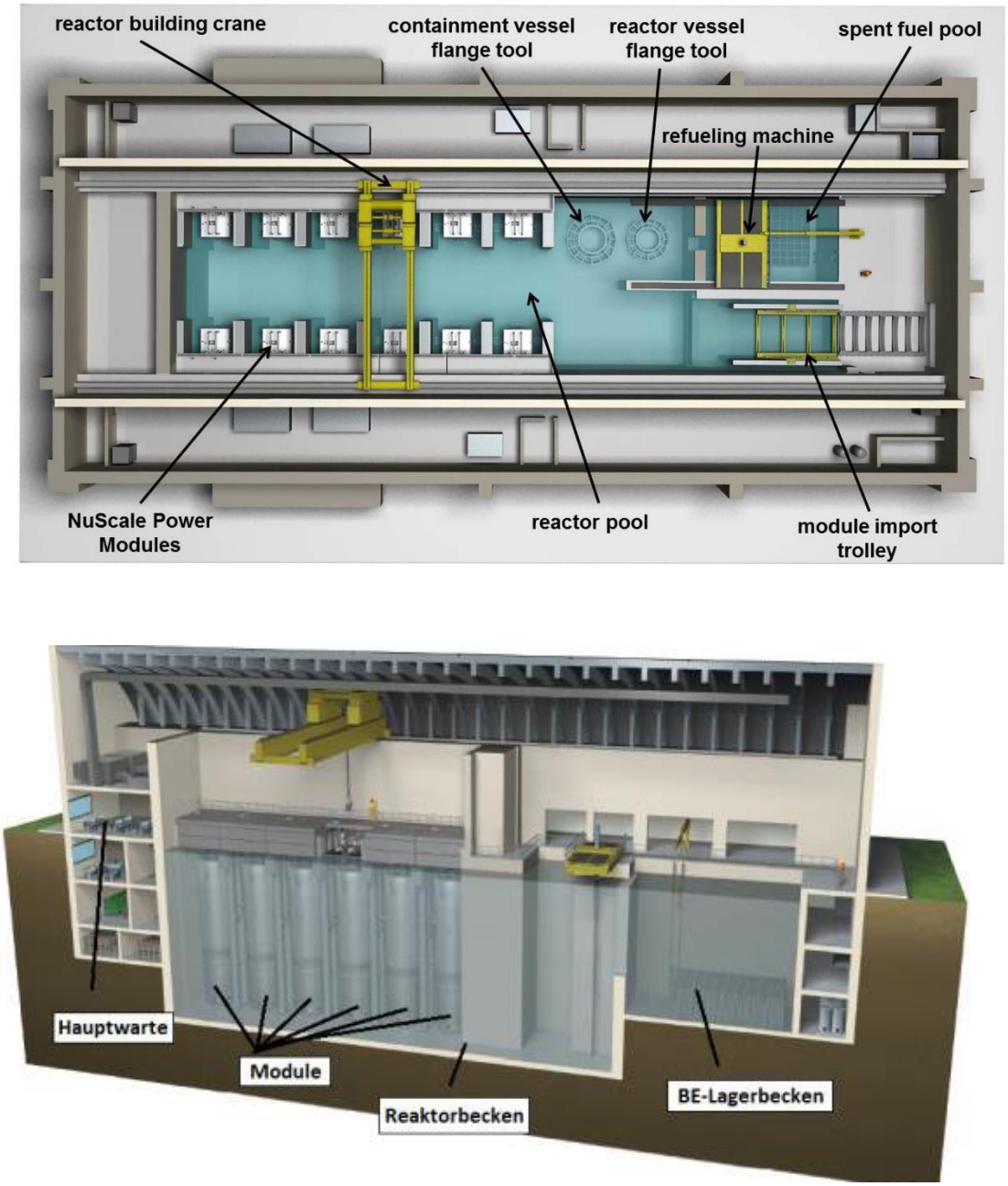


Abb. 3.3 Übersicht über das Reaktorgebäude /SCH 20/

Abgebrannte Brennelemente sollen für etwa fünf Jahre im Abklingbecken gelagert werden. Das Brennelementlagerbecken verfügt über eine ausreichend große Kapazität, um abgebrannte Brennelemente aus zehn Jahren Betrieb zu lagern. Auf dem Betriebsgelände soll sich darüber hinaus eine ausreichend große Lagerfläche befinden, um alle abgebrannten und abgeklungenen Brennelemente für einen Zeitraum von 60 Jahren trocken zu lagern.

3.2 Reaktormodul

Das Reaktormodul umfasst den Sicherheitsbehälter (SB) und das Reaktorkühlsystem (Englisch: reactor coolant system, RCS). Das RCS besteht aus dem RDB mit Kern und Steuerstäben, den Primärkühlkreislauf mit einem Druckpolster (Druckhalter) und zwei Dampferzeugern. Für einen Brennelementwechsel wird das Modul in ein spezielles Becken transportiert und auseinandergeschraubt. Der Aufbau eines Leistungsmoduls ist in Abb. 3.4 gezeigt.

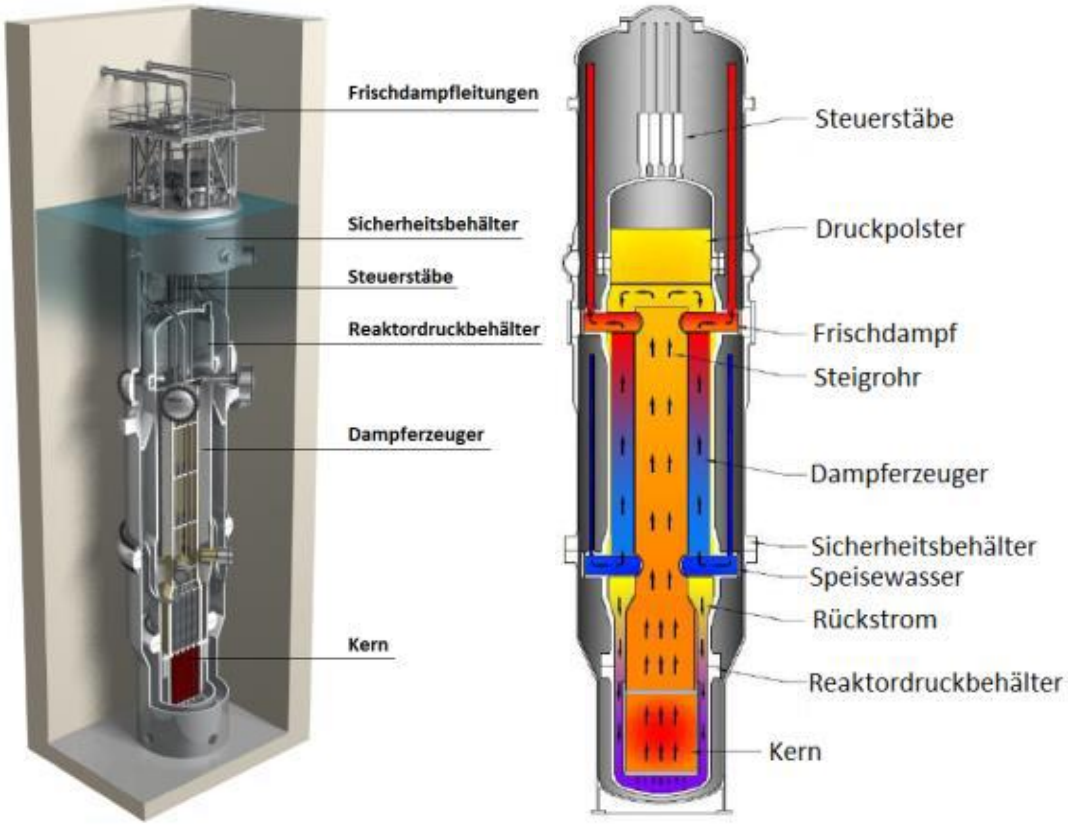


Abb. 3.4 Aufbau eines NuScale Leistungsmoduls /SCH 21a/ und Darstellung des Kühlmittelkreislaufs im RCS

3.2.1 RDB mit Kern

Der RDB besteht aus einem zylindrischen Stahlbehälter mit Innendurchmesser von ca. 3 m und ca. 18 m Höhe. Eine Außenansicht des RDB ist in Abb. 3.5 gezeigt. Der untere Teil des RDB kann abgelöst werden, um einen Zugang für den Brennelementwechsel zu schaffen. Im oberen Bereich befinden sich Steuerstabantrieb und -führungen, die Re-

aktorsicherheitsventile (RSVs), die Notkühl-Entlüftungsventile, der Druckhalter und die Dampferzeuger.

Der Kern besteht aus 37 Brennelementen in 17 x 17 Brennstabanordnung und 16 Steuerelementen. Die Länge der Brennelemente beträgt 2 m. Der Anreicherungsgrad des Brennstoffs beträgt weniger als 4,95 %. Die Leistung wird sowohl mit den Regelstäben als auch mit dem Anteil an Borsäure im Kühlmittel gesteuert. Von den 16 Steuerstäben dienen vier zur Leistungssteuerung und zwölf zum Abfahren bzw. zur Schnellabschaltung (RESA).

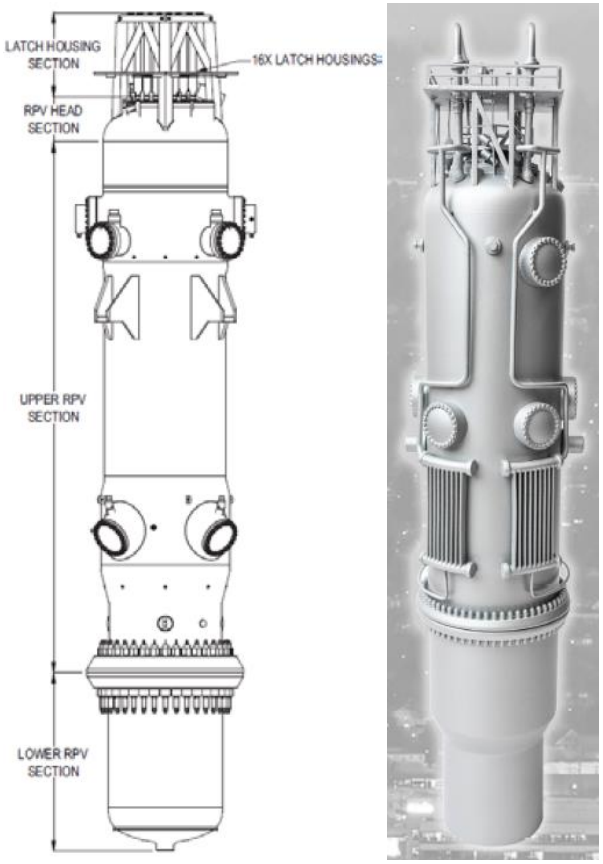
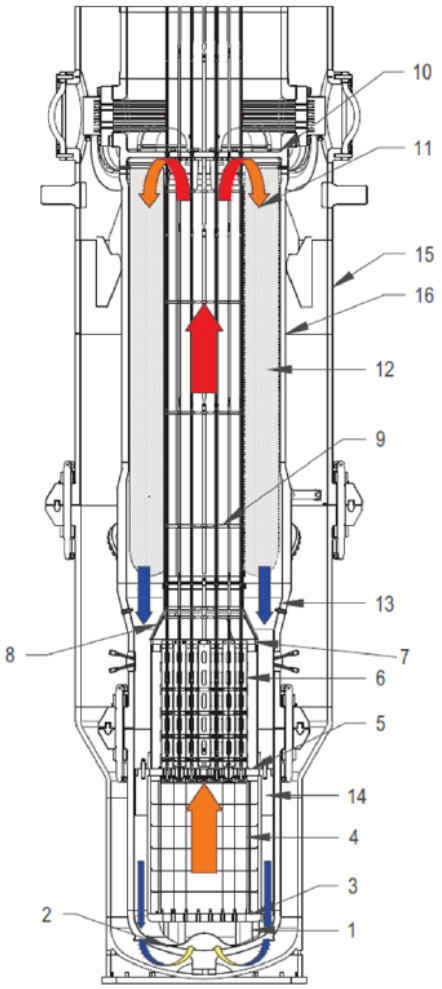


Abb. 3.5 Außenansicht eines NuScale RDB /SCH 20/

3.2.2 Reaktorkühlsystem

Der Primärkühlkreislauf im NuScale-SMR ist entsprechend dem Konzept der Naturumlaufkühlung entwickelt worden. Die Wärme der Kernreaktionen wird in jedem Umlauf von den Wärmetauschern aus dem Primärkühlkreislauf abgeführt. Der Naturumlauf basiert auf dem physikalischen Auftriebsprinzip, das kalte Kühlmittel wird von unten durch den Kern geleitet und erwärmt sich im Kern. Ein Umlauf durch den Primärkühlkreislauf ist

schematisch in Abb. 3.6 dargestellt. Die Dichte des Kühlmittels nimmt dabei ab und das Kühlmittel erfährt dadurch eine Auftriebskraft im Primärkühlkreislauf. Das Kühlmittel strömt nach Austritt aus dem Kern durch die Steigleitungen ins obere Plenum. Über einen ringförmigen Rückströmraum/Fallleitung strömt das erhitzte Kühlmittel aus dem oberen Plenum über die beiden konzentrisch um den Reaktor angeordneten Dampferzeugern mit 1380 verflochtenen und helikalen Röhren nach unten in den Rückströmraum. Die aus dem Kern zugeführte Wärme im Kühlmittel wird in den Wärmetauschern auf den sekundären Kühlkreislauf übertragen. Im Unterschied zu „üblichen“ DWR strömt im NuScale-SMR Speisewasser durch die Dampferzeuger-Röhren von unten nach oben. Außerdem ist der Systemdruck auf der Außenseite höher als auf der Innenseite. Jeder Dampferzeuger hat am Eingang zwei Speisewasser- und am Ausgang zwei Dampfsammler. Der um 30 °C überhitzte Dampf verlässt RDB und Sicherheitsbehälter in Richtung Turbine im Maschinenhaus.



#	Bauteil
1	Untere Kernstützblöcke in der Fallleitung
2	Umlenkung des kalten Strangs ins untere Plenum
3	Untere Kernplatte
4	Reaktorkern
5	Obere Kernplatte
6	Steuerelementführungsrohre
7	Stützplatte der Steuerelementführungsrohre
8	Übergangsbereich der Steigleitung
9	Unterstützung der Steuerstabführungsrohre
10	Druckhalter-Abtrennung
11	Umlenkung des heißen Strangs
12	Downcomer über die Dampferzeuger
13	Übergangsbereich der Fallleitung
14	Oberer Kernstützblock
15	Sicherheitsbehälter
16	Reaktordruckbehälter

Abb. 3.6 Schematische Darstellung der Strömungen im Primärkühlkreislauf /SCH 20/

Konzentrische, schraubenförmige Dampferzeuger

Die 1380 Rohre der NuScale-Dampferzeuger sind zu Rohrbündeln zusammengefasst. Diese Rohrbündel werden sekundärseitig durchströmt (entsprechend wird der Frischdampf innerhalb der Rohre erzeugt), was die Dampferzeuger beim NuScale-SMR von Dampferzeugern in herkömmlichen DWR unterscheidet. Der Vorteil dieser Bauweise ist das verminderte Risiko, dass ein möglicher Schaden an einem Rohr auch naheliegende Rohre beschädigt. Dies liegt im niedrigeren Druck des Sekundärkühlkreises begründet, ein Versagen einer Rohrleitung führt zu Quetschungen und nicht zu einem Bersten. Die Reserve für die Wärmeübertragungsfläche der Dampferzeuger fällt entsprechend bei NuScale-Modell geringer aus im Vergleich zu anderen Anlagen, d. h., wenn während der Nutzungsdauer der Anlage zu viele beschädigte Rohrleitungen verschlossen werden müssen, dann müssen die Wärmetauscher ersetzt oder die Leistung des Reaktors reduziert werden. Ein NuScale- Dampferzeuger ist in Abb. 3.7 gezeigt.

Abb. 3.7 Beide verflochtenen Dampferzeuger eines NuScale-Moduls; die heiße Steigleitung wird umschlossen /STU 17/

Druckhalter

Der Druckhalter befindet sich oberhalb des oberen Plenums und damit auch oberhalb der Dampferzeuger. Der Dampferzeuger wird thermisch durch die Druckhalter-Abtrennung (Baffle Plate) vom Primärkühlkreislauf getrennt und ist über acht Durchlässe mit Durchmessern von 10 cm hydraulisch mit dem Primärkühlkreislauf verbunden. Im Druckhalter gibt es eine Heizeinrichtung (Druckaufbau) und Sprühdüsen (Druckabsenkung), Wasser und Dampf bilden ein Gleichgewicht unter Sattdampfbedingungen. Die eingestellten Druckverhältnisse im Druckhalter werden dem Primärkühlkreislauf aufgeprägt. Das Volumen des Druckhalters beträgt 176 m³ und damit ungefähr 23 % des Gesamtvolumens des RCS. Die Füllstandsgrenzen liegen bei 80 % und 35 %. An den Druckhalter schließen beide Reaktorsicherheitsventile des Reaktorschutzes und alle drei Notkühl-Entlüftungsventile an.

3.2.3 Sekundärer Kühlkreislauf

Der Aufbau des sekundären Kühlkreislaufes ist schematisch in Abb. 3.8 dargestellt. Alle Komponenten des sekundären Kühlkreislaufes sind modulspezifisch vorhanden (u. a. Kühlturm, Generator und Kondensator), das heißt es gibt keine gemeinsame Nutzung einzelner Komponenten durch mehrere Module und keinen modulübergreifenden Kühlmittelaustausch. Der überhitzte Frischdampf aus beiden Dampferzeugern eines Moduls wird über eine Sammelleitung außerhalb des Sicherheitsbehälter zusammengeführt und über das Turbinenregelventil (Englisch: (turbine control valve) auf die Turbine geleitet. Alternativ kann der Frischdampf auch über die Frischdampf-Umleitstation direkt abgekühlt (auch unter Volllast) in den Kondensator gegeben werden. Ein Teil des überhitzten Frischdampfs dient der Vorwärmung des Speisewassers, auch Prozesswärme kann entnommen werden. Der entspannte Frischdampf aus der Turbine wird im Kondensator verflüssigt und aufbereitet. Danach wird das Kondensat in mehreren Stufen vorgewärmt und mit den Speisewasser-Pumpen zurück in die Dampferzeuger geleitet. Die Trennung der Frischdampf- und Speisewasserleitungen, die zu den beiden Dampferzeugern führen, erfolgt nach /NUS 20i/ außerhalb des Sicherheitsbehälters.

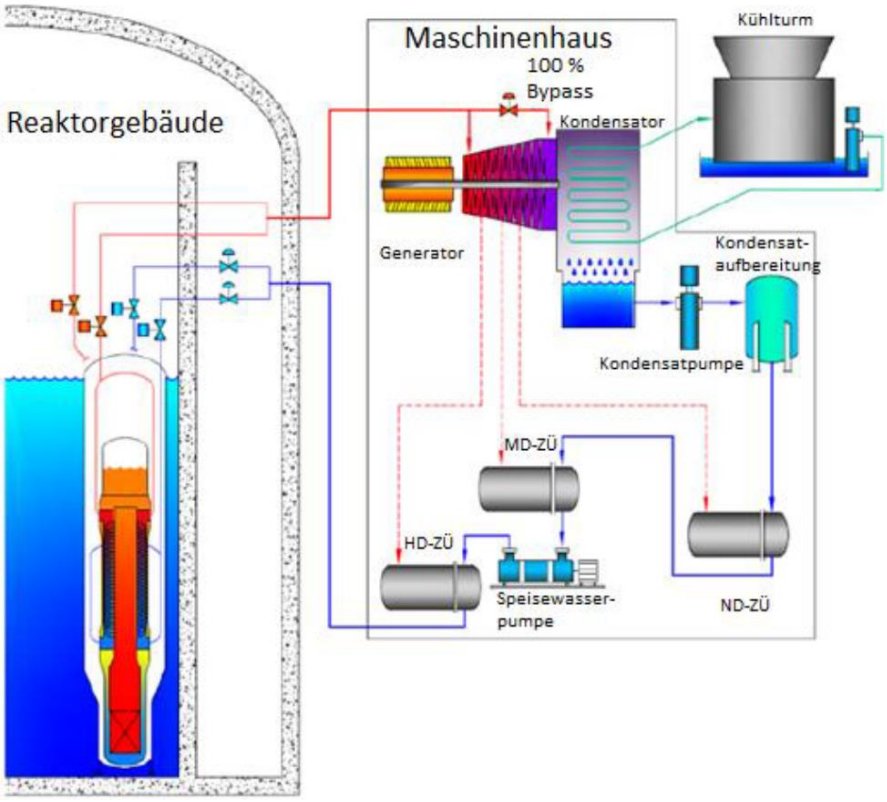


Abb. 3.8 Aufbau des sekundären Kühlkreislaufs /SCH 20/

3.2.4 Hilfs- und Sicherheitssysteme

Reaktorabschaltsystem (Reactor Trip System, RTS)

Das Reaktorabschaltsystem (Englisch: reactor trip system, RTS) ist in /NUS 20k/ beschrieben.

Der NuScale Reaktor besitzt 16 Steuerelemente zur Reaktivitätskontrolle, die in zwei Bänken, der Abschalt- und der Steuerbank, organisiert sind. Die Abschaltbank besteht aus acht im Kern symmetrisch verteilten Steuerelementen. Abschalt- und Steuerbank sind in je zwei Gruppen aus vier Elementen unterteilt. Jedes Steuerelement enthält 24 Kontrollstäbe aus Borcarbid (B_4C) und einer Silber-Indium-Cadmium-Legierung in den Spitzen. Die Bewegungssteuerung der Steuerelemente übernimmt das Steuerelementfahrsystem. Zusammen mit dem Steuerelementfahrsystem bilden die Abschaltstäbe das RTS. Eine RESA kann entweder aufgrund von Überschreitungen von Grenzwerten im Reaktor durch das RTS, durch die Betriebsmannschaft oder den Verlust der Stromversorgung herbeigeführt werden. Nach der Auslösung der RESA fallen die Abschaltstäbe gravitativ in den Kern ein und reduzieren die Reaktivität im Kern, um den Kern unterkritisch zu fahren und zu halten.

Volumenregelsystem (Chemical and Volume Control System, CVCS)

Das Volumenregelsystem (Englisch: chemical and volume control system, CVCS) ist kein Sicherheitssystem und wird bei Störfällen nicht benötigt. Während des Betriebs reinigt das System das RCS-Kühlmittel und sorgt für dessen korrekte chemische Zusammensetzung einschließlich der richtigen Borkonzentration. Der Druck im RCS wird u. a. vom Sprühsystem des CVCS geregelt. Ein niedriger Kühlmittelstand kann ggf. durch Einspeisen bzw. ein hoher Kühlmittelstand durch Entnahme von Kühlmittel und Abgabe an das nukleare Abwasseraufbereitungssystem (Liquid Radioactive Waste System) ausgeglichen werden. Beim Anfahren dient das CVCS durch zusätzliche Wärmezufuhr in das Kühlmittel als „Anschub“ für den Naturumlauf im Reaktor. Jedes Reaktormodul hat ein eigenes CVCS, das angeschlossene Boreinspeisesystem ist ein Einzelsystem, welches bis zu zwölf Module sowie das Lagerbecken mit boriertem Kühlmittel versorgt. Das CVCS benötigt für den Betrieb die Niederspannungs-Stromversorgung. Eine Übersicht über das System ist in Abb. 3.9 gezeigt. Wichtig für die Einspeisung bei einem schweren Störfall ist der Teil links unten mit der Aufbereitungsleitung und den zwei CVCS-

Aufbereitungspumpen (Englisch: makeup pumps). Die CVCS-Umlaufpumpen (English: recirculation pumps) werden für eine Einspeisung nicht benötigt.

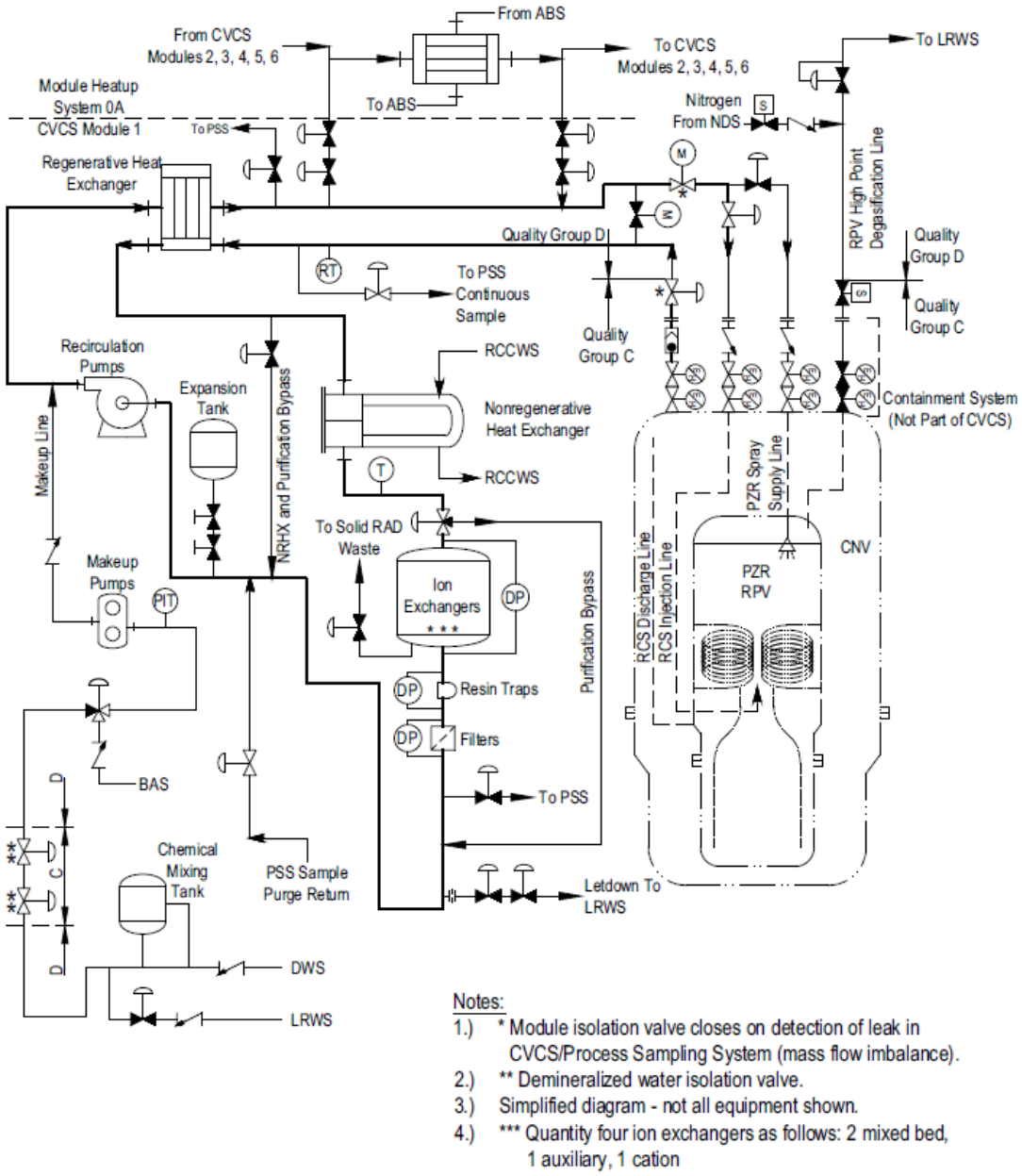


Abb. 3.9 Übersicht über das CVCS, aus /NUS 20d/

Das Kühlmittel zum CVCS wird aus dem Rückströmraum des Primärkühlkreislaufs entnommen. Diese CVCS-Entnahmeleitung durchdringt den RDB oberhalb des Kerns, wodurch verhindert wird, dass der RDB-Wasserspiegel im Fall eines Fehlers in der Durchdringung unter die Oberseite des Kerns abfließt. Das Kühlmittel kann zu einer Probenentnahme durch das Probenentnahmesystem teilweise umgeleitet werden und fließt dann zur Kühlung über den regenerativen Wärmetauscher.

Von dort wird das Kühlmittel weiter zum nicht-regenerativen Wärmetauscher gefördert, wo die Temperatur auf ein Niveau gesenkt wird, das mit den Filterharzen der Ionenaustauscher kompatibel ist. Nach dem Abkühlen im nicht-regenerativen Wärmetauscher wird das Kühlmittel zur Reinigung über die Ionenaustauscher und die Reaktorkühlmittelfilter geleitet. Nachdem das Kühlmittel den Reinigungszweig verlassen hat, kann es zur Probenentnahme teilweise umgeleitet, oder an das nukleare Abwassersystem zur Reduzierung des Kühlmittelfüllstandes oder zur Rückführung in den Primärkühlkreislauf an die CVCS-Umlaufpumpen abgegeben werden.

Nachzerfallswärmeabfuhrsystem (Decay Heat Removal System, DHRS)

Das Nachzerfallswärmeabfuhrsystem (Englisch: decay heat removal system, DHRS) ist ein Sicherheitssystem und zweifach redundant (2 x 100 %) für jedes Modul unabhängig aufgebaut. Es ist in /NUS 20c/ beschrieben und in Abb. 3.10. abgebildet Die Redundanzen sind geschlossene Kreisläufe und nicht vermascht. Jeweils einer der beiden Dampferzeuger ist an den Frischdampf-Leitungen angebunden und über Leitungen und durchflusslimitierenden Düsen mit einem passiven DHRS-Kondensator im Reaktorbecken verbunden. Die DHRS-Kondensatoren sind an gegenüberliegenden Positionen im Reaktorbecken. Die Leitung einer Redundanz ist im Leistungsbetrieb über zwei parallele DHRS-Auslöseventile (2 x 100 %) abgesperrt. Die Auslassleitung des DHRS-Kondensators führt zur Speisewasserleitung und damit in den Dampferzeuger zurück. Der Kühlmittelkreislauf ist in Abb. 3.11 gezeigt. Die Leitungen stehen auch im Leistungsbetrieb unter Druck, sind mit Kühlmittel gefüllt und ohne Absperrung direkt mit der Speisewasserleitung verbunden. Die Nachzerfallswärmeabfuhr erfolgt auch unter Druck ohne vorangehende Druckentlastung der Wärmetauscher. Im Betrieb ergibt sich der Kühlmitteldurchsatz durch das DHRS über einen Naturumlauf. Die passiven DHRS-Kondensatoren liegen aus diesem Grund höher als die Dampferzeuger – der Förderdruck für das Speisewasser ergibt sich aus dem Höhenunterschied zwischen dem DHRS-Kondensatorboden und dem niedriger liegenden Dampferzeuger-Einlass. Für die Wärmeabfuhr ist das Reaktorbecken als Not- und Nachwärmesenke (Englisch: ultimate heat sink, UHS) notwendig. Das Reaktorbecken, die automatische Auslösung beider DHRS-Redundanzen über die DHRS-Auslöseventile bei Stromausfall und die Vermaschung des Sekundärkühlkreises im Leistungsbetrieb stellen damit die einzigen Überschneidungen zwischen den Redundanzen dar, die Einfluss auf die Funktionalität des Systems haben können.

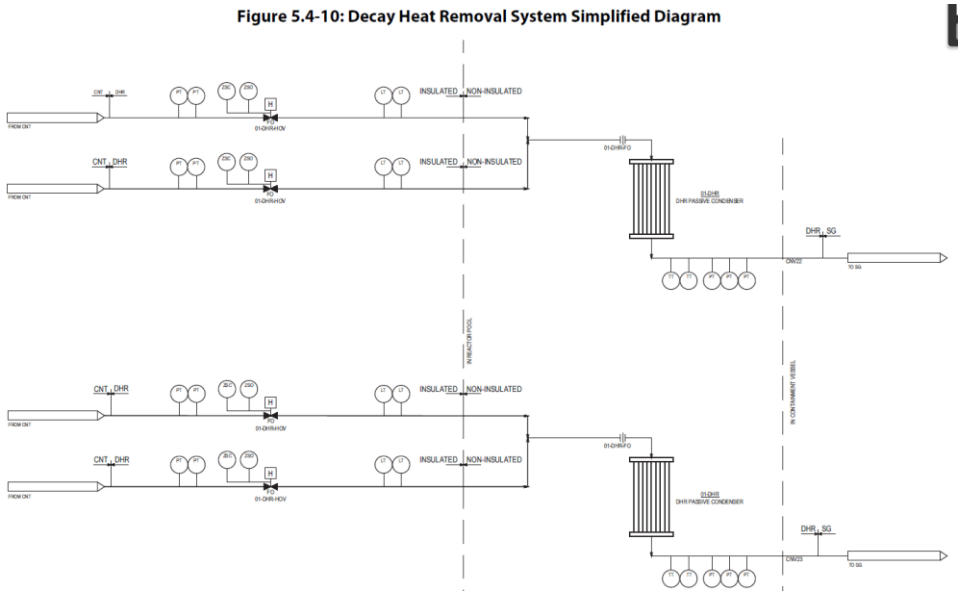


Abb. 3.10 Aufbau des DHRS /NUS 20c/

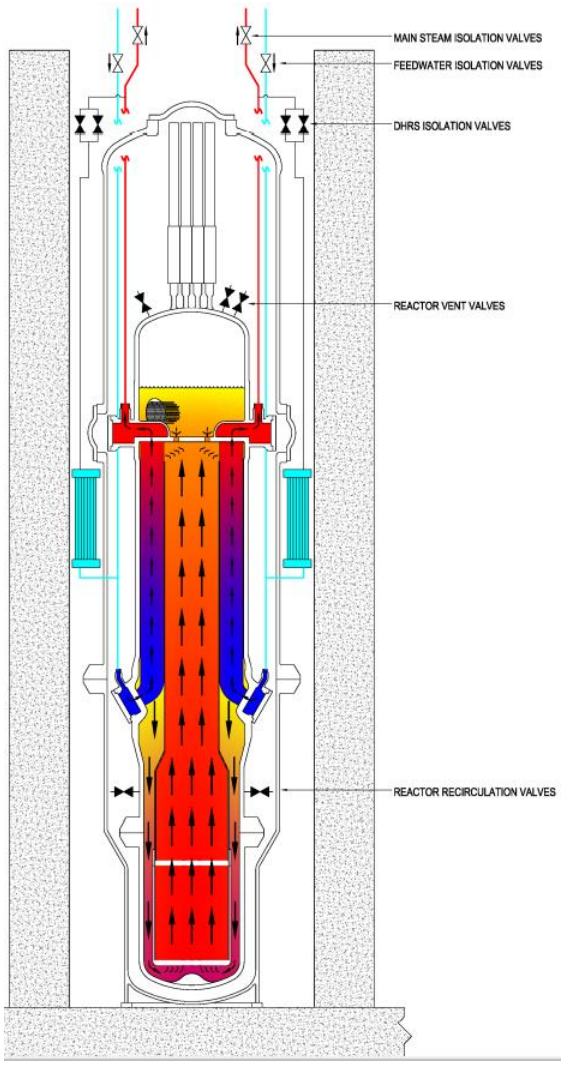


Abb. 3.11 Strömungspfade im Primärkühlkreislauf und DHRS /NUS 20h/

Jede Redundanz des DHRS ist für eine vollständige Nachzerfallswärmeabfuhr des Kerns ausgelegt und überführt das Modul in einen sicheren und druckentlasteten Zustand. Ein Ansprechen der Reaktorsicherheitsventile kann durch eine Wärmeabfuhr über beide Redundanzen des DHRS in der Regel vermieden werden. Das System benötigt keine Stromversorgung und besteht aus

- zwei parallelen Auslöseventilen, die sich im Bereich des Sicherheitsbehälter befinden,
- einer durchflusslimitierenden Düse,
- einem passiven DHRS-Kondensator im Reaktorbecken,
- zwei- bis dreifach redundanten Instrumentierungen zur Druck-, Temperatur- und Ventilstellungsmessung.

Das DHRS kann automatisch durch das System zur automatischen Auslösung von Sicherheitsfunktionen (Englisch; engineered safety features actuation system, ESFAS) als Teil des Reaktorschutzsystems oder durch manuelle Betätigung aus der Warte oder lokal an Schaltschränken des ESFAS aktiviert werden. Nach Aktivierung des DHRS öffnen die Auslöseventile vollständig innerhalb von 30 Sekunden über den pneumatischen Druck im Stickstoff-Zylinder (Die Auslöseventile schließen wieder innerhalb von 30 Sekunden, wenn der Differenzdruck zwischen Speisewasser-System und Frischdampf-System unter 3.4 bar fällt). Darüber hinaus öffnen die Auslöseventile bei einem Ausfall mehrerer Busse des hoch-zuverlässigen und unterbrechungsfreien Gleichstromnetzes (Englisch. highly reliable DC power system, EDSS). Das DHRS ist bis zu einem Maximalinnendruck von 145 bar und einer Maximaltemperatur von 343 °C ausgelegt. Dies entspricht den Werten aus dem RCS bis zum Ansprechen der RSVs und beinhaltet damit den Schutz der Integrität bei Auslaufen von RCS-Kühlmittel nach einem Dampferzeuger-Bypassleck. Die volle Funktionalität der Auslöseventile wird bei jedem geschützten Abfahrbetrieb der Anlage (Mode 3 entsprechend Abschnitt 6.1) geprüft. Folgende Größen im DHRS werden mit Sensoren überwacht:

- der Frischdampfdruck über acht sicherheitsrelevante Drucksensoren,
- die Position der Auslöseventile (zwei mögliche Zustände, auf oder zu),
- die Kondensattemperatur,

- der Kondensatdruck und
- der Druck im Stickstoff-Zylinder zur Öffnung der Auslöseventile.

Dampferzeuger-Abschlusssystem

Das Dampferzeuger-Abschlusssystem ist entsprechend /NUS 20e/ Teil des Sicherheitsbehälter-Abschlusssystems. Kommt es zu einem Dampferzeuger-Abschluss, so werden die Speisewasserleitung und die Frischdampf-Leitung abgesperrt und der Kühlkreis für das DHRS geöffnet. Der Dampferzeuger-Abschluss kann automatisch über die Anforderung zum Sicherheitsbehälter-Abschluss erfolgen oder manuell aus der Warte, wo auch eine Stellungsüberwachung möglich ist. Darüber hinaus schließen die Ventile des Dampferzeuger-Abschlusssystems automatisch bei Stromausfall oder bei Verlusten der Hydraulikflüssigkeit in der Steuerleitung. Das Dampferzeuger-Abschlusssystem besteht aus dem Frischdampf-Absperrventil (Englisch: main steam isolation valve, MSIV) von ca. 30 cm Innendurchmesser, dem Bypass-MSIV (parallel zum MSIV) und dem Speisewasser-Absperrventil (Englisch: feedwater isolation valve, FWIV) mit ca. 13 cm Innendurchmesse). MSIV und FWIV sind im Normalbetrieb geöffnet, das Bypass-MSIV ist im Normalbetrieb geschlossen und wird im Anfahrvorgang der Anlage verwendet.

Alle Dampferzeuger-Abschlussventile sind Kugelventile mit austauschbaren Dichtungen. Das MSIV ist ungefähr 30 cm vom Sicherheitsbehälter entfernt. Das Speisewasserabschluss- und das Speisewasserregelventil sind direkt an das Sicherheitsbehälter angeschweißt. Das Speisewasserregelventil schließt im Fall eines Speisewasserlecks außerhalb des Sicherheitsbehälter in weniger als einer Sekunde und damit deutlich schneller als das FWIV. Diese Steuerung verhindert einen größeren Kühlmittelverlust des Sekundärkühlkreises, welcher die Verfügbarkeit des Dampferzeugers für die Nachzerfallswärmeabfuhr gefährden könnte. Das Kühlmittel zwischen dem Speisewasserregelventil und dem FWIV kann sich nach Abschluss der Ventile aufheizen und der entstehende Druck wird passiv über einen kleinen Anschluss im Speisewasser-Regelventil abgelassen. Die Funktion der Druckentlastung bei geschlossenem Ventil wird regelmäßig geprüft.

Die Steuerung der Ventile (ähnliches gilt für die Auslöseventile des DHRS mit Öffnung und Schließung vertauscht) erfolgt hydraulisch über Stellglieder. Die Öffnung erfolgt dabei über einen hydraulischen Zylinder und die Schließung über einen mit Stickstoff gefüllten, passiven pneumatischen Stickstoff-Zylinder (der Druck im Zylinder wird gemes-

sen, Messwerte und mögliche Alarmierungen werden an die Warte übergeben). Jedes Dampferzeugerabschlussventil hat hierfür eigene unabhängig aufgebaute Steuerleitungen. Für den Schließvorgang wird dabei die hydraulische Flüssigkeit über zwei sicherheitsrelevante parallele Magnetsteuerventile abgelassen (die Steuerventile und Steuerleitungen sind in unterschiedlichen Bereichen des Reaktorgebäudes untergebracht).

Die Steuerventile öffnen bei Stromausfall automatisch über den stromlos werdenden Haltemagneten. Die Dampferzeuger-Abschlussventile sind so aufgebaut, dass sich diese bei anliegendem pneumatischen Zylinderdruck nicht öffnen lassen. Einzig über den hydraulischen Zylinder kann nach dem Schließen der Steuerventile das Dampferzeuger-Abschlussventil wieder geöffnet werden. Die Ventile des Sicherheitsbehälter-Abschlusssystems können nur einzeln nacheinander von der Betriebsmannschaft geöffnet werden. Die Signale der Stellungsüberwachung der Dampferzeuger-Abschlussventile werden über zwei unabhängige Instrumentierungseinheiten des Reaktorschutzsystems verarbeitet. Die automatische Auslösung des Sicherheitsbehälter-Abschlusses basiert auf zwei unabhängigen Redundanzen des ESFAS. Wenn für eine Messgröße zwei von vier Sensoren (‘2oo4‘) aus einer Redundanz des ESFAS das Auslösekriterium für den Sicherheitsbehälter-Abschluss erfüllen, so wird der Sicherheitsbehälter-Abschluss initiiert. Die Redundanz des ESFAS und des übergeordneten Reaktorschutzsystems sind diversitär aufgebaut und steuern jeweils eines der beiden Steuerventile der Dampferzeuger-Abschlussventile an. Die volle Funktionalität der Dampferzeuger-Abschlussventile (sowie der DHRS-Auslöseventile) wird bei jedem geschützten Abfahrbetrieb der Anlage (Mode 3 entsprechend Abschnitt 6.1) geprüft.

Notkühlsystem (Emergency Core Cooling System, ECCS)

Das Notkühlsystem (Englisch: emergency core cooling system, ECCS) ist ein Sicherheitssystem zur Abführung der Nachzerfallswärme des Kernes. Es besteht aus drei unabhängigen Abblaseventilen (RVVs), 3 x 50 % (Innendurchmesser 13 cm), am Druckhalter und aus zwei unabhängigen Rücklaufventilen (RRVs), 2 x 100 % (Innendurchmesser 5 cm), die etwas oberhalb der Kernzone (ca. 1,8 m) den Sicherheitsbehälter horizontal mit dem Rückströmraum des RDB verbinden und an gegenüberliegenden Seiten des RDB angebracht sind. Die RVVs befinden sich in der oberen Kalotte.

Zur Steuerung der Ventile werden hydraulische Steuerleitungen, Steuerungsventile, Öffnungsfedern und druckbelasteten Kontrollkammern verwendet. Das System ist in /NUS 20e/ beschrieben, der passive Strömungsumlauf ist in Abb. 3.13 gezeigt. Die Re-

dundanzen der RRV sind nicht vermascht, aber die drei RVVs teilen sich beide Redundanzen des ESFAS, wobei ein RVVs über beide Redundanzen aktiviert werden kann. Die anderen beiden RVVs können nur von jeweils einer Redundanz des ESFAS aktiviert werden. Weiter ist zu erwarten, dass die sich bildenden Naturumläufe durch die unterschiedlichen Ventile sich im Sicherheitsbehälter gegenseitig beeinflussen können.

Für die Funktion der Kernkühlung benötigt das ECCS die Wärmeübertragung des Sicherheitsbehälter an das Reaktorbecken, diese funktionell wichtige Eigenschaft ist nicht redundant verfügbar. Darüber hinaus muss genügend Kühlmittel im RCS und Sicherheitsbehälter für eine erfolgreiche Notkühlung zur Verfügung stehen, d. h. KMV mit Leck außerhalb des Sicherheitsbehälters können zum Ausfall des ECCS führen. Das Kühlmittelinventar des Leistungsbetriebes reicht für den erfolgreichen Betrieb des ECCS aus, eine Kühlmitteleinspeisung ist nur bei einem KMV vorzunehmen.

Das ECCS wird normalerweise[8] erst nach einer Teilbefüllung des Sicherheitsbehälters in Betrieb gesetzt, so dass die RRV bereits unterhalb des Wasserspiegels im Sicherheitsbehälter liegen. Dann erfolgt zunächst eine Druckentlastung des RCS. Der Dampf im RDB wird dabei über die RVVs mit eingebauten Zerstäubern in den Sicherheitsbehälter geleitet. Der Dampf kühlt an den Außenwänden des Sicherheitsbehälter (passive Kühlfunktion) ab und sammelt sich als Kondensat im unteren Bereich des Sicherheitsbehälter. Dann kann das Kondensat über die RRV zurück in den Rückströmraum des RDB strömen und gelangt von dort in den Kern, wo es verdampft und über die RVVs wieder in den Sicherheitsbehälter gelangt. Dadurch ergibt sich eine Naturumlauf-Zirkulationsströmung, wobei die Wärme über die Sicherheitsbehälter-Wand an das Reaktorbecken abgegeben wird.

Die Ventile arbeiten nach dem „fail-safe“-prinzip, das heißt, sie öffnen selbsttätig bei Ausfall der Energieversorgung nach Unterschreiten eines Ansprechdruckes im RDB bzw. bei Überschreiten eines Füllstandsgrenzwerts im Sicherheitsbehälter. Bis zur Aktivierung des ECCS hat sich der Sicherheitsbehälter über die RSVs oder über ein Leck in den Sicherheitsbehälter (bei einem entsprechenden auslösenden Ereignis) teilweise gefüllt.

[8] Eine Ausnahme kann sich bei einem länger andauernden Stromausfall über mehr als 24 h ergeben.

Alternativ kann durch das Betriebspersonal ein Fluten des Sicherheitsbehälter über das CFDS veranlasst werden, um den Sicherheitsbehälter aufzufüllen. Das ECCS sorgt im Notfall für die ausreichende Abfuhr der Nachzerfallswärme und dafür, dass der Kern mit Kühlmittel überdeckt ist. Eine Auslösung des ECCS ist auch manuell aus der Reaktorwarte möglich oder automatisch nach Transienten mit einer schnellen Druckangleichung zwischen RCS und Sicherheitsbehälter. In der Reaktorwarte sind die Ventilstellungsmeldungen und der Status der Steuerventil-Haltemagnete verfügbar. Darüber hinaus werden Kerneingangs- und Kernausgangstemperaturen gemessen. Die Kühlleistung des ECCS reicht aus, um den Druck im Sicherheitsbehälter nach einer RESA innerhalb von 24 h auf die Hälfte zu reduzieren.

Die Aktivierung des ECCS erfolgt über Federkraft nach dem Stromlosschalten (oder einem Ausfall mehrerer EDSS-Busse) der Auslösesteuerventile zur Entlüftung der Kontrollkammern, deren Inhalt sich in den Sicherheitsbehälter entleert. Jeweils ein RRV und ein RVV werden gemeinsam durch eine der beiden Redundanzen des ESFAS angesteuert. Das dritte RVV besitzt alle auslöserelevanten Komponenten doppelt und kann dadurch über beide ESFAS-Redundanzen aktiviert werden.

Die Steuerung der Ventile erfolgt automatisch durch das ESFAS, wenn die Auslösekriterien (siehe Abschnitt 7.1) erfüllt sind, hierfür stehen pro Messgröße jeweils vier Sensoren zur Verfügung, die Schaltung erfolgt aus bei Ansprechen zweier Sensoren (2oo4). Die ECCS-Ventile öffnen nach Aktivierung innerhalb von 10 Sekunden. Eine alternative Möglichkeit der ECCS-Ventilöffnung besteht nach einem schnellen Druckabfall im RCS (z. B. bei einem KMV), die ECCS-Ventile öffnen ohne Auslösung, wenn der Druckunterschied zwischen beiden Seiten des Ventils (Sicherheitsbehälter und RCS) sehr klein ist (passive Öffnungsfunktion, welche unabhängig von der hydraulischen Ventilsteuerung funktioniert und eine zusätzliche Sicherheit gegen einen Systemausfall bietet).

Die Deaktivierung des ECCS erfolgt über Rücksetzsteuerventile mit Kühlmittel aus dem CVCS oder RCS, welches gegen die Federkraft der Öffnungsfeder wirkt. Für die Deaktivierung muss der Rücksetzsteuerventil-Haltemagnet unter Strom gesetzt werden. Durch die Öffnung der Rücksetzsteuerventil wird Kühlmittel in die Kontrollkammern eingelassen, bei genügend hohem Druck schließen die Rücksetzsteuerventile durch das Stromlosschalten der Steuerventil-Haltemagnete.

Neben den Aktivierungs- und Deaktivierungsmöglichkeiten zur Schaltung der ECCS-Ventile verfügt das ECCS auch über einen Schutz vor unbeabsichtigter Aktivierung

(Englisch: inadvertent actuation block, IAB). Das Prinzip des Steuerungssystems eines ECCS-Ventils ist schematisch in Abb. 3.12 gezeigt. Der IAB wird für Differenzdrücke über 90 bar zwischen RDB und Sicherheitsbehälter aktiv, beispielsweise im Leistungsbetrieb mit evakuiertem Sicherheitsbehälter. Das Schutzventil verhindert dabei die Entlüftung der Kontrollkammern, welche ansonsten die ECCS-Ventilöffnung herbeiführen würden. In diesem Fall verhindert eine Feder die Öffnung des Entlüftungspfades der Kontrollkammern und damit die Öffnung der ECCS-Ventile.

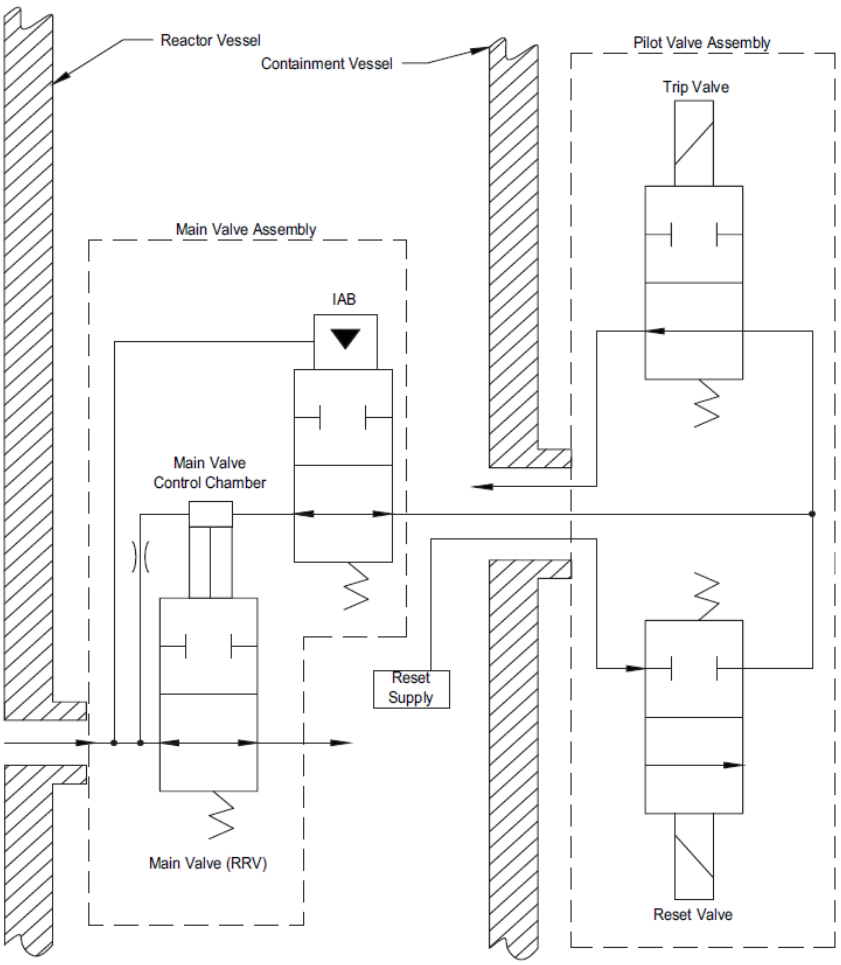


Abb. 3.12 Steuerungssystem eines ECCS-Ventils /NUS 20e/

Ist der IAB aktiv, so muss die Druckdifferenz zwischen RDB und Sicherheitsbehälter wieder auf ungefähr unter 65 bar fallen (typischerweise nimmt der Druck im RCS ab und der Sicherheitsbehälter füllt sich bei steigendem Druck mit Kühlmittel aus dem RCS, das über die RSVs abgegeben wird), damit die Sperre bzw. der Schutz sich automatisch aufhebt und die ECCS-Ventile öffnen.

Das ECCS wird im Fall eines kompletten Stromausfalls, der zu einer niedrigen Ladespannung der Gleichstrombatterien führt, nach 24 h automatisch aktiviert, um im weiteren Verlauf einer Stromausfalltransiente die Energieverluste an den Haltemagneten der ECCS-Ventile einzusparen.

Die Funktionalität aller ECCS-Ventile wird bei jedem geschützten Abfahrbetrieb der Anlage (Mode 3 entsprechend Abschnitt 6.1) geprüft. Die Funktionsprüfung findet dabei nicht unter Auslegungsbedingungen statt, da dies nur mit einem entsprechenden Differenzdruck zwischen RDB und Sicherheitsbehälter möglich wäre und die Hauptventilsteuerkammer zum Sicherheitsbehälter entlüftet werden müsste. Die Tests werden deshalb unter kälteren Bedingungen als im Anforderungsfall und bei einem niedrigeren Differenzdruck durchgeführt.

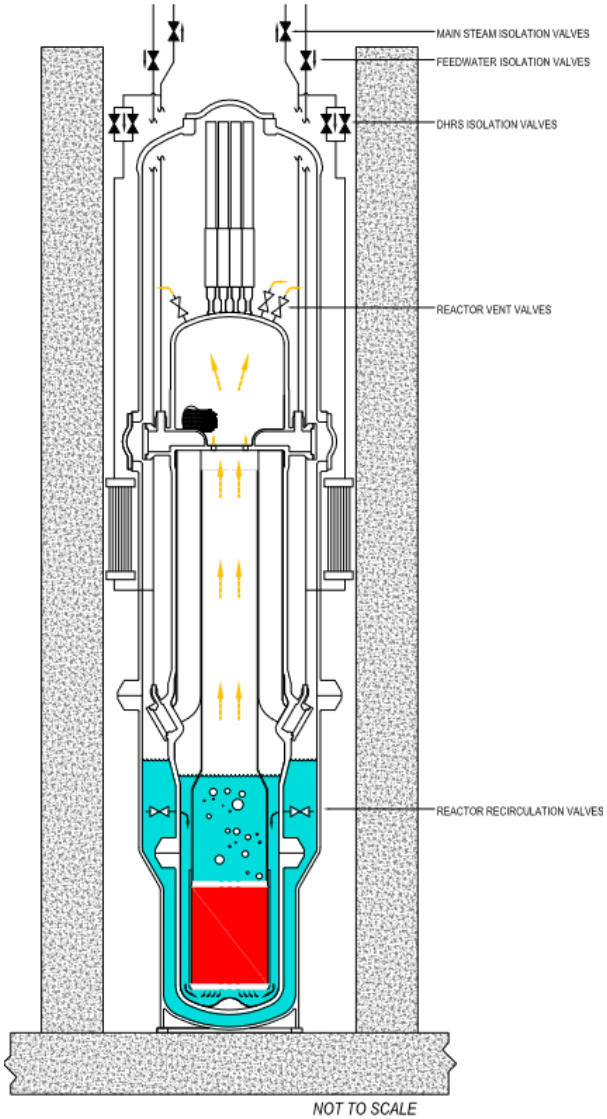


Abb. 3.13 Strömungsdarstellung des ECCS /NUS 20h/

Flut- und Drainagesystem des Sicherheitsbehälters (CFDS)

Das Flut- und Drainagesystem des Sicherheitsbehälters (CFDS) ist kein Sicherheitssystem und dient dem Fluten oder der Drainage des Sicherheitsbehälter während eines Brennelementwechsels oder während eines schweren Störfalls. Es ist in /NUS 20d/ beschrieben und in Abb. 3.14 dargestellt.

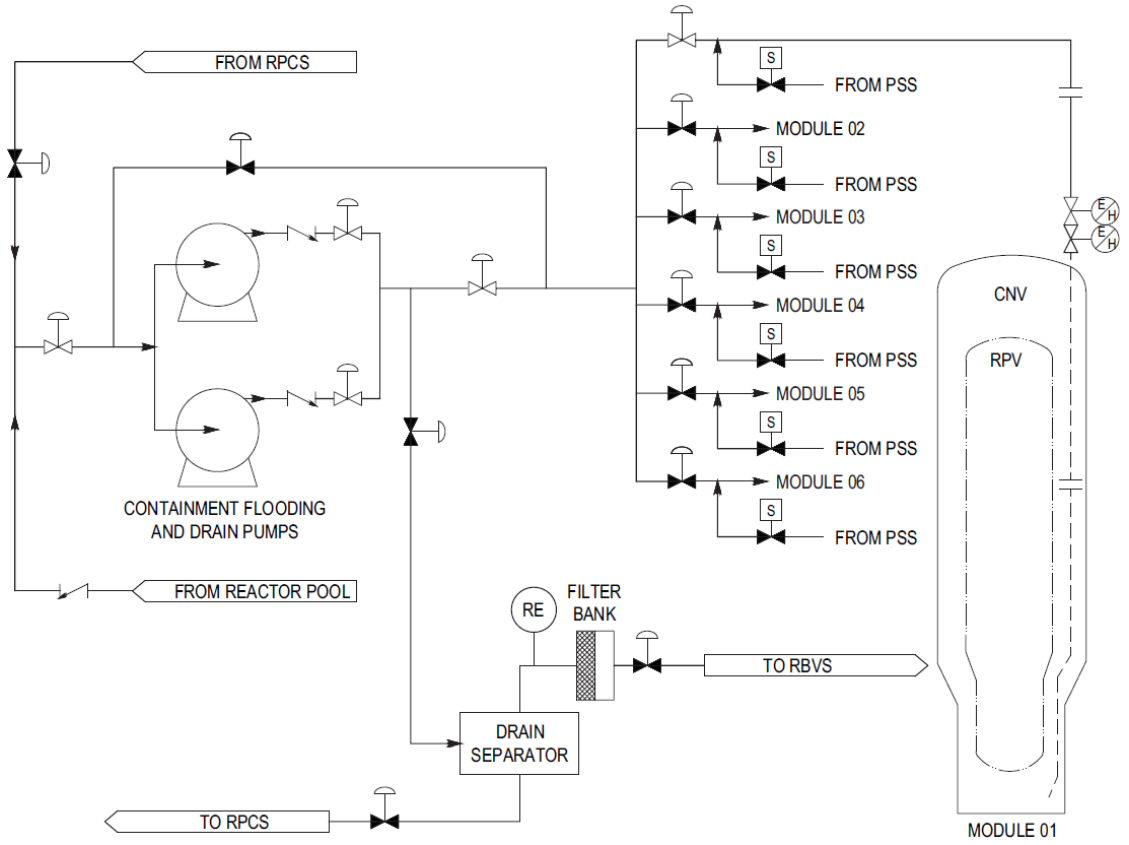


Abb. 3.14 CFDS /NUS 20d/

Im Sicherheitsbehälter herrscht im Leistungsbetrieb ein Vakuum, um die Konvektionswärmeverluste für den Primärkühlkreislauf gering zu halten. Vor dem Brennelementwechsel wird der Sicherheitsbehälter über das CFDS mit boriertem Reaktorbeckenwasser (entweder direkt aus dem Reaktorbecken oder aus dem Beckenkühlsystem) gefüllt. In der Anfahrphase nach einem Brennelementwechsel wird das Kühlmittel aus dem Sicherheitsbehälter über das Drainagesystem abgepumpt, im Anschluss wird der Sicherheitsbehälter mit dem Sicherheitsbehälter-Drainagesystem vakuumiert. Zur Unterstützung des Drainagesystem beaufschlagt das System den Sicherheitsbehälter mit einem Druck durch Einblasen von Luft. Darüber hinaus kann Beckenkühlmittel über das CFDS

im Laufe eines schweren Störfalls in den Sicherheitsbehälter eingespeist werden, solange der Druck im Sicherheitsbehälter nicht zu hoch ist.

Für die gesamte Anlage stehen zwei CFDS zur Verfügung. Jedes System besitzt zwei CFDS-Pumpen (2 x 100 %) und versorgt bis zu sechs Module, allerdings können die Module nur nacheinander und nicht gleichzeitig versorgt werden. Ist das System in Betrieb, so muss für die Umschaltung auf ein anderes Modul die CFDS-Pumpe gestoppt und das Abschlussventil des versorgten Moduls geschlossen werden, bevor das Abschlussventil eines anderen Moduls zur Versorgung geöffnet werden kann. Darüber hinaus muss das Sicherheitsbehälter-Absperrventil (Englisch: containment isolation valve, CIV) für die Anschlussleitung in den Sicherheitsbehälter geöffnet sein. Eine weitere Einschränkung ergibt sich für Temperaturen oberhalb von 177 °C im heißen Strang, in diesem Fall ist eine Versorgung des Moduls nur über eine zusätzliche Aktivierung einer speziellen Heizvorrichtung möglich.

Für das Fluten und die Drainage werden die gleichen Rohrverbindungen in den Sicherheitsbehälter verwendet. Flutungs- und Drainagevorgänge werden durch Füllstandsensoren im Sicherheitsbehälter, Messung der Durchflussraten, Drücke und Temperaturen im System überwacht. Außerdem werden Leckagen in den Sicherheitsbehälter detektiert, die einfließenden Kühlmittelmengen bestimmt und die Informationen an das Reaktorschutzsystem weitergegeben. Die CFDS-Pumpen sind Kreiselpumpen und laufen mit Strom aus dem Niederspannungs-Wechselstromnetz (Englisch: low voltage AC electrical distribution system, ELVS).

3.2.5 Zuverlässigkeit der Naturumläufe im DHRS und im ECCS

NuScale untersucht und bewertet die Zuverlässigkeit der Naturumläufe im DHRS und im ECCS (siehe dazu /NUS 20/). Hierfür werden die thermohydraulischen Unsicherheiten quantifiziert und Ausfallmaßgrößen definiert. Für das Nachkühlsystem ergibt sich ein Ausfall bei Überschreitung der Hüllrohrtemperatur von 1200 °C. Das DHRS versagt, wenn der Druck im RCS den Auslegungsdruck von 174 bar übersteigt (das Öffnen von ECCS-Ventilen oder von RSVs wird in der Analyse unterdrückt). Die Zuverlässigkeitsuntersuchungen verwenden einzelne charakteristische Szenarien aus Szenariengruppen, wie KMV, in den Sicherheitsbehälter und generelle Transienten. Für das ECCS konnten folgende Parameter als wichtige Einflussgrößen auf die Zuverlässigkeit identifiziert werden:

- Nachzerfallsleistung (kleinerer Wert führt zu kürzerer Missionszeit),
- konvektiver Wärmeübergang zwischen Sicherheitsbehälter-Außenwand und Reaktorbecken (besserer Wärmeübergang senkt Druck im Sicherheitsbehälter und Füllstand im RDB),
- Kühlmittelinventar im RDB zu Beginn des Störfalls (niedriges Inventar reduziert den hydrostatischen Druck für den Kühlmittelrücklauf in den RDB),
- Menge an nicht-kondensierbaren Gasen im Sicherheitsbehälter und RDB (weniger nicht-kondensierbare Gase verbessern die Kondensationsrate im Sicherheitsbehälter),
- Druckverlustbeiwerte der ECCS-Ventile (höhere Druckverlustbeiwerte verringern den Füllstand im Sicherheitsbehälter und führen zu einem höheren Druck im RDB),
- Temperatur des Reaktorbeckens (niedrigere Temperaturen erhöhen den Wärmestrom aus dem Sicherheitsbehälter und verringern den Druck im Sicherheitsbehälter und den Füllstand im RDB).

Einen besonderen Einfluss auf das DHRS haben folgende Größen:

- Nachzerfallsleistung (kleinerer Wert führt zu kürzerer Missionszeit),
- konvektiver Wärmeübergang zwischen der Außenwand des DHRS-Kondensators und dem Reaktorbecken (ein geringerer Wärmeübergang führt zu höheren Drücken im RDB),
- konvektiver Wärmeübergang in den Dampferzeuger (ein geringerer Wärmeübergang führt zu höheren Drücken im RDB),
- Kühlmittelinventar im DHRS (ein erhöhtes Kühlmittelinventar reduziert die Kondensationsfläche im DHRS-Kondensator und reduziert damit den Wärmestrom),
- Menge an nicht-kondensierbaren Gasen im DHRS-Kondensator (die nicht-kondensierbaren Gase reduzieren die Kondensationsrate im DHRS-Kondensator),
- Verstopfung der Dampferzeuger (dadurch reduziert sich die Wärmeübergangsfläche in den Dampferzeuger).

Die Versagenswahrscheinlichkeiten der Systeme konnten aus den Analysen in /NUS 20/ übernommen werden:

- DHRS: 4 E-06 über die gesamte Missionszeit,
- ECCS: E-07 über die gesamte Missionszeit.

3.3 Elektrische Systeme und Stromversorgung

Es sind mehrere Stromversorgungssysteme in einer NuScale-Anlage im Einsatz. Das Hochspannungs-Wechselstromnetz mit acht Schienen bei 13,8 kV, die zugehörige Umschaltanlage (13.8 kV and switchyard system, EHVS) verbindet das Übertragungsnetz, den Generator und die Stromverteilungssysteme der Anlage und gilt auch als externe Stromversorgung. Eine externe Stromversorgung ist für die Beherrschung der Auslegungsstörfälle laut /NUS 20j/. nicht erforderlich Das Mittelspannungswechselstromnetz (EMVS) versorgt Systeme mit Mittelspannungslasten von 4,16 kV sowie die ELVS-Schienen. Es besteht aus acht Schienen für alle zwölf Reaktormodule.

Das ELVS besteht aus jeweils vier Schienen pro Modul. Diese vier Schienen werden von zwei EMVS-Schienen mit einer transformierten Wechselspannung von 480 V versorgt. Die ELVS-Schienen 1 und 3 werden von einer EMVS-Schiene und die ELVS-Schienen 2 und 4 von einer anderen EMVS-Schiene versorgt. Die ELVS-Schienen 1 und 2 sind über einen Dieselgenerator notstromgesichert und die Schienen 3 und 4 über den anderen Dieselgenerator. Das ELVS versorgt modulspezifische, aber auch modulunabhängige Verbraucher. Beispiele für modulspezifische Verbraucher sind die Speisewasser- und die Kondensatpumpen. Das normale Gleichspannungssystem (Englisch normal DC power system) ist ein Beispiel für einen modulunabhängigen Verbraucher. Es dient der Versorgung aller nicht sicherheitsrelevanten Verbraucher innerhalb der Steuer- und Regelsysteme. Außerdem versorgt das ELVS das EDSS mit einer transformierten und gleichgerichteten Spannung von 125 V.

Das EDSS teilt sich in einen gemeinsam von allen Modulen genutzten Teil und einen modulspezifischen Teil. Der modulspezifische Teil dient dem Modul als unterbrechungsfreie Stromversorgung und besteht aus vier unabhängigen Bussen. Die Busse A und D eines Moduls werden jeweils von den ELVS-Schienen 1 und 4 versorgt, die Busse B und C von den ELVS-Schienen 2 und 3. Jeder EDSS-Bus ist mit zwei Batterien notstromversorgt.

Das EDSS versorgt die Modulsteuersysteme (Reaktorschutzsystem und das ESFAS), Modulsicherungssysteme und weitere Verbraucher, die im Normalbetrieb oder nach ei-

ner RESA erforderlich sind. Der gemeinsam genutzte Teil des EDSS wird von den ELVS-Schienen der Module 6 und 7 versorgt und besteht aus zwei Bussen. Auch der gemeinsam genutzte Teil des EDSS ist über zwei Batterien pro Bus unterbrechungsfrei.

Neben den beiden bereits erwähnten Notstrom-Dieselgeneratoren mit Spannungen von 480 V zur Versorgung der ELVS-Schienen steht auch ein Hilfsgenerator (z. B. ein Gasturbinengenerator) mit einer Spannung von 13,8 kV zur Versorgung des EHVS zur Verfügung. Der Hilfsgenerator und die Dieselgeneratoren sind keine Sicherheitssysteme und werden zur Beherrschung der Auslegungsstörfälle nicht benötigt. Mit den Notstrom-Dieselgeneratoren können die Notstrom-Batterien des EDSS geladen und ausgewählte Systeme im Notfall unterbrechungsfrei betrieben werden. Dieselgeneratoren und der Hilfsgenerator starten automatisch 30 Sekunden nach einem anhaltenden Ausfall des EHVS und werden nach erfolgtem Start manuell mit dem Verbrauchersystem verbunden. Die Notstromversorgung wird in regelmäßigen Abständen auf deren Startfähigkeit und deren Funktion unter Last getestet.

3.4 Vergleich zu konventionellen Druckwasserreaktoren

Im Vergleich zu konventionellen Druckwasserreaktoren entsprechend Tab. 3.1 zeigen sich einige Gemeinsamkeiten, wie die Form der Brennelemente und Brennstäbe, einige Skalierungen auf ca. 3 %, wie die der thermischen Leistung und der Durchflussraten, ein etwas niedrigerer Systemdruck und eine entsprechend niedrigere Kühlmitteltemperatur. Der Naturumlauf im RCS arbeitet dabei mit einer höheren Aufwärmspanne über den Kern von 56 K gegenüber 35 K beim US-amerikanischen EPR.

Auch in den Anlagenkenngrößen in Tab. 3.2 zeigen sich im Vergleich zu herkömmlichen DWR teilweise Skalierungsgrößen, wie die elektrische Leistung und die Anzahl der Brennelemente. Einige Systemkomponenten wie die meisten Pumpen oder Rohrleitungen, sind im Konzept von NuScale nicht vorgesehen. Darüber hinaus sind die Abmessungen für den RDB und den Sicherheitsbehälter deutlich kleiner.

Tab. 3.1 Vergleich der NuScale Reaktorkenndaten mit Daten für den US-EPR und den US-APWR, aus /NUS 20k/

Parameter	NuScale	US-EPR	US-APWR
Key Reactor Parameter			
Core thermal output (MWt)	160	4590	4451
System pressure (psia)	1850	2250	2250
Number of loops	NA	4	4
Inlet temperature (°F) [best estimate (BE) flow]	497	563.4	550.6
Core average temperature (°F) (BE flow)	543	596.8	588.8
Average temperature rise in core (°F) (BE flow)	100	62.7	72.1
Minimum design flow (lb/hr)	4.27E+6	173E+6	168E+6
Maximum design flow (lb/hr)	5.24E+6	195E+6	188E+6
Best estimate flow (lb/hr)	4.66E+6	180E+6	175E+6
Core bypass flow (%)	8.5	5.5	9.0
Average linear power density (kW/ft)	2.5	5.22	4.65
Peak linear power for normal operating conditions (kW/ft)	5.0	13.6	12.1
Normal operation peak heat flux (10^6 Btu/hr-ft^2)	0.171	.460	0.421
Total heat flux hot channel factor (F_Q)	2.0	2.60	2.60
Heat transfer area on fuel surface (ft^2)	6,275	86,166	91,360
Normal operation core average heat flux (Btu/hr-ft^2)	85,044	177,036	162,000
Core flow area (ft^2)	9.79	63.6	68.0
Core average coolant mass velocity (10^6 lbm/hr-ft^2) (BE)	0.49	2.8	2.25
Core average coolant velocity (ft/sec)	2.7	16	14.1
Core			
Equivalent diameter of active core (in)	59.28	148.3	119.7
Number of fuel assemblies	37	241	257
Fuel Assembly			
Effective fuel length (in.)	95.89	165.4	165.4
Nominal fuel weight per assembly (lb)	550	1182	1350
Rods per fuel assembly	264	264	264
Fuel Assembly pitch (in.)	8.466	8.466	8.466
Fuel rod pitch (in.)	0.496	0.496	0.496
Number of grids per assembly	5	10	11
Fuel Rod			
Cladding outside diameter (in.)	0.374	0.374	0.374
Pellet-cladding gap (in.)	0.00325	0.0033	0.0033
Cladding material	M5®	M5®	ZIRLO
Fuel column length (in.)	78.74	160	165.4
Fuel pellet diameter (in.)	0.3195	0.3195	0.322
Fuel pellet density (% theoretical density)	96.0	96.0	97

Tab. 3.2 Vergleich einiger wichtiger Kenngrößen des NuScale SMR mit einem herkömmlichen DWR aus /NUS 20h/

NuScale Plant Parameter or Feature (per NPM)	Typical PWR	NuScale
Nominal gross electrical output (MWe)	1,186	50
Core thermal output (MWt)	3,411	160
Number of fuel assemblies	193	37
Fuel assembly lattice	-17x17	17x17
Effective fuel length (ft)	12	6.56
Fuel rods per fuel assembly	264	264
Average linear heat rate (kW/ft)	5.4	2.5
Number of Control Rod Assemblies	53	16
Design life (years)	40	60
Reactor Coolant System		
Number of heat transfer loops	4	No External Loops
Reactor Coolant Pipes (in.)	27.5-31	None
Operating pressure (psia)	2,250	1,850
Hot leg temperature (°F)	618	590
Reactor Vessel		
Vessel inner diameter (in.)	173	107.5
Thermal shielding- and reflector design	Neutron pad design	Stacked stainless steel reflector blocks
In-core instrumentation	Bottom mounted	Top mounted
Steam Generator		
Number	4	2
Type	Vertical U-tube	Helical coil
Heat transfer area (ft2)	55,000	Approximately 18,000
Number of tubes	5,626	1,380
Reactor Coolant Pumps	4	0
Pressurizer		
Internal volume (ft3)	1,800	568
Surge nozzle nominal diameter (in.)	14	None
Residual Heat Removal Pumps	2	None
Containment		
Type	PCCV	Steel Pressure Vessel
Inner diameter (ft-in.)	140-0	14-2
Height (ft-in.)	205-0 (inner)	75-8.5 (outer)
Containment Spray Pumps	2	None
High Pressure Safety Injection Pumps	2	None
Charging / Safety Injection Pumps	2	None
Low Pressure Safety Injection Pumps	2	None
Accumulators	4	None
I&C System type	Analog	Digital
Emergency Diesel Generators	2	None
Turbine Type	1800 rpm, Tandem Compound Six Flow	3,600 rpm, 10 stage with Superheat
Emergency Feedwater Pumps	3	None
Charging Pumps (CVCS pumps)	2	2
Used for Safety Injection	Yes	No
Volume Control Tank	1	0
Reactor Component Cooling Water Pumps	4	6 total for 12 NPMs

Viele Sicherheitssysteme und Komponenten eines herkömmlichen DWR sind im Konzept von NuScale nicht vorgesehen. Tab. 3.3 zeigt einen Vergleich der verwendeten Sicherheitssysteme und Komponenten. Insbesondere verzichtet das NuScale-Konzept auf zusätzliche Notstromdiesel, ein primärseitiges Noteinspeisesystem und ein sekundärseitiges Notspeisewassersystem.

Tab. 3.3 Vergleich der NuScale Sicherheitssysteme mit den Sicherheitssystemen in herkömmlichen DW, aus /NUS 20h/

Safety System or Component	Typical PWR	NuScale
Reactor Pressure Vessel	X	X
Containment Vessel	X	X
Reactor Coolant System	X	X
Decay Heat Removal System	X	X
Emergency Core Cooling System	X	X
Control Rod Drive System	X	X
Containment Isolation System	X	X
Ultimate Heat Sink	X	X
Residual Heat Removal System	X	
Safety Injection System	X	
Refueling Water Storage Tank	X	
Condensate Storage Tank	X	
Auxiliary Feedwater System	X	
Emergency Service Water System	X	
Hydrogen Recombiner or Ignition System	X	
Containment Spray System	X	
Reactor Coolant Pumps	X	
Safety-Related Electrical Distribution System	X	
Alternative Off-Site Power	X	
Emergency Diesel Generators	X	
Safety-Related Class 1E Battery System	X	
Anticipated Transient Without Scram (ATWS) System	X	

4 Umfang der PSA der Stufe 1 für einen SMR

Die PSA für einen SMR orientiert sich bisher in der Regel an den Standards für Leistungsreaktoren der dritten Generation[9]. Dies zeigt sich insbesondere in den entsprechenden Dokumenten von NuScale zur PSA im Rahmen der Auslegungsphase /NUS 20/, Kapitel 19. Größtes Problem bei der Erstellung der PSA ist die fehlende Betriebserfahrung ähnlicher Anlagen oder ähnlicher Systeme in bestehenden Anlagen. Die im Folgenden beschriebenen Arbeiten zur PSA für einen NuScale-Reaktor bzw. eine SMR-Anlage aus zwölf Reaktormodulen folgen im Vorgehen teilweise dem Vorgehen in der PSA von NuScale und orientieren sich größtenteils an einer PSA für Anlagen der 3. Generation. Ein Ablaufplan für die Erstellung der PSA der Stufe 1 ist in Abb. 4.1 gezeigt.

Die Analysen gliedern sich in die folgenden Abschnitte:

- Festlegung der Merkmale von Endzuständen (Kapitel 5): Die Endzustände des SMR werden untersucht mit Kriterien für Kernschäden oder Versagen der druckführenden Umschließung oder des Sicherheitsbehälter.
- Ermittlung eines Spektrums auslösender Ereignisse (Kapitel 6): Die Ermittlung relevanter auslösender Ereignisse für den SMR basiert auf bestehenden Listen, deren Anwendbarkeit und Relevanz bewertet werden. Die Relevanz möglicher auslösender Ereignisse auf die Kernintegrität hängt unter anderem von den Betriebsphasen oder -zustände ab, in denen sich der Reaktor befindet (z. B. Brennelementwechsel oder Leistungsbetrieb). Die unterschiedlichen Betriebsphasen werden zunächst analysiert. In den unterschiedlichen Betriebsphasen können Betriebsparameter, Verfügbarkeiten von Sicherheitssystemen oder Zustände von Barrieren voneinander abweichen.
- Ermittlung der Eintrittshäufigkeiten der zu untersuchenden auslösenden Ereignisse (Abschnitt 6.7); Die Eintrittshäufigkeiten der unterschiedlichen Transienten, Reaktivitätsstörungen und Leckstörfälle basieren größtenteils auf Werten von NuScale in /NUS 20/. Auch die Eintrittshäufigkeiten für die zu untersuchenden übergreifenden Ereignisse wurden den entsprechenden Unterlagen entnommen.

[9] Beispielsweise wird in den Unterlagen von NuScale an mehreren Stellen ausführlich erörtert, warum manche Vorgaben für das aktuelle Design des SMRs nicht relevant bzw. anwendbar sind.

- Ereignisablaufanalysen und Erstellung von Ereignisbäumen (Kapitel 7.): Die Ereignisablaufanalysen werden anhand der Systembeschreibungen des NuScale-SMR erstellt. Ausgehend von einem auslösenden Ereignis werden die zur Störfallbeherrschung notwendigen Systeme auf Verfügbarkeit überprüft. Je nach Systemverfügbarkeit werden Ereignissequenzen mit zu erwartenden Endzuständen ermittelt. Die Ergebnisse werden in einem Ereignisbaum graphisch zusammengefasst.

- Systemanalysen und Erstellung von Fehlerbäumen für die benötigten Systemfunktionen (Kapitel 8): Die Zuverlässigkeit der Systeme in der Ereignisablaufanalyse wird in der Systemanalyse ermittelt. Alle denkbaren Ausfallmöglichkeiten werden auf Komponentenebene beschrieben und in Fehlerbäumen logisch miteinander verknüpft, um die Ausfallwahrscheinlichkeiten bzw. Zuverlässigkeit der Systeme oder der benötigten Systemfunktionen zu ermitteln.

- Bestimmung der benötigten Zuverlässigkeitskenngrößen (Abschnitt 9.2): Für die Bestimmung der Zuverlässigkeit der Systeme werden die in den Fehlerbäumen modellierten Komponentenzuverlässigkeitskenngrößen quantifiziert. Das betrifft auch die verwendeten Handmaßnahmen, Notfallmaßnahmen und Ausfälle der passiven Systeme.

- Quantifizierung des probabilistischen Modells und Ergebnisdiskussion (Kapitel 9 und 10): Sind alle Fehlerbäume der modellierten Systemfunktionen mit Ereignisbäumen verknüpft und alle Zuverlässigkeitskenngrößen der Komponenten ermittelt, dann lassen sich die Ereignisbäume quantifizieren.
  Es ergeben sich die Gesamthäufigkeit für Schadenszustände, die Häufigkeiten von Schadenszuständen bezogen auf die auslösenden Ereignisse und die Häufigkeiten einzelner Ereignissequenzen. Importanz- und Sensitivitätsanalysen helfen bei der Bestimmung der Ergebnisanteile bestimmter auslösender Ereignisse, Komponenten oder Sequenzen und erlauben somit eine Aussage über die Ausgewogenheit des Anlagendesign in Bezug auf die Unfallsicherheit und eine Aussage über das Verbesserungspotentials der Anlage bzw. des Anlagenkonzeptes.

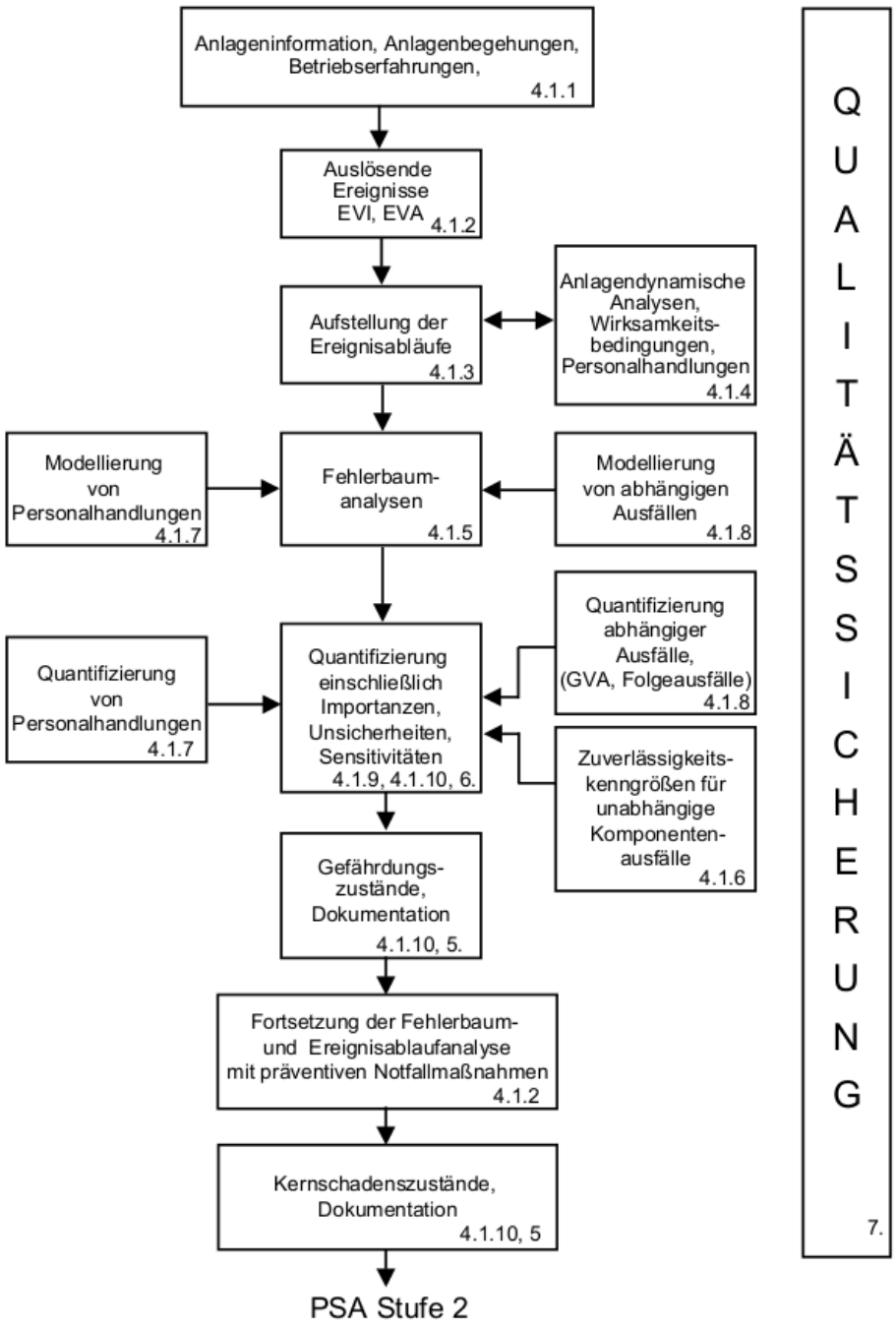


Abb. 4.1 Generelles Vorgehen bei der Erstellung einer PSA der Stufe 1 /BMU 05/

5 Festlegung der Merkmale von Endzuständen und Risikomaße für eine PSA der Stufe 1 für ein bzw. mehrere Reaktormodule eines ausgewählten SMR

In konventionellen Druckwasserreaktoren gibt es drei Sicherheitsbarrieren zum Schutz der Umwelt vor radioaktiven Stoffen. Ausgehend vom Brennstoff werden der Brennstoff und alle entstehenden Spaltprodukte durch Hüllrohre aus Zirkalloy umschlossen. Das Versagen der Hüllrohre für Temperaturen über 1.200 °C entspricht dem Merkmal eines Endzustandes (Merkmal Kernschaden). Dieses Merkmal ist entsprechend /NUS 20/auch im Fall eines SMR anwendbar.

Die zweite (druckführende Umschließung des RCS) und dritte Sicherheitsbarriere (der Sicherheitsbehälter) sind sowohl für die Untersuchung der PSA der Stufe 1 als auch der Stufe 2 relevant und in einem SMR analog zu konventionellen Druckwasserreaktoren vorhanden. Das Versagen der druckführenden Umschließung bzw. des Sicherheitsbehälter ist für Drücke über 174 bar im RCS bzw. über 90 bar im Sicherheitsbehälter zu unterstellen (Überschreitung des Auslegungsdruckes nach /NUS 20b/ bzw. /NUS 20g/). Versagt die druckführende Umschließung bereits aufgrund des auslösenden Ereignisses oder der Maßnahmen zur Verhinderung eines Kernschadens, handelt es sich auch um ein besonderes Merkmal des Endzustands der PSA der Stufe 1.

Ähnlich kann ein Leck außerhalb des Sicherheitsbehälter mit einem entstehenden Kernschaden und einem Dampferzeuger-Bypassleck (ähnliches gilt für das Leck in ein angeschlossenes System) ein Merkmal eines Endzustandes der PSA der Stufe 1 sein. Ein Schaden am Sicherheitsbehälter ergibt sich hauptsächlich direkt aus dem auslösenden Ereignis oder durch eine Druckaufprägung durch das CVCS. Ein Hochdruckversagen der druckführenden Umschließung führt allerdings auch zu einer Gefährdung der Sicherheitsbehälterintegrität. Weitere mögliche Unterscheidungen von Merkmalen für Endzustände finden sich in /HAG 21/, diese sind in Tab. 5.1 aufgelistet. Vor allem die Druckverhältnisse im RCS und die Funktionalität der Sicherheitsbarrieren sollen in die Beschreibung des Kernschadenszustandes einfließen.

Tab. 5.1 Merkmale von Kernschadenszustände und mögliche Anwendung für einen NuScale SMR

Merkmale eines Kernschadenszustandes	Für einen NuScale SMR zu betrachten
Auslösendes Ereignis und bei übergreifenden Einwirkungen auch die Art der Einwirkung	Ja, beispielsweise im Fall von Bränden können sich eingeschränkte Möglichkeiten im weiteren Unfallverlauf ergeben
Art des Ereignisablaufs (z. B. Transiente oder KMV mit/ohne primärseitige Druckentlastung)	Ja, der weitere Verlauf eines Unfalls mit Kernschmelze hängt typischerweise von den Druckverhältnissen im RCS ab
Verfügbarkeit der Notstromversorgung	Im Wesentlichen ist die Notstromversorgung nur für die Verhinderung des Kernschadens relevant
Primärseitige Bespeisung bis mindestens 30 min nach Brennstabschaden	Eine Kernschaden trotz effektiver primärseitiger Bespeisung ist nicht zu erwarten
Sekundärseitige Wärmeabfuhr verfügbar	Die Verfügbarkeit des DHRS könnte einen Einfluss auf das Ausmaß des Kernschadens haben
Sicherheitsbehälter-Abschluss	Ja, die Barrierefunktion des Sicherheitsbehälter ist relevant
Druck im Primärkühlkreislauf	Ja, der Ablauf der Kernschmelze hängt typischerweise von den Druckverhältnissen im RCS ab
Zeitspanne vom auslösenden Ereignis bis zum Schadenszustand	Eine wichtige Information für den Quellterm

Der Hersteller definiert einen Kernschadenszustand wie folgt /NUS 20/: Befindet sich das Modul nach einer Einsatzzeit der störfallbeherrschenden Systeme (mission time) von 72 h nicht in stabilem oder sich verbesserndem Zustand (ohne vorliegenden Kernschaden), so gilt das Szenario als nicht beherrscht. Die dauerhafte Unterkritikalität ist (untypischerweise) kein notwendiges Charakteristikum für einen beherrschten Störfall.

Zusammenfassend können folgende Unterscheidungsmerkmale für einen Endzustand festgestellt werden:

- Sicherer Endzustand mit intaktem Kern (OK): Temperatur der Hüllrohre stets unterhalb von 1.200 °C für 72 h, Temperatur gleichbleibend oder fallend und Druck im RCS unter 174 bar und Sicherheitsbehälter unter 90 bar für 72 h.
  Eine geschlossene druckführende Umschließung ist für einen sicheren Endzustand nicht notwendigerweise erforderlich (bspw. ist die Durchdringung dieser Barriere im Fall einer Notkühlung dauerhaft gegeben). Ein intakter Sicherheitsbehälter allein ist

auch kein Merkmal eines sicheren Endzustandes. Für einen sicheren Endzustand ist die Möglichkeit der Nachzerfallswärmeabfuhr notwendigerweise erforderlich. Unterscheidungen des sicheren Endzustandes kann durch die Angabe der vorherrschenden Maßnahme zur erfolgreichen Nachzerfallswärmeabfuhr unterschieden werden. Die entsprechenden Möglichkeiten sind in Abschnitt 5.1 aufgeführt.

- Kernschadenszustand: Temperatur der Hüllrohre erreicht bzw. übersteigt 1.200 °C, Die Kernschadenszustände werden weiter unterschieden hinsichtlich Zustands bzw. Integrität weiterer Barrieren (im Zusammenhang mit dem auslösenden Ereignis oder den Maßnahmen der Störfallbeherrschung zur Verhinderung des Kernschadenszustandes):
  - Kernschaden (Sicherheitsbehälter intakt, RCS intakt): Integrität des Sicherheitsbehälters innerhalb 72 h nicht verletzt, RCS druckentlastet[10] (Endzustand TE bzw. TEMP);
  - Kernschaden unter hohem Druck im RCS: Integrität des Sicherheitsbehälter innerhalb 72 h nicht verletzt, RCS nicht druckentlastet[11] (Drücke zwischen 128 bar und 145 bar) aber möglicherweise aufgrund hoher Kühlmittel- bzw. Dampftemperaturen gefährdet (Endzustand HT bzw. T-HD);
  - Kernschaden mit Sicherheitsbehälter-Bypass: Ein Leck in einer nicht-absperrbaren Leitung außerhalb des Sicherheitsbehälter liegt bereits vor (aufgrund eines entsprechenden auslösenden Ereignisses) und konnte nicht abgesperrt werden (Endzustand Sicherheitsbehälter bzw. BYPA;
  - Kernschaden mit Leck am Sicherheitsbehälter. Zusätzlich ist von einer Umgehung der druckführenden Umschließung durch geöffnete RVVs oder periodisch öffnende RSVs auszugehen (Endzustand SL bzw. Sicherheitsbehälter L);
  - Kernschaden mit Druckversagen des Sicherheitsbehälter: Ein Versagen des Sicherheitsbehälter aufgrund eines aufgeprägten Überdruckes von mehr als 90 bar (25 % oberhalb des Auslegungsdrucks /NUS 20g/). Zusätzlich ist von einer Umgehung der druckführenden Umschließung durch geöffnete RVVs oder

[10] Die Druckentlastung des Primärkreises erfolgt (bei Ausfall des DHRS) über die Öffnung der RVVs. Die Sicherheitsbarriere der druckführenden Umschließung ist damit umgangen.

[11] Dennoch ist von einer Umgehung der druckführenden Umschließung durch wiederholt ansprechende RSVs auszugehen.

periodisch öffnende RSVs auszugehen (Endzustand SV bzw. Sicherheitsbehälter V);

- Kernschaden bei geöffnetem Sicherheitsbehälter: Ein Schaden entsteht während dem Brennelementwechsel bei geöffnetem Sicherheitsbehälter (Endzustand SO bzw. SBO);

- Ein möglicher Kernschadenszustand ergibt sich nach einem Hochdruckversagen des RCS: Die druckführende Umschließung des RCS versagt aufgrund zu hohen Druckes, über 174 bar, die weitere Kernkühlung kann nicht garantiert werden und die Integrität des Kerns ist gefährdet. Ein zusätzliches Versagen oder eine Umgehung des Sicherheitsbehälters kann nicht ausgeschlossen werden oder liegt aufgrund eines entsprechenden auslösenden Ereignisses bereits vor (Endzustand HV bzw. HD V). Die Kernschadensendzustände werden in den Konsequenzen der Ereignisablaufanalysen in den Abschnitten 7.4 und 7.5 für alle Transienten mit Kernschaden (KS) angegeben.

5.1 Möglichkeiten zur Nachzerfallswärmeabfuhr im Störfallverlauf

Ein sicherer Endzustand erfordert eine erfolgreiche Nachzerfallswärmeabfuhr. Die Anlage bietet vier Möglichkeiten den Kern im Störfallverlauf zu kühlen. Diese Möglichkeiten sind zum einen passiv, über das DHRS oder das ECCS, oder aktiv über eine Einspeisung mit dem CVCS oder das CFDS-Fluten des Sicherheitsbehälters. Die Besonderheiten sind nachfolgend aufgeführt.

Nachwärmeabfuhr über das Nachwärmeabfuhrsystem

Je nach Bedingungen im Reaktor kann die automatische Aktivierung des zweifach redundanten DHRS (in RiskSpectrum® auch mit HR abgekürzt) verzögert erfolgen, hierzu zählen z. B. Fälle, in denen die RESA aufgrund zu hoher Reaktorleistung ausgelöst wird, gezeigt für den Fall einer Dampferzeugerüberspeisung („increase in steam flow“) /NUS 20b/. Der Start des Systems ist an mehrere Bedingungen gekoppelt, die einen Temperaturanstieg (und damit einen Wärmerückstau) im RCS abdecken (Temperatur im RCS zu hoch, Frischdampfdruck zu hoch oder Druck im RCS zu hoch). Multiples Sensor-Versagen oder das gemeinsame Versagen der DHRS-Auslöseventile (DHRS actuation valves, zwei Stück pro Redundanz) können zum Ausfall des DHRS führen. Zur auslegungsgemäßen Nachzerfallswärmeabfuhr und Kühlung des heißen Kerns reichen

eine Redundanz und das Öffnen eines DHRS-Auslöseventils dieser Redundanz /NUS 20b/. Gleichzeitig zur Aktivierung des DHRS erfolgt der Dampferzeuger-Abschluss. Für den Dampferzeuger-Abschluss werden deshalb unter anderem die gleichen Kriterien wie für die Aktivierung des DHRS verwendet. Das DHRS steht in der Regel bereits kurze Zeit nach der RESA (ca. 10 s) vollständig zur Verfügung, der Naturumlauf stabilisiert sich innerhalb von 1 bis 2 Minuten. Das DHRS ist das einzige Kühlsystem, das schon wenige Sekunden nach der RESA zur Verfügung steht. Alle weiteren Systeme setzen erst deutlich verzögert ein.

Wärmeabfuhr über die Reaktorsicherheitsventile in den Sicherheitsbehälter

Ist das DHRS nicht verfügbar, so kann die Wärmeabfuhr aus dem RCS über die RSVs (öffnen bei 110 % des Nominaldruckes, 143 bar und 145 bar /NUS 20c/) in den Sicherheitsbehälter erfolgen. Hierfür ist das Öffnen mindestens eines der zwei RSVs erforderlich. Öffnet mindestens ein Ventil vollständig, so wird nach einer gewissen Zeit für die weitere Nachzerfallswärmeabfuhr das ECCS (initiiert durch Wasserstand im Sicherheitsbehälter zu hoch oder Druck im Kühlkreislauf zu niedrig) verwendet oder die Wiederbespeisung des RDB über das CVCS (Regulierung des Druckhalterfüllstandes auf den Betriebsbereich /NUS 20d/, Abkürzung VC) veranlasst. Da es zu diesem Zeitpunkt bereits zu einem Abschluss des CVCS und des Deionatsystems (demineralized water system) gekommen ist, stellt die Wiederbespeisung durch das CVCS eine Handmaßnahme der Betriebsmannschaft dar.

Wichtig ist die Druckregelung der Wiederbespeisung, da bei geöffneter Verbindung zum Sicherheitsbehälter ein Überdruck im Sicherheitsbehälter möglich ist. Das CVCS kann bei Einspeiseraten bis 1,3 l/s in 72 h 340 m³ Wasser einspeisen, der Sicherheitsbehälter fasst maximal 174 m³ (Einbauten nicht berücksichtigt). Dabei kann das CVCS bis zu Drücken von 155 bar einspeisen, mit einem Sicherheitsbehälter-Versagen ist ab 90 bar zu rechnen.

Bleiben beide RSVs geschlossen, so kann die Nachzerfallswärme nach dem CFDS-Fluten des Sicherheitsbehälter (initiiert durch die Betriebsmannschaft, Abkürzung CF) schrittweise abgeführt werden. Im ersten Schritt gelangt die Wärme über den Primärkühlkreislauf an die RDB-Außenwand, die Wärme wird durch die Wand transportiert und an das Kühlmittel im gefluteten Sicherheitsbehälter abgegeben, gelangt über Konvektion an die Außenwand des Sicherheitsbehälters, tritt durch die Wand durch und wird im letzten Schritt im Reaktorbecken abgegeben aufgenommen.

Nachwärmeabfuhr über das Notkühlsystem

Sind die RSVs geöffnet, dann kann über das ECCS (in RiskSpectrum® auch mit EC abgekürzt) der Kühlkreislauf druckentlastet und das gekühlte Wasser aus dem Sicherheitsbehälter wieder in den Kühlkreislauf zurückgeführt werden. Das ECCS wird aufgrund eines hohen Füllstandes im Sicherheitsbehälter oder durch niedrigen Druck im Kühlkreislauf automatisch angefordert, kann aber auch von der Betriebsmannschaft gestartet werden. Die Kühlleistung des ECCS übersteigt dabei die Kühlleistung einer Redundanz des DHRS und ist ausreichend, um den Druck im RCS abzubauen /NUS 20e/. Das ECCS steht im Vergleich zum DHRS deutlich später zur Verfügung, da der Sicherheitsbehälter zunächst teilweise gefüllt sein muss, damit sich die RRV-Sicherheitsbehälterseitig unter Wasser befinden (im Bereich einer bis weniger Stunden).

Übersicht über alle Möglichkeiten der Nachzerfallswärmeabfuhr

Ein NuScale-Reaktormodul verfügt insgesamt über vier Möglichkeiten der Wärmeabfuhr, eine dieser Möglichkeiten ist zweifach redundant vorhanden. Die Möglichkeiten zur Wärmeabfuhr können teilweise parallel genutzt werden (DHRS mit Nachzerfallswärmeabfuhr über den Sicherheitsbehälter).

Tab. 5.2 Möglichkeiten der Nachzerfallswärmeabfuhr im Störfallverlauf

Möglichkeit der Nachzerfalls-wärmeabfuhr	Anzahl Redundanzen	Hand-maßnahme erforderlich	Einschränkungen für die Verwendung
DHRS (HR)	2	nein	Gleichzeitige Verwendung mit anderen Formen der Nachzer-fallswärmeabfuhr möglich, aller-dings am wirksamsten für ein druckbeaufschlagtes RCS; keine Verwendung bei größeren Verlus-ten an Kühlmittelinventar auf der Sekundärseite der Dampferzeu-ger. Keine Verwendung bei Ver-lust des Naturumlaufes im RCS (u. a. bei zu wenig Kühlmittel)
Einspeisung über das CVCS und Dampfabgabe in den SB über die RSVs (VC)	2 RSVs, CVCS-Einspeise- und Sprühleitung	ja, Inbetrieb-nahme der CVCS-Einspeisung	Elektrische Stromversorgung der CVCS-Aufbereitungspumpen notwendig, die Kühlmethode wird typischerweise entweder durch den Beginn der Notkühlung über das ECCS oder einen aufgefüll-ten SB beendet. Das Inventar im RCS dient als Puffer bei Proble-men mit der Einspeisung bzw. der Überbrückungszeit bis zur Durchführung der Maßnahme
ECCS (EC)	3 Redundanzen der RVVs, 2 Re-dundanzen der RRV	nein, Start über Handmaßnahme auch möglich	Adäquates Kühlmittelinventar notwendig (nicht redundant)
CFDS Füllung des SB (Abkürzend CF)	Jeweils eine Re-dundanz des CFDS für 6 Mo-dule verfügbar	ja, Fluten über CFDS oder dau-erhafte Einspei-sung über CVCS	Für ATWS ist diese Form der Wärmeabfuhr typischerweise nicht ausreichend

Die Abkürzungen HR, VC, EC und CF werden auch in den Ereignisablaufanalysen in den Abschnitten 7.4 und 7.5 für beherrschte Unfalltransienten angegeben.

6 Ermittlung eines abdeckenden Spektrums zu untersuchender, anlageninterner auslösender Ereignisse für alle Betriebsphasen

Als auslösende Ereignisse werden hier solche Ereignisse verstanden, die entweder automatische Maßnahmen oder Maßnahmen des Betriebspersonals erfordern, um die Einhaltung der Schutzziele Reaktivitätskontrolle oder Brennelementkühlung zu gewährleisten. Ohne Gegenmaßnahmen können diese Ereignisse zu Brennstabschäden und damit zu einer größeren Aktivitätsfreisetzung führen.

Für Anlagen mit Leichtwasserreaktoren lassen sich folgende Gruppen anlageninterner auslösender Ereignisse unterscheiden:

- Reaktivitätsstörungen,
- Störungen der Wärmeabfuhr (Transienten),
- Kühlmittelverluststörfälle (KMV),
- übergreifende Einwirkungen von innen (mechanische, z. B. durch Lastabstürze oder Handhabungsfehler, thermische, wie Brand etc.).

Folgende Quellen wurden für die Ermittlung des Spektrums der zu untersuchenden auslösenden Ereignisse herangezogen:

- Dokumente des Herstellers, insbesondere /NUS 20/, die auslösenden Ereignisse sind entsprechend der folgenden Auswirkungen auf den Reaktor teilweise zusammengefasst (z. B. das fehlerhafte Öffnen eines RSVs, ein anderweitiges, nicht-absperrbares Leck in den Sicherheitsbehälter und eine Überspeisung durch das CVCS werden gemeinsam betrachtet). Die zusammengefassten Ereignisse sind folgendermaßen abgekürzt:
  - TGS-TRAN-NPC: Allgemeine Transiente;
  - TGS-TRAN-NSS: Verlust von Versorgungssystemen;
  - EHVS-LOOP: Verlust der externen Stromversorgung;
  - EDSS-LODC-ET: Ausfall des EDSS;
  - TGS-FMSLB-UD: Bruch einer Leitung im Sekundärkühlkreis;
  - MSS-ALOCA-SG: Dampferzeuger-Bypassleck;

- ECCS-ALOCA-RV1: Fehlerhaftes Öffnen eines ECCS-Ventils;
- RCS-ALOCA-IC: KMV in den Sicherheitsbehälter;
- CVCS-ALOCA-CIC: KMV der CVCS-Einspeiseleitung in den Sicherheitsbehälter;
- CVCS-ALOCA-COC: KMV der CVCS-Einspeiseleitung in das Reaktorgebäude;
- CVCS-ALOCA-LOC: KMV der CVCS-Entnahmeleitung in das Reaktorgebäude; allerdings sind die Beschreibungen der zusammengefassten Ereignisse hier nicht vollständig, eine ausführliche Darstellung ergibt sich in Tab. 6.1 und Tab. 6.2 bzw. in /NUS 20/;

- die Fachbände zu PSA-Methoden des deutschen PSA-Leitfadens /FAK 05/ und /FAK 16/ als Teil des deutschen Regelwerks;
- ein weiteres europäisches Regelwerk /ANV 15/.

Für die einzelnen Ereignisse wird geprüft, ob sie in der PSA für SMRs zu untersuchen oder vernachlässigbar sind. Die auslösenden Ereignisse, die im Folgenden betrachtet werden sollen, werden den einzelnen Anlagenbetriebszuständen zugeordnet. Die Anlagenbetriebszustände sind nachfolgend beschrieben.

6.1 Anlagenbetriebszustände

Folgende Anlagenbetriebszustände sind in /NUS 20/ aufgeführt:

- Anlage im Leistungsbetrieb „Operation“ (Mode 1);
- Anlage heiß und im Abfahrbetrieb „Hot Shutdown“ (Mode 2), bei Kühlmitteltemperaturen größer oder gleich 216 °C;
- Anlage im geschützten Abfahrbetrieb „Safe Shutdown“ (Mode 3), bei Kühlmitteltemperaturen kleiner als 216 °C;
- Anlage im Übergangsbetrieb „Transition“ (Mode 4),
- Anlage beim Wechsel der Brennelemente „Refuelling“ (Mode 5); der Brennelementwechsel wird alle 24 Monate durchgeführt und dauert ungefähr zehn Tage /NUS 20/. Dieser Zeitraum entspricht 120 h pro Jahr. Der Brennelementwechsel lässt sich in sieben Anlagenbetriebszustände untergliedern:

1. Abfahren und anfängliche Kühlung, 7 h pro Jahr
2. Kühlung über den Sicherheitsbehälter, 16,6 h pro Jahr
3. Transport und Entnahme, 11,5 h pro Jahr
4. Neubeladung und Wartung, 37,5 h pro Jahr
5. Befestigung, Transport und Wiederanschluss, 36,9 h pro Jahr
6. Aufwärmphase, 6,5 h pro Jahr
7. Betrieb bei geringer Leistung, 6,4 h pro Jahr

Es ergeben sich damit insgesamt 122,4 h pro Jahr.

Entsprechend entfallen maximal 8.644 h pro Jahr auf den Leistungsbetrieb (Mode 1).

6.2 Transienten (Mode 1)

Transienten sind Ereignisse, die zu einem Ungleichgewicht zwischen Wärmeerzeugung im Kern und Wärmeabfuhr aus dem RCS führen. Der vollständige Ausfall der Wärmeabfuhr aus dem Kern kann zu Brennelementschäden führen.

Bei den Transienten werden auch Störungen der Reaktivitätskontrolle betrachtet. Unkontrollierte Reaktivitätsänderungen führen zu Leistungsänderungen.

In Tab. 6.1 sind die möglichen Transienten aufgelistet.

Tab. 6.1 Transienten und Reaktivitätsstörungen

Auslösendes Ereignis nach /NUS 20/ und /ANV 15/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
Störungen der Reaktivitätskontrolle			
Inadvertent reactor trip TGS-TRAN-NPC	Nicht berücksichtigt	RESA, Abfahren der Anlage	j
Inadvertent boration	Nicht berücksichtigt	Leistungsreduktion	nein
Inadvertent deboration	Lecks aus Deionat führenden Systemen	Leistungsanstieg, RESA; dieses Ereignis wird abdeckend durch „Fehlausfahren der Steuerstäbe“ untersucht	nein
Ecxessive rod or rod-group withdrawal, control rod ejection	Fehlausfahren der Steuerstäbe	Leistungsanstieg, RESA	j
Inadvertent control rod drop	Nicht berücksichtigt	Leistungsreduktion	nein
Control rod misalignment	Nicht berücksichtigt	Schieflast, RESA; dieses Ereignis wird abdeckend durch „Fehlausfahren der Steuerstäbe“ untersucht	nein
ATWS berücksichtigt für alle analysierten auslösenden Ereignisse	ATWS bei Ausfall Haupt-speisewasser, beim Notstromfall, bei Ausfall Hauptwärmesenke und Hauptspeisewasser oder bei sonstigen Transienten	keine Leistungsreduktion, primärseitige Druckentlastung, Bor-Einspeisung über ECCS oder CVCS	ja, als multiples Versagen
Störungen der Eigenbedarfsversorgung			
Loss of offsite power, loss of AC power to station auxiliaries EHVS-LOOP	Notstromfall, extern	RESA, Ausfall Speisewasser-versorgung und Frischdampfabgabe, Nachzerfallswärmeabfuhr über DHRS, nach 24 h Notkühlung über ECCS	ja

Auslösendes Ereignis nach /NUS 20/ und /ANV 15/	**Auslösendes Ereignis aus /FAK** 05/ **und /FAK** 16/	**Auswirkungen**	**Zu untersuchen?**
Loss of direct current EDSS-LODC-ET	Nicht berücksichtigt	Kontrolle über Reaktor von Warte aus nicht möglich, RESA, Sicherheitsbehälterabschluss, Nachzerfallswärmebfuhr über DHRS, ECCS setzt verzögert ein	ja
Partial loss of AC power TGS-TRAN-NSS	Nicht berücksichtigt	Ausfall von CVCS und d CFDS, Verlust von Stromschienen, RESA, Nachzerfallswärmeabfuhr über DHRS	ja
Fehlanregung von Sicherheitssystemen			
Inadvertent actuation of the decay heat removal system	Fehlerhafte Anregung der Notkühlsignale	Leistungsreduktion, Wärmeverlust in das Reaktorbecken	nein
Störungen der Frischdampfabgabe			
Inadvertent turbine control valve open	Fehlöffnen von Turbinen- und Umleitstellventilen	Druckabfall im Frischdampf-System, Leistungsreduktion	nein
Ecxessive increase in secondary steam flow	Nicht berücksichtigt	Druckabfall im Frischdampf-System, Leistungsreduktion	nein
Inadvertent main steam safety valve open, main steam line break TGS-FMSLB-UD	Transienten durch Frischdampf-Leitungslecks innerhalb oder außerhalb Sicherheitsbehälter	Druckabfall im Frischdampf-System, RESA, Nachzerfallswärmeabfuhr über DHRS in das Reaktorbecken	ja
Turbine trip, loss of external electric loads	Nicht berücksichtigt	Wärmeabgabe über Umleitstation, Leistungsbegrenzung für den Reaktor	nein

Auslösendes Ereignis nach /NUS 20/ und /ANV 15/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
Loss of condenser vacuum, loss of cooling water systems TGS-TRAN-NPC	Ausfall Hauptwärmesenke, Sekundärkühlkreisabschluss, Ausfall Hauptwärmesenke und Hauptspeisewasser	Druckanstieg im Frischdampfsystem, Verlust der Hauptwärmesenke (z. B. des Umlaufkühlsystems, Circulating Water System /NUS 20i/), RESA, Nachzerfallswärmeabfuhr über DHRS; abgedeckt durch die allgemeine Transiente	nein
Störungen der Speisewasserversorgung			
Loss of feedwater flow TGS-TRAN-NPC	Ausfall Haupt-Speisewasser	RESA, Nachzerfallswärmeabfuhr über DHRS	ja
Main feedwater line break TGS-FMSLB-UD, pipe break in decay heat removal system	Transienten durch Speisewasserleitungslecks, Speisewasserleitungsleck im Maschinenhaus, Speisewasserleitungsleck innerhalb Sicherheitsbehälter; nicht absperrbar, Leck im Nachkühlsystem im Sicherheits-behälter oder in der Reaktorhalle	Ausfall der Speisewasserversorgung, RESA, Nachzerfallswärmeabfuhr über den zweiten, nicht betroffenen DHRS-Strang	ja
Feedwater malfunction causing increase in feedwater flow, inadvertent closure of main steam isolation valves TGS-FMSLB-UD	Dampferzeugerüberspeisung	RESA, Dampferzeugerüberspeisung, Nachzerfallswärmeabfuhr über DHRS	ja
Sonstige			
Loss of subcooling in the riser, failure in the module heat-up system, core flow blockage	Nicht berücksichtigt	Funktionales Versagen des Naturumlaufes im RCS. Temperaturanstieg im Kern, RESA	ja
Loss of containment vacuum	Nicht berücksichtigt	Wärmeverlust in das Reaktorbecken, Leistungsreduktion	nein

Auslösendes Ereignis nach /NUS 20/ und /ANV 15/	**Auslösendes Ereignis aus /FAK** 05/ **und /FAK** 16/	**Auswirkungen**	**Zu untersuchen?**
Nicht berücksichtigt	Leck am Sicherheitsbehälter	Wärmeverlust in das Reaktorbecken, Leistungsreduktion, Fehlanforderung des ECCS	ja
Loss of service water. loss of support systems TGS-TRAN-NSS	Ausfall Hauptwärmesenke	Unverfügbarkeit des CVCS und des CFDS, Verlust von Stromschienen, RESA, Nachzerfallswärmeabfuhr über DHRS	ja
Pressurizer spray fails to open	Nicht berücksichtigt	Druckanstieg im RCS, RESA, Nachzerfallswärmeabfuhr über DHRS	ja
Increase of reactor coolant inventory: charging > letdown	Nicht berücksichtigt	Druckanstieg im RCS, RESA, Nachzerfallswärmeabfuhr über DHRS	ja
Pressurizer spray fails to close CVCS-ALOCA-IC	Nicht berücksichtigt	Geringfügige Drucktransiente; abgedeckt durch „Increase of reactor coolant inventory“	nein
Decrease of reactor coolant inventory: charging < letdown	Nicht berücksichtigt	Füllstandsabfall, RESA, Notkühlung über ECCS oder Nachzerfallswärmeabfuhr über DHRS; Abgedeckt durch KMV	nein

Reaktivitätsstörungen mit Einfahren der Steuerstäbe oder einer zu hohen Borierung führen zu einer Leistungsreduktion und zu einem sicheren Anlagenzustand ohne den Einsatz von Hilfssystemen. Reaktivitätsstörungen mit positiven Reaktivitätseinträgen sollen zusammengefasst betrachtet werden.

Ausfälle und Lecks der Sekundärseite des Kühlsystems können vereinfacht in Leitungslecks (auf Frischdampf- und Speisewasser-Seite) und Verlust der Hauptwärmesenke aufgeteilt werden. In beiden Fällen werden die Dampferzeuger für den Sekundärkühlkreis abgesperrt und für die Nachzerfallswärmeabfuhr über das DHRS in das Reaktorbecken geöffnet. Zusätzlich soll im Sekundärkühlkreis noch der Fall einer Dampferzeugerüberspeisung untersucht werden.

Aus den oben aufgelisteten Ereignissen ergeben sich folgende weiter zu untersuchende Ereignisse:

- Allgemeine Transiente (nur RESA wird ausgelöst oder Ausfall der Hauptwärmesenke), siehe Abschnitt 7.4.1,
- Fehlausfahren der Steuerstäbe[12], siehe Abschnitt 7.4.2,
- Ausfall der externen Stromversorgung, siehe Abschnitt 7.4.3,
- EDSS-Ausfall, siehe Abschnitt 7.4.4,
- Leitungsleck im Sekundärkühlkreis, siehe Abschnitt 7.4.5,
- Dampferzeugerüberspeisung, siehe Abschnitt 7.4.6,
- Überspeisung durch das CVCS (Anstieg des Kühlmittelinventars), siehe Abschnitt 7.4.7,
- Ausfall von Komponentenhilfssystemen (CVCS und CFDS), siehe Abschnitt 7.4.8,
- Leck am Sicherheitsbehälter, siehe Abschnitt 7.4.9,
- Funktionales Versagen des Naturumlaufes im RCS nach einem Verlust der Unterkühlung im Steigrohr, siehe Abschnitt 7.4.10.

[12] Abdeckend soll eine Transiente mit maximalem Reaktivitätseintrag bei größtmöglicher Eintragsgeschwindigkeit betrachtet werden.

6.3 Kühlmittelverluststörfälle

Der Verlust von RCS-Kühlmittel kann, wenn er nicht unterbunden oder überspeist wird, zum Ausfall der Wärmeabfuhr führen. In Tab. 6.2 sind die möglichen Kühlmittelverluststörfälle aufgelistet.

Insgesamt sind sechs unterschiedliche Leckstörfälle zu untersuchen:

- KMV in den Sicherheitsbehälter durch Leitungsbrüche oder fehlerhaftes Öffnen von Armaturen (Leck nicht absperrbar), siehe Abschnitt 7.5.1,
- KMV der CVCS-Einspeiseleitung in den Sicherheitsbehälter (Leck nicht absperrbar), siehe Abschnitt 7.5.2,
- KMV der CVCS-Einspeiseleitung in das Reaktorgebäude durch Leitungsbrüche oder fehlerhaftes Öffnen von Armaturen (Leck absperrbar), siehe Abschnitt 7.5.3,
- KMV der CVCS-Entnahmeleitung in das Reaktorgebäude durch Leitungsbrüche oder fehlerhaftes Öffnen von Armaturen (Leck absperrbar), siehe Abschnitt 7.5.4,
- Dampferzeuger-Bypasslecks (KMV in den Sekundärkühlkreislauf), siehe Abschnitt 7.5.5, und
- Fehlöffnen eines Ventiles des ECCS, siehe Abschnitte 7.5.1 und 7.5.6.

Es gibt verschiedene Versagensmechanismen, die nach /NUS 20e/zum Fehlöffnen eines ECCS-Ventils führen können:

- Mechanisches Versagen; dieser Fall entspricht direkt einem primärseitigen Leck, Abschnitt 7.5.1,
- Elektrisches Versagen oder Versagen der Ansteuerung; bei niedrigen Drücken im RDB entspricht dieser Fall dem eines primärseitigen Lecks, Abschnitt 7.5.1. Im Leistungsbetrieb spricht der IAB an und die fehlerhaften Ventile öffnen. Eine RESA wird in diesem Fall nicht ausgelöst.

Tab. 6.2 Kühlmittelverluststörfälle

Auslösendes Ereignis /NUS 20/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
RCS leakage, LOCA inside containment CVCS-ALOCA-IC (reactor vessel rupture)	Leck im Primärkühlsystem (verschiedene Querschnitte) Lecks in einer Hauptkühlmittelleitung Lecks am Druckhalter	Kühlmittelverlust in den Sicherheitsbehälter, Abschluss Sicherheitsbehälter, RESA, Notkühlung über ECCS	ja
Steam generator tube failure MSS-ALOCA-SG	Dampferzeugerheizrohrleck	Kühlmittelverlust in den Sekundärkühlkreis, RESA, Sicherheitsbehälterabschluss, Dampferzeugerabschluss, Nachzerfallswärmeabfuhr über einen Strang des DHRS	ja
LOCA outside containment CVCS-ALOCA-COC	Leck im Volumenregelsystem	Kühlmittelverlust in das Reaktorgebäude, RESA, Leckisolierung, Nachzerfallswärmeabfuhr über DHRS	ja
Interfacing systems LOCA ECCS-ALOCA-RV1	Leck in ein angeschlossenes System	Wird durch Leck im CVCS abdeckend berücksichtigt	ja
Spurious reactor safety valve (RSV) opening CVCS-ALOCA-IC	Fehloffenes Druckhalter-Sicherheitsventil. kleines Leck am Druckhalter durch Fehlöffnen eines Sicherheitsventils	Kühlmittelverlust in den Sicherheitsbehälter, RESA, Notkühlung über ECCS	ja
Spurious Opening of an ECCS Valve (RVV oder RRV) ECCS-ALOCA-RV1	Nicht berücksichtigt	Kühlmittelverlust, RESA, Notkühlung über ECCS, Wiederbefüllung über CVCS	ja
Inadvertent actuation of a reactor vent valve (RVV) CVCS-ALOCA-IC	Nicht berücksichtigt	Kühlmittelverlust, RESA, Notkühlung über ECCS	ja

Auslösendes Ereignis /NUS 20/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
Inadvertent actuation of reactor relief valve (RRV) CVCS-ALOCA-IC	Fehloffenes DH-AV – durch Wartungsfehler, im Notstromfall oder nach TUSA, Lecks am Druckhalter bei Ausfall Hauptspeisewasser, bei Ausfall Hauptwärmesenke oder bei anderen Transienten	Kühlmittelverlust, RESA, Notkühlung über ECCS	ja
Letdown relief valve opening CVCS-ALOCA-IC	Nicht berücksichtigt	Kühlmittelverlust in den Sicherheitsbehälter, RESA, Notkühlung über ECCS	ja
RCS-ALOCA-CIC	Leck im Volumenregelsystem	Kühlmittelverlust in den Sicherheitsbehälter, Abschluss Sicherheitsbehälter, RESA, Notkühlung über ECCS	ja
Letdown or sample line break CVCS-ALOCA-LOC	Nicht berücksichtigt	Kühlmittelverlust in das Reaktorgebäude, RESA, Leckisolierung, Einspeisung über CVCS, Nachzerfallswärmeabfuhr über DHRS	ja
Pressurizer heater fails or Failure in a pressurizer heater penetration CVCS-ALOCA-IC	Nicht berücksichtigt	Leck im Druckhalter an der Öffnung für die Druckhalterheizung, Kühlmittelverlust in den Sicherheitsbehälter, RESA, Notkühlung über ECCS	ja

6.4 Übergreifende Einwirkungen von innen

Zur Begrenzung der Auswirkungen eines anlageninternen Brandes oder einer anlageninternen Überflutung ist die Anlage in unterschiedliche Brandabschnitte und Überflutungsbereiche eingeteilt, die so ausgelegt sind, dass ein Brand auf die betroffenen Brandabschnitte und eine Überflutung auf die entsprechende Überflutungsbereiche beschränkt bleiben. Brandabschnitte sind aus diesem Grund u. a. mit Brandschutztüren und automatisch abschließenden Brandschutzklappen voneinander abgetrennt. Die Abschnitte sind so gewählt, dass ein anlageninterner Brand oder eine anlageninterne Überflutung in einem Modul nicht auf die anderen Module übergreift. Das gesamte Konzept ist in /NUS 20/ und /NUS 20d/ genauer beschrieben. Zunächst sollen die möglichen Ursachen für übergreifende Einwirkungen von innen untersucht werden.

6.4.1 Anlageninterne Überflutung

Systeme, die ein wesentliches Risiko für eine anlageninterne Überflutung im Reaktorgebäude darstellen, sind nach /NUS 20/ das Reaktorbecken und nachfolgend aufgeführte Systeme, die über Pumpen Wasser aus dem Reaktorbecken entnehmen:

- das CFDS,
- das Kühlsystem des Brennelementlagerbeckens und
- das Kühlsystem des Reaktorbeckens.

Darüber hinaus sind folgende Systeme im Sekundärkühlkreis eine mögliche Ursache für Überflutungen im Reaktor- oder Turbinengebäude:

- das Frischdampfsystem und
- das Kondensat- und Speisewassersystem.

Kühlwassersysteme, die große Mengen Kühlmittel führen, und das Feuerlöschsystem stellen zusätzlich ein wesentliches Risiko für eine interne Überflutung im Reaktor-, Turbinen-, Entsorgungs-, Kontrollraum- oder Nebengebäude dar. Interne Überflutungen in unterschiedlichen Gebäuden, u. a. das Reaktor-, die Turbinen- oder das Entsorgungsgebäude, können eine RESA auslösen (dies führt zu einer allgemeinen Transiente). Eine Gefahr der Beschädigung von Systemen zur Störfallbeherrschung besteht nur im

Reaktorgebäude. Dort sind Überflutungen, die entsprechende Schäden verursachen könnten, in folgenden Bereichen möglich:

- Bereich der CVCS-Aufbereitungspumpen: Ein Überflutungsschutz ist vorhanden, dennoch soll konservativ ein Ausfall der CVCS-Aufbereitungspumpen unterstellt werden.
- Bereich der Komponentenkühlwasserpumpen: In diesem Bereich befinden sich keine Komponenten zur Störfallbeherrschung.
- Bereich der Deionat-Pumpen: Eine Überflutung in diesem Bereich kann zu einem Ausfall der Deionat-Pumpen führen.

Folgen einer anlageninternen Überflutung

In der Folge einer anlageninternen Überflutung im Reaktorgebäude kommt es zu einem auslösenden Ereignis „Ausfall von Komponentenhilfssystemen“ entsprechend der Ereignisablaufanalyse in Abschnitt 7.4.8. In der Folge einer anlageninternen Überflutung im Turbinengebäude wird eine allgemeine Transiente ausgelöst, Abschnitt 7.4.1.

6.4.2 Anlageninterner Brand

Ein Brand kann durch unterschiedliche Zündquellen entstehen, dazu zählen feste Zündquellen, wie Stromerzeuger (z. B. Dieselgeneratoren), Batterien, Elektronikschränke, Transformatoren und Stromverbraucher (z. B. Elektromotoren, Ventilatoren und Pumpen), und nur temporär vorhandene Zündquellen (z. B. Schweiß-, Trenn- oder Schneidearbeiten). Ein Brand in folgenden Bereichen kann relevante Folgen haben:

- Ein Brand im Bereich der CVCS-Aufbereitungspumpen kann zu Schäden an den Pumpen oder zu einer unerwünschten Überspeisung durch das CVCS (über einen fehlerhaften Betrieb des CVCS) führen.
- Ein Brand in der Umspannanlage oder in den Stromverteilbereichen kann einen Notstromfall zur Folge haben.
- Ein Brand in der Reaktorwarte, im Elektronikkorridor oder in den Bereichen des Reaktorschutzsystems (in einer der beiden Redundanzen) kann zu einer fehlerhaften Aktivierung des ECCS oder zu einer Öffnung einzelner ECCS-Ventile führen.

- Ein Brand in Teilen des Maschinenhauses oder im Bereich des Sekundärkühlkreises kann zu einer Dampferzeugerüberspeisung führen.
- Ein Brand im Bereich der Steuerstabantriebe kann ein Fehlausfahren der Steuerstäbe zur Folge haben.
- Ein Brand in den Batterieräumen oder den Räumen der EDSS-Schaltanlagen kann zu einem Ausfall der EDSS-Batterieversorgung oder zu einem Ausfall eines EDSS-Busses führen.
- Ein Brand im Bereich der Komponentenkühlwasserpumpen und der CFDS-Pumpen kann zu einer allgemeinen Transiente mit möglichem Ausfall eines oder mehrerer Komponentenhilfssysteme führen.
- Brände in anderen Bereichen des Reaktorgebäudes führen zu einer allgemeinen Transienten.
- Ein bereichsübergreifender Brand kann u. a. einen Ausfall aller Hilfssysteme zur Folge haben.

Folgen eines anlageninternen Brandes

Die möglichen Folgen eines anlageninternen Brandes hängen vom Brandort innerhalb der Anlage bzw. innerhalb eines Modulbereiches ab. Modulspezifische Räume sind bestimmte Räume im Reaktorgebäude. Alle weiteren Räume sind keinem spezifischen Modul zugeordnet.

Im Fall anlageninterner Brände im Reaktorgebäude in sieben, einen Brandabschnitt bildenden Räumen Beeinträchtigungen an den CVCS von sechs Modulen entstehen, u. a. Schäden an den CVCS-Aufbereitungspumpen und den Absperrventilen des Deionatsystems. Als auslösendes Ereignis kann mit einer Überspeisung durch das CVCS übergreifend in allen sechs betroffenen Modulen gerechnet werden /NUS 20/, die Ereignisablaufanalyse findet sich in Abschnitt 7.4.7.

Brände in der Umspannanlage oder in den Bereichen der Stromverteilung wirken sich möglicherweise auch auf alle Module gleichermaßen aus und führen in einen Ausfall der Stromversorgung entsprechend Abschnitt 7.4.3. Eine fehlerhafte Aktivierung des ECCS (siehe Abschnitt 7.5.6) über beide Redundanzen des ESFAS ergibt sich für alle Module gleichermaßen im Zuge von Bränden in der Warte bzw. im Reaktorkontrollgebäude

(siehe Abb. 3.1) oder im Reaktorgebäude in einem Brandabschnitt mit den entsprechenden drei Räumen. Des Weiteren ergibt sich eine modulspezifische Aktivierung des ECCS über eine Redundanz des ESFAS in Folge eines Brandes, z. B. im Raum der ESFAS-Redundanz I für Modul 1 oder im entsprechenden Raum der ESFAS-Redundanz II für Modul. In diesen Fällen sind jeweils zwei RVVs und ein RRV von der Aktivierung betroffen. Ein zusätzlicher Ausfall der CVCS für sechs Module folgt auf einen brandabschnittsübergreifenden Brand der Räume in den beiden bereits oben aufgeführten Brandabschnitten des Reaktorgebäudes oder der ESFAS-Redundanz I für ein abschnittsübergreifenden Brand der entsprechenden dortigen Räume (alle Module gleichermaßen betroffen).

Ein Ausfall der Steuerstabantriebe für sechs Module kann aus einem Brand im Bereich der mechanischen Anlagenteile der Steuerstabsysteme (zwei Räume, die zusammen einen Brandabschnitt bilden) entstehen. Dieser Ausfall hat keine Auswirkungen auf die Störfallbeherrschung und führt zu einer allgemeinen Transiente, siehe Abschnitt 7.4.1.

Neben dem Einfluss auf die Steuerstabantriebe ist darüber hinaus mit einem Ausfall der ESFAS-Redundanz II aller Module zu rechnen (z. B. ist davon ein RVV und ein RRV betroffen, die sich im Bedarfsfall nicht öffnen). Ein Ausfall der ESFAS-Redundanz I für sechs Module ergibt sich im Zusammenhang mit einem Brand in Raum 411, das CFDS fällt für sechs Module in Folge eines Brandes im Raum 409 aus. Ein Ausfall einzelner EDSS-Busse eines Moduls ergibt sich bei Bränden in den Räumen der Batterieladegeräte und Schaltanlagen, für Modul 1 sind dies die vier Räume mit dem jeweiligen Ladegerät für die Batterien der EDSS-Busse A, B, C und D.

Von einem Verlust der unterbrechungsfreien Stromversorgung (Batterieversorgung) zweier EDSS-Busse eines Moduls, (siehe Abschnitt 7.4.4) ist al Folge anlageninterner Brände in den Batterieräumen des betroffenen Moduls auszugehen, die entsprechenden vier Batterieräume der EDSS-Busse A, B, C und D. von Modul 1.

Brandabschnittübergreifende Brände in den Räumen 411, 507 und 601 führen zu einem Ausfall beider Redundanzen des ESFAS in sechs Modulen. Schließlich ergeben sich noch allgemeine Transienten in allen Modulen in Folge von internen Bränden in anderen Räumen des Kontroll- oder Reaktorgebäudes.

6.4.3 Zusammenfassung

Alle möglichen auslösenden Ereignisse als Folge eines anlageninternen Brandes oder einer anlageninternen Überflutung werden in Tab. 6.3 zusammengefasst.

Tab. 6.3 Mögliche auslösende Ereignisse nach einem anlageninternen Brand oder einer anlageninternen Überflutung

Auslösendes Ereignis	Auslösung durch internen Brand oder interne Überflutung	Begründung
Allgemeine Transiente	Brand, Überflutung	Ein Brand kann eine allgemeine Transiente auslösen, beispielsweise über das fehlerhafte Schließen der MSIV. Während einer internen Überflutung kann eine allgemeine Transiente beispielsweise über das Fehlverhalten einer Pumpe ausgelöst werden.
Fehlausfahren der Steuerstäbe	keine	Ein Brand oder eine Überflutung kann nicht die Steuerstabantriebe so stören, dass es zu einem fehlerhaften Ausfahren der Steuerstäbe kommt.
Ausfall der Stromversorgung /Notstromfall	Brand	Ein Brand oder eine Überflutung kann die elektrischen Versorgungseinrichtungen beschädigen, allerdings besteht kein Überflutungsrisiko in den entsprechenden Räumlichkeiten.
EDSS-Ausfall (mindestens zweier EDSS-Busse)	keine	Ein Brand kann einzelne elektrische Versorgungseinrichtungen beschädigen und zum Ausfall einzelner EDSS-Busse oder der Notstromversorgung mehrerer EDSS-Busse führen. Ein durch einen Brand verursachter gemeinsamer Ausfall zweier EDSS-Busse ist nicht zu erwarten. Es besteht kein Überflutungsrisiko der Räumlichkeiten des EDSS.
Leitungsleck im Sekundärkühlkreis	keine	Ein Brand oder eine Überflutung kann keine Rohrleitungen oder Behälter beschädigen und kann nicht zu einem Leitungsleck führen
Dampferzeugerüberspeisung	keine	Ein Brand oder eine Überflutung kann nicht die Fördermenge der Speisewasserpumpen und damit die Einspeiserate in die Dampferzeuger erhöhen
Überspeisung durch das CVCS	Brand	Ein Brand kann zu einem fehlerhaften Betrieb des CVCS führen. Eine Überspeisung und ein Ansprechen der RSVs könnten folgen. Die Steuerleitungen sind nicht anfällig für Überflutungen.

Auslösendes Ereignis	Auslösung durch internen Brand oder interne Überflutung	Begründung
Ausfall von Komponentenhilfssystemen	Überflutung	Ein Brand kann sich unterschiedlich auf die Hilfssysteme auswirken, allerdings fallen in keinem Szenario alle Hilfssysteme aus. Die Hilfssysteme, insbesondere deren Pumpen, können von einer internen Überflutung betroffen sein.
Leck zwischen Reaktorbecken und Sicherheitsbehälter	keine	Ein Brand oder eine Überflutung kann kein Leck in einem Behälter verursachen; der Sicherheitsbehälter befindet sich eingetaucht im Reaktorbecken
Funktionales Versagen des Naturumlaufs	keine	Ein Brand oder eine Überflutung hat keinen Einfluss auf die Funktionalität des Naturumlaufes
Leck der CVCS-Einspeiseleitung in den Sicherheitsbehälter	keine	Es ist nicht zu erwarten, dass ein Brand oder eine Überflutung zu einem Schaden in Rohrleitungen führt.
Leck der CVCS-Entnahmeleitung in das Reaktorgebäude	keine	Es ist nicht zu erwarten, dass ein Brand oder eine Überflutung zu einem Schaden in Rohrleitungen führt.
Leck der CVCS-Einspeiseleitung in Reaktorgebäude	keine	Es ist nicht zu erwarten, dass ein Brand oder eine Überflutung zu einem Schaden in Rohrleitungen führt.
KMV in den Sicherheitsbehälter	keine	Ein Brand oder eine Überflutung kann keine Rohrleitungen oder Behälter beschädigen und kann nicht zu einem Leitungsleck führen
Dampferzeuger-Bypassleck	keine	Ein Brand oder eine Überflutung kann keine Rohrleitungen oder Behälter beschädigen und kann nicht zu einem Leitungsleck führen
Fehlerhafte Aktivierung des ECCS	Brand	Ein Brand könnte zu einer fehlerhaften Aktivierung des ECCS führen. Diese Steuerleitungen sind nicht anfällig für Überflutungen.
Fall eines Moduls in den Betriebsbereich	keine	Ein Fehlfahren des Reaktorgebäudekrans durch Brandeinfluss ist nach /NUS 20/ ausgeschlossen
Überdruck im kalten RCS – POS2&6	keine	Im Fall eines Brandes oder einer Überflutung wird der An- oder Abfahrvorgang unterbrochen

Als Folge eines anlageninternen Brandes ist mit folgenden auslösenden Ereignissen zu rechnen:

- Allgemeine Transiente (mit zusätzlichen Ausfällen von Komponentenhilfssystemen),
- Überspeisung durch das CVCS,

- Ausfall der Stromversorgung/Notstromfall,
- fehlerhafte Aktivierung des ECCS.

Das gleichzeitige, korrelierte Auftreten eines internen Brandes und eines Ausfalls der externen Stromversorgung bzw. eines Notstromfalls stellt ebenfalls ein auslösendes Ereignis dar.

Im Fall einer internen Überflutung ergeben sich möglicherweise:

- der Ausfall von Komponentenhilfssystemen oder
- eine allgemeine Transiente.

In vielen Anlagenbereichen kann somit ein interner Brand oder eine interne Überflutung zu einem Systemausfall und zur Einleitung der RESA führen. Andernfalls könnte auch das Betriebspersonal das Abfahren aller Module veranlassen. Darüber hinaus könnte eine interne Überflutung im Reaktorgebäude die Einsatzbereitschaft der Kühlmittelaufbereitung der CVCS und des CFDS beeinträchtigen, was sich modulübergreifend auswirkt. Die entsprechenden Systeme sollen deshalb in der Betrachtung einer internen Überflutung im Reaktorgebäude nicht berücksichtigt werden. Weitere modulübergreifende Beeinträchtigungen sind als Folge des Brandes oder der internen Überflutung nicht zu erwarten.

6.5 Ereignisse bei Nichtleistungsbetrieb (Mode 2 bis Mode 5)

Spezifische auslösende Ereignisse für die Nichtleistungsbetrieb sind in der folgenden Tab. 6.4 aufgelistet. Einige auslösende Ereignisse für den Leistungsbetrieb sind auch in den anderen Betriebsphasen relevant, eine Übersicht befindet sich in Abschnitt 6.6.

Tab. 6.4 Ereignisse bei Nichtleistungsbetrieb

Auslösendes Ereignis /NUS 20/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
Mechanische Einwirkungen (Lastabsturz, Handhabungsfehler			
Modul drop in operating area (crane failure) IE-POS3-RBC-DROP-OP-FTS IE-POS5-RBC-DROP-OP-FTS	Brennelement-Handhabungsfehler Absturz schwerer Lasten	Möglicher Schaden an mehreren Modulen	ja
Modul drop in refueling area (crane failure) IE-POS3-RBC-DROP-RF-FTS IE-POS5-RBC-DROP-RF-FTS	Brennelement-Handhabungsfehler ‚Absturz schwerer Lasten	Möglicher Schaden an einem Modul	ja
Kühlmittelverluststörfälle			
Interfacing systems LOCA	Leck in ein angeschlossenes System	Wird durch Leck im CVCS abdeckend berücksichtigt	nein
Pool leakage	Leck am Flutraum/Absetzbecken Ausfall der Nachzerfallswärmeabfuhr (Brennelementwechsel)	Ausfall der UHS; Ausfall der Kühlung bei einem Brennelementwechsel; das Betriebspersonal hat mehr als 72 h Zeit[13] zu reagieren, es stehen Leckpfadsuch-, Isolations- und Wiederbefüllungsmöglichkeiten zur Verfügung	nein

[13] Pro Meter Höhe im Reaktorbecken und den angeschlossenen Becken (Brennelementbecken und Brennelementlagerbecken) stehen 1100 m³ Wasser zur Verfügung. Bei einer Austrittsrate von 20 l/s wäre der Füllstand nach 15 h um 1 m abgesunken /NUS 20d/. Das Leck wird entweder vom Becken-Leckage-Überwachungssystem, vom Beckenkühlsystem des Brennelementlagerbeckens oder Reaktorbeckens oder vom Standortkühlwassersystem entdeckt und das Betriebspersonal alarmiert. Das Betriebspersonal hat die Möglichkeit das Aufbereitungssystem mit drei Pumpen einer Kapazität bis 80 l/s in Betrieb zu nehmen, um den Füllstand des Reaktorbeckens zu halten.

Auslösendes Ereignis /NUS 20/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
Cold overpressurization event	Überdruck im kalten RCS	Verlust der Integrität der druckführenden Umschließung	ja
	Leck am Sicherheitsbehälter	Für den Transport wird der Sicherheitsbehälter befüllt und druckbeaufschlagt, Wärmeübergang und Umlaufrate des Naturumlaufes im RCS werden beeinflusst	ja
Störungen der Wärmeabfuhr (Transienten)			
Loss of subcooling in the riser Failure in the module heat-up system Core flow blockage		Funktionales Versagen des Naturumlaufes im RCS. Temperaturanstieg im Kern	ja
Forced flow transients during stable startup		Keine Einspeisung durch das CVCS; abgedeckt durch Leck im CVCS	nein
Loss of Offsite Power, Loss of AC Power to station auxiliaries EHVS-LOOP	Notstromfall (extern oder intern)	Nachzerfallswärmeabfuhr über den gefluteten Sicherheitsbehälter in das Reaktorbecken	ja
Loss of Direct Current EDSS-LODC-ET		Kontrolle über Reaktor aus Kontrollraum nicht möglich, Nachzerfallswärmeabfuhr über den gefluteten Sicherheitsbehälter in das Reaktorbecken	ja
Inadvertent actuation of the decay heat removal system	Fehlerhafte Anregung der Notkühlsignale	Wärmeverlust über den Sicherheitsbehälter in das Reaktorbecken	nein

Auslösendes Ereignis /NUS 20/	Auslösendes Ereignis aus /FAK 05/ und /FAK 16/	Auswirkungen	Zu untersuchen?
Reaktivitätsstörungen (Deborierungen, Kritikalitätsereignisse)			
Inadvertent deboration	Lecks aus Deionat führenden Systemen Fehlerhaft Deionat im Nachkühlsystem Entborieren beim Anheben des Füllstands Fehler beim Borieren zum Abfahren Fehlerhaftes Entborieren beim Anfahren nach Ausfall aller Hauptkühlmittelpumpen	Leistungsanstieg, RESA; dieses Ereignis wird abdeckend durch „Fehlausfahren der Steuerstäbe“ untersucht	nein
Ecxessive rod or rod-group withdrawal, control rod ejection	Fehlausfahren der Steuerstäbe	Leistungsanstieg, RESA	ja
Failure of control rods to insert	Ausfall der RESA	Boreinspeisung; der Ausfall der RESA oder auch der generelle Ausfall der Kernabschaltung führt zu einem konstanten Weiterbetrieb der Anlage	nein
	Beladefehler	Schieflast bei Anfahren, RESA; dieses Ereignis wird abdeckend durch „Fehlausfahren der Steuerstäbe“ untersucht	nein

Folgende Ereignisse sollen weiter untersucht werden:

- Fall eines Moduls in den Betriebs- oder Beladebereich, siehe Abschnitt 7.6.1,
- Überdruck im kalten RCS, siehe Abschnitt 7.6.2),
- Ausfall der externen Stromversorgung, siehe Abschnitt 7.4.3,
- EDSS-Ausfall, siehe Abschnitt 7.4.4,
- Leck zwischen Reaktorbecken und Sicherheitsbehälter, siehe Abschnitt 7.4.9,
- Funktionales Versagen des Naturumlaufes siehe Abschnitt 7.4.10,
- Fehlausfahren der Steuerstäbe, siehe Abschnitt 7.4.2.

6.6 Zu untersuchende auslösende Ereignisse

Die verschiedenen POS sind in Abschnitt 6.1 beschrieben. Die folgenden Phasen des Nichtleistungsbetriebs: unterscheiden sich wesentlich:

- POS1: Hier werden das RTS und das CVCS benötigt.
- POS3 und 5: Hier wird der Kran für die Bewegung der Brennelemente verwendet.
- POS7: Hier wird der Kern wieder kritisch gefahren.

Das Spektrum der zu untersuchenden auslösenden Ereignisse ist in Tab. 6.5 dargestellt. Die Spalte POS1 umfasst dabei Mode 2, Mode 3 und Mode 5 POS1. Auslösende Ereignisse mit Relevanz für POS1, POS3, POS5 und POS7 nach Tab. 6.5 sind auch für Mode 2 bis Mode 5 (alle POS) relevant.

Tab. 6.5 Auslösende Ereignisse für unterschiedliche Anlagenbetriebszustände

Auslösendes Ereignis		Anlagenbetriebszustände			
		LB	NLB Modes 2 bis 5[14]		
			POS1&6[15]	POS2-5	POS7
Transienten und Reaktivitätsstörfälle					
TA	Allgemeine Transiente	X			
RS	Fehlausfahren der Steuerstäbe	X			X
TN	Ausfall der externen Stromversorgung	X	X	X	X
TD	EDSS-Ausfall	X	X	X	X
TS	Leitungsleck im Sekundärkühlkreis	X	X		X
TÜ	Dampferzeuger-Überspeisung	X			
TH	Überspeisung durch das CVCS	X	X		X
TV	Ausfall von Komponentenhilfssystemen	X	X		X
TL	Leck zwischen Reaktorbecken und Sicherheitsbehälter	X	X	X	X
TF	Funktionales Versagen des Naturumlaufes	X	X	X	X
Kühlmittelverluststörfälle					
LC	Leck der CVCS-Einspeiseleitung in den Sicherheitsbehälter	X	X		X
LR	Leck der CVCS-Entnahmeleitung in das Reaktorgebäude	X	X		X
LE	Leck der CVCS-Einspeiseleitung in das Reaktorgebäude	X	X		X
LP	KMV in den Sicherheitsbehälter	X	X		X
LH	Dampferzeuger-Bypassleck	X	X		X
LV	Fehlerhafte Aktivierung des ECCS	X	X		X
Ereignisse bei Nichtleistungsbetrieb					
NF	Fall eines Moduls – POS3&5			X	
NÜ	Überdruck im kalten RCS – POS2&6			X	
Übergreifende Einwirkungen von innen					
IB-	*Interner Brand*	X	X	X	X
TA	Allgemeine Transiente	X			X
TN	Ausfall der Stromversorgung	X	X	X	X
TH	Überspeisung durch das CVCS	X	X		X

[14] Sind alle Unterspalten belegt, so ist das auslösende Ereignis relevant in allen Modes und allen POS für Mode 5.

[15] Dies umfasst die NLB-Modes 2, 3 und Mode 5 POS 1 und 6.

Auslösendes Ereignis		Anlagenbetriebszustände			
		LB	NLB Modes 2 bis 5[14]		
			POS1&6[15]	POS2-5	POS7
LV	Fehlerhafte Aktivierung des ECCS	X	X		X
IÜ-	*Interne Überflutung*	X	X	X	X
TA	Allgemeine Transiente	X			
TV	Ausfall von Komponentenhilfssystemen	X	X		X

6.7 Eintrittshäufigkeiten der auslösenden Ereignisse

Die Eintrittshäufigkeiten der auslösenden Ereignisse gehen größtenteils auf die entsprechenden Werte in /NUS 20/ zurück und sind in Tab. 6.6 aufgeführt. Ereignisse während der Betriebsphasen Mode 2, 3 und 4 werden mit den Ereignissen im Leistungsbetrieb zusammen berücksichtigt. In Mode 5 sind die Betriebsdauern für POS1, POS6 und POS7 mit jeweils ca. 7 h pro Jahr gering (Häufigkeiten 8 E-04 pro Jahr). Diese Betriebsphasen gleichen dem Leistungsbetrieb, allerdings befinden sich die Abschaltstäbe in POS1 und POS6 im Kern, eine RESA wäre im Störfallablauf nicht notwendig. Dieses Detail soll in der Analyse der Einfachheit halber nicht berücksichtigt werden, und POS1, POS6 und POS7 werden zusammen mit dem Leistungsbetrieb betrachtet.

Die Betriebsphasen POS2 bis POS5 machen zusammen eine Häufigkeit von 1,2 E-02 pro Jahr aus. Der Ausfall der externen Stromversorgung, ein EDSS-Ausfall, ein funktionales Versagen des Naturumlaufes und ein Leck zwischen Sicherheitsbehälter und Reaktorbecken sollen für diese Fälle spezifisch angepasst untersucht werden. Die auslösenden Ereignisse ‘Fall eines Moduls in den Betriebsbereich‘ und ‘Überdruck im kalten RCS‘ können in den Betriebsphasen POS3 und POS5 bzw. POS2 und POS6 vorkommen.

Tab. 6.6 Eintrittshäufigkeiten der wichtigsten auslösenden Ereignisse

Auslösendes Ereignis		Eintrittshäufigkeit pro Jahr		
		LB	NLB, Mode 5 POS2 – POS6	Quelle
Transienten und Reaktivitätsstörfälle				
TA	Allgemeine Transiente	1,3 E+00	–	/NUS 20/
RS	Fehlausfahren der Steuerstäbe	2,0 E-04[16]	–	/ALR 22/
TN	Ausfall der externen Stromversorgung	2,2 E-02[17]	2,7 E-04	/NUS 20/, /DOY 21/
TD	EDSS-Ausfall	4,7 E-05	5,8 E-07	/NUS 20/
TS	Leitungsleck im Sekundärkühlkreis	4,4 E-05	–	/NUS 20/
TÜ	Dampferzeuger-Überspeisung	1,0 E-05	–	/LIN 01/
TH	Überspeisung durch das CVCS	1,0 E-05	–	Abschätzung
TV	Ausfall von Komponentenhilfssystemen	1,6 E-02	–	/NUS 20/
TL	Leck zwischen Reaktorbecken und Sicherheitsbehälter	1,0 E-07	1,2 E-09	Abschätzung
Kühlmittelverluststörfälle				
LC	Leck der CVCS-Einspeiseleitung in den Sicherheitsbehälter	1,4 E-04	–	/NUS 20/
LR	Leck der CVCS-Entnahmeleitung in das Reaktorgebäude	1,4 E-04	-	/NUS 20/
LE	Leck der CVCS-Einspeiseleitung in das Reaktorgebäude	2,8 E-04	–	/NUS 20/
LP	KMV in den Sicherheitsbehälter	2,0 E-03	–	/NUS 20/
LH	Dampferzeuger-Bypassleck	4,5 E-05	–	/NUS 20/
LV	Fehlerhafte Aktivierung des ECCS	1,1 E-05	–	/NUS 20/

[16] Eine alternative Eintrittshäufigkeit für das Fehlausfahren der Steuerstäbe (uncontrolled CRA withdrawal) ergäbe sich aus /NUS 20b/: „Ein Fehlausfahren der Steuerstäbe (Englisch: wird ein- oder mehrmalig während des Reaktor-Lebenszyklus (60 Jahre) erwartet." – dies entspräche einer Eintrittshäufigkeit von 1,7 E-02 pro Jahr – diese Abschätzung wird als konservative Annahme betrachtet und deshalb alternativ ein Literaturwert verwendet. Das Fehlausfahren der Steuerstäbe ist abdeckend für alle Reaktivitätsstörfälle mit eingebrachter Reaktivität (reactivity insertion accident).

[17] Für den Ausfall der Stromversorgung werden vier Fälle unterschieden, ein technischer Ausfall im externen Stromnetz, ein wetterbedingter Ausfall im externen Stromnetz, ein Ausfall des Umspannwerkes und ein Ausfall aufgrund eines anlageninternen Fehlers, /DOY 20/, /DOY 21/. Die wetterbedingten und technischen Ausfälle im Stromnetz (die Ausfallhäufigkeiten sind standortabhängig, 2,0 E-02 pro Jahr nach /DOY 21/, 6,5 E-03 pro Jahr nach /DOY 20/) können durch die Umschaltung auf den Inselbetrieb (Lastabwurf auf Eigenbedarf) beherrscht werden und eine mögliche Netzstromwiederherstellung kann in der Unfallanalyse berücksichtigt werden. In den anderen Fällen erfolgt eine Umschaltung auf Notstromversorgung (Notstromfall) und eine Abschaltung aller Module. Hierfür wird der Wert 1,3 E-02 für die Versagenshäufigkeit des Umspannwerkes verwendet, aus /DOY 21/, und 1,8 E-03 für den kraftwerksinternen übergreifenden Stromausfall, /DOY 20/.

Auslösendes Ereignis		Eintrittshäufigkeit pro Jahr		
		LB	NLB, Mode 5 POS2 – POS6	Quelle
Ereignisse bei Nichtleistungsbetrieb				
NF	Fall eines Moduls – POS3&5	–	1,1 E-07	/NUS 20/
NÜ	Überdruck im kalten RCS – POS2&6	–	1,2 E-07	Abschätzung
Übergreifende Einwirkungen von innen				
IB-	*Interner Brand*			
TA	Allgemeine Transiente	1,0 E±00	–	/NUS 20/
TN	Ausfall der Stromversorgung[18]	6,5 E-02	7,8 E-04	/NUS 20/
TH	Überspeisung durch das CVCS	6,0 E-02	–	/NUS 20/
LV	Fehlerhafte Aktivierung des ECCS	9,6 E-03	–	/NUS 20/[19]
IÜ-	*Interne Überflutung*			
TA	Allgemeine Transiente	3,2 E-02	–	/NUS 20/
TV	Ausfall von Komponentenhilfssystemen	1,9 E-02	–	/NUS 20/

Die Unsicherheit der Eintrittshäufigkeiten wird analog zur Vorgehensweise von NuScale /NUS 20/ über eine Lognormal-Verteilung mit einem Fehlerfaktor von EF = 10 modelliert.

[18] Der Ausfall der Stromversorgung nach einem internen Brand ist auch Teil der PSA deutscher Anlagen, hier ergibt sich eine ähnliche Eintrittshäufigkeit für einen Ausfall der Stromversorgung aus einem Brand im Schaltanlagengebäude

[19] Die in der Quelle angegebenen auslösenden Ereignisse beziehen sich auf Brände in Abschnitten mit ECCS-Equipment. Die Häufigkeit der Brände ist mit 1,0 E-01 pro Jahr angegeben. Für die Auslösung des ECCS sind allerdings zusätzlich die Brandausbreitung über die gesamten Räume (Wahrscheinlichkeit 0,5) und die wärmebedingte Fehlauslösung eines ECCS-Auslöseventils erforderlich (Wahrscheinlichkeit 0,154).

7 Ereignisablaufanalysen, Mindestwirksamkeiten der Systemfunktionen und Zeitbudgets der Handmaßnahmen

Alle identifizierten auslösenden Ereignisse können durch den Einsatz von Systemfunktionen beherrscht werden, d. h. es ergibt sich dann auslegungsgemäß keinen Kernschadenszustand. Der Ausfall von Systemfunktionen kann zu Ereignisabläufen führen, die unbeherrscht sind und damit einen Kernschaden zur Folge haben.

7.1 Automatische Schutzeinrichtungen zur Störfallbeherrschung

Der Reaktorschutz (Module Protection System) überwacht viele wichtige Betriebsparameter. Unter Störungsbedingungen werden dabei Grenzwerte erreicht (Reaktorschutzkriterien), die automatisch Aktivitäten im System auslösen. Die Auslösebedingungen und die angesprochenen Systemfunktionen aus /NUS 20a/ sind in Tab. 7.1 dargestellt. Ein Sicherheitsbehälterabschluss führt zur Schließung aller CIVs durch das Sicherheitsbehälterabschlusssystem (Englisch: containment isolation system, CIS) und damit zu Absperrungen der nachfolgend aufgeführten Systeme, die allerdings nur das betrachtete Modul betreffen:

- das CFDS,
- das Sicherheitsbehälter-Vakuumsystem (Englisch: containment evacuation system, CES),
- die Komponentenkühlung der Komponenten des RCS,
- das CVCS (CVCS-Abschluss) sowie
- die Dampferzeuger (Dampferzeuger-Abschluss).

Der CVCS-Abschluss des betroffenen Moduls beinhaltet die Absperrung der CIV bzgl. der CVCS-Einspeiseleitung, der CVCS-Entnahmeleitung, der CVCS-Sprühleitung und der RCS-Entgasungsleitung. Der Dampferzeuger-Abschluss löst die Schließung der Ventile MSIV, MSIV-Bypassventil, Backup-MSIV, Backup-MSIV-Bypassventil, FWIV und Speisewasser-Regelventil aus. Der Abschluss des Deionatsystems (bzgl. des betroffenen Moduls) könnte für ATWS und Störfälle mit sinkender Borsäure im Primärkühlkreislauf (Reaktivitätsstörfälle) von Bedeutung sein, da als Folge dem RCS-Kühlmittel im CVCS kein Deionat mehr zugeführt wird. Nahezu alle RESA-Ereignisse führen auch zum Abschalten des Deionatsystems. Die einzige Ausnahme besteht für Drücke im RCS zwi-

schen 110 bar und 119 bar und gleichzeitiger RCS-Temperatur unter 316 °C. Zusätzlich liegt die Auslöseschwelle für den Deionatabschluss bei einer höheren Mindestdurchflussrate im Primärkühlkreislauf als die Schwelle für die Auslösung der RESA. Weitere automatische Signale sind für das Auslösen der Sprödbruchabsicherung des RCS bei niedrigen Temperaturen (Englisch: low temperature overpressure protection, LTOP) vorgesehen. Die Auslöseschwelle hängt in diesem Fall von der aktuellen Temperatur im RCS ab.

Tab. 7.1 Automatische Auslösung von Sicherheitsfunktionen durch das ESFAS

Prozessgröße	Auslösebedingung	Ansprechende Systemfunktionen
Reaktorleistung	Anfahrbetrieb: > 25 % der Nominalleistung Leistungsbetrieb: > 120 % der Nominalleistung	RESA, Deionatabschluss
Änderung der Reaktorleistung	> 15 % der Nominalleistung pro Minute	RESA, Deionatabschluss
Druck im RCS, Betriebsdruck ca. 128 bar	> 138 bar	RESA, DHRS, Dampferzeugerabschluss, Deionatabschluss, Abschaltung der Druckhalterheizung
	< 119 bar	RESA, Deionat-Abschluss (falls die Temperatur im Primärkühlkreislauf über 316 °C)
	< 110 bar	RESA, Dampferzeugerabschluss, CVCS-Abschluss, Deionatabschluss
	< 55 bar	ECCS (wird verhindert, falls die Temperatur im Primärkühlkreislauf < 246 °C oder Druck im Sicherheitsbehälter < 0,07 bar)
Sicherheitsbehälterdruck, Betriebsdruck maximal 0,2 bar	> 0,66 bar	RESA, Sicherheitsbehälterabschluss, Deionatabschluss
Temperatur im RCS, typische mittlere Temperatur ca. 285 °C	> 321 °C	RESA, DHRS, Dampferzeugerabschluss, Deionatabschluss, Abschaltung der Druckhalterheizung

Prozessgröße	Auslösebedingung	Ansprechende Systemfunktionen
Füllstand im Druckhalter, im Betrieb ungefähr 60 %	> 80 % der max. Höhe	RESA, CVCS-Abschluss, Deionatabschluss
	< 35 % der max. Höhe	RESA, Deionatabschluss, Abschaltung der Druckhalterheizung
	< 20 % der max. Höhe	Sicherheitsbehälterabschluss
Frischdampfdruck, Betriebsdruck ca. 34 bar	> 55 bar	RESA, DHRS, Dampferzeugerabschluss, Deionatabschluss, Abschaltung der Druckhalterheizung
	< 21 bar (erfüllt für einen Leistungsbetrieb > 15 % der Nominalleistung)	RESA, Dampferzeugerabschluss, Deionatabschluss
	< 1,4 bar	RESA, Dampferzeugerabschluss, Deionat-Abschluss
Frischdampfüberhitzung	> 83 K < 0 K	RESA, Dampferzeugerabschluss, Deionatabschluss
Durchflussrate im RCS, Betriebsrate ungefähr 760 l/s	< 48 l/s	Deionatabschluss
	< 0 l/s	RESA, CVCS-Abschluss, Deionatabschluss
Batterieladespannung	< 80 % der normalen ELVS-Spannung für mehr als 60 s	RESA, DHRS, Sicherheitsbehälterabschluss, Deionatabschluss, Abschaltung der Druckhalterheizung
	< 80 % der normalen ELVS-Spannung für mehr als 24 h	ECCS
Temperatur unter dem Bioshield	> 121 °C	RESA, Sicherheitsbehälterabschluss, Deionatabschluss
Wasserstand im Sicherheitsbehälter	> 6,4 m (+/- 0,3 m)	ECCS (wird verhindert, falls Temperatur im Primärkühlkreislauf < 177 °C und Füllstand im Druckhalter > 20 %)
Stromversorgung über modulspezifische EDSS-Busse	Verlust von beiden EDSS-Bussen einer Redundanz (Auslösung unabhängig vom ESFAS)	RESA, DHRS, ECCS, Sicherheitsbehälterabschluss /NUS 20/

7.2 Systemfunktionen und Mindestwirksamkeiten

Zur Beherrschung der auslösenden Ereignisse können Systemfunktionen nach Tab. 7.2 angefordert werden. In den Unterkapiteln sind die Systemfunktionen näher beschrieben und deren Mindestwirksamkeiten angegeben.

Tab. 7.2 Übersicht über die automatischen Systemfunktionen und Handmaßnahmen zur Störfallbeherrschung

System-funktion	Titel	Kapitel	Mindestwirksamkeit	Quelle
RESA-SF1	Durchführung der RESA	7.2.1	14 der 16 Steuerstabelemente fallen vollständig ein.	/NUS 20/
DHRS-SF1	Nachzerfallswärmeabfuhr über das DHRS	7.2.2	#1: Beide Redundanzen erreichen Mindestperformance	/NUS 20/
			#2: Eine der beiden Redundanzen erreicht Mindestperformance.	/NUS 20/
			#3: Die nicht-betroffene Redundanz erreicht Mindestperformance.	/NUS 20/
RSV-SF1	Dampfabgabe über die RSVs	7.2.3	#1: Ein RSV öffnet anforderungsgemäß (bei 143 bar bzw. 145 bar im RCS).	/NUS 20/
			#2: Die geöffneten RSVs schließen wieder (bei ca. 130 bar im RCS).	/NUS 20/
DE-SF1	Absperrung eines Dampferezeuger-Bypasslecks	7.2.4	Vollständiger Frischdampf- und Speisewasserabschluss des betroffenen Dampferzeugers	/NUS 20/
LTOP-SF1	Druckentlastung des RCS bei niedrigen Temperaturen	7.2.5	Eines der drei RVVs öffnet vollständig und zeitnah.	/NUS 20c/
ECCS-SF1	Notkühlung über RVV und RRV	7.2.6	Ein RVV und ein RRV öffnen vollständig und anforderungsgemäß.	/NUS 20/
IAB-SF1	Blockierung aller ECCS-Ventile über den IAB	7.2.7	Alle fünf ECCS-Ventile bleiben über den IAB bis zum Abbau des Druckunterschiedes zwischen Sicherheitsbehälter und RCS ($\Delta p > 69$ bar) geschlossen.	/NUS 20e/

System-funktion	Titel	Kapitel	Mindestwirksamkeit	Quelle
CVCS-SF1	Absperrung der CVCS-Einspeise-leitung	7.2.8	Leckdetektion und automatisches zeitnahes Schließen eines CVCS-CIV	/NUS 20/
CVCS-SF2	Absperrung der CVCS-Entnahme-leitung	7.2.8	Leckdetektion und automatisches zeitnahes Schließen eines CVCS-CIV	/NUS 20/
CVCS-HM1	Wiederbespeisung des RCS durch das CVCS	7.2.9	#1: Dauerhafte Einspeisung von borangereichertem Kühlmittel über eine CVCS-Aufbereitungspumpe	/NUS 20/
			#2: Kurzzeitige Druckhalter-sprühung mit einer CVCS-Aufbereitungspumpe	/NUS 20/
CVCS-HM2	Deionat-Abschluss oder Verhinderung einer dauerhaften RCS-Überspeisung	7.2.10	Deionat-Abschluss über ein Absperrventil, manuelle Abschaltung der fehlerhaft einspeisenden CVCS-Aufbereitungspumpen oder das Schließen manueller Armaturen	Eigene Abschätzung
CFDS-HM1	CFDS-Fluten des Sicherheitsbehälters	7.2.11	Eine CFDS-Pumpe wird innerhalb von einigen Minuten auf das betroffene Modul durchgeschalten und füllt dessen Sicherheitsbehälter.	/NUS 20/, zeitliche Anforderung abgeschätzt
CFDS-HM2	CFDS-Drainage des Sicherheitsbehälters	7.2.12	Eine CFCS-Pumpe wird zur Drainage dauerhaft auf das betroffene Modul geschalten und das CES erzeugt einen Überdruck im Sicherheitsbehälter.	Eigene Abschätzung
ELVS-HM1	Notstrom über Gasturbinen-generator oder Dieselgeneratoren	7.2.13	Gasturbine oder beide Dieselgeneratoren erzeugen dauerhaft (72 h) Notstrom und sind mit dem EHVS bzw. ELVS verbunden.	/NUS 20/
EHVS-HM1	Wiederherstellung der externen Stromversorgung	7.2.14	Die externe Stromversorgung wird innerhalb 24 h wiederhergestellt.	/NUS 20/
KRAN-HM1	Modulöffnung	7.2.15	Das Modul wird innerhalb von 5 h geöffnet.	Eigene Abschätzung
KRAN-HM2	Brennelement-entnahme	7.2.15	Einzelne Brennelemente werden innerhalb von 3 h entfernt.	Eigene Abschätzung

7.2.1 Durchführung der Reaktorschnellabschaltung – RESA-SF1

Die RESA, durchgeführt vom RTS, ist dann erfolgreich, wenn mindestens 14 der 16 Steuerstabelemente[20] innerhalb einer vorgegebenen Zeitspanne vollständig in den Kern eingefallen sind /NUS 20/. Der Ausfall der beiden Abschaltstäbe mit der höchsten Reaktivität ist dabei möglich, ohne den Erfolg der Systemfunktion zu verhindern.

7.2.2 Nachzerfallswärmeabfuhr über das DHRS – DHRS-SF1

Für das DHRS gibt es verschiedene Mindestanforderungen. In einigen Ereignisabläufen ergibt sich eine Störfallbeherrschung direkt über die Verfügbarkeit beider Redundanzen des DHRS im Erfolgspfad der Alternative 1. Der Ausfall einer Redundanz des DHRS, Alternative 2, führt typischerweise im weiteren Störfallverlauf zu einem Ansprechen der RSVs. Fällt aufgrund des auslösenden Ereignisses eine Redundanz des DHRS aus, z. B. Dampferzeuger-Bypassleck, so ist die Mindestanforderung, dass das DHRS im nicht betroffenen Dampferzeuger läuft, Alternative 3.

Die Mindestanforderungen an eine Redundanz des DHRS sind:

- Öffnen mindestens eines der beiden DHRS-Auslöseventile;
- Erfolgreicher Abschluss des Dampferzeugers (Frischdampf- und Speisewasser-Abschluss);
- Nach der letzten Wartung erfolgte Entlüftung des DHRS;
- Erfolgreiche Initiierung des DHRS durch automatische Aktivierung oder manuelle Aktivierung aus der Warte;
- Erreichen einer stabilen Mindestumlaufrate des Naturumlaufes zur ausreichenden Wärmeabfuhr nach einer kurzen Einschwingphase. Dafür muss u. a. das Reaktorbecken als Not- und Nachwärmesenke verfügbar sein.

[20] Nach Angaben in /NUS 20k/ gibt es eine Unterteilung in Steuer- und Abschaltelemente (regulating bank und shutdown bank) mit jeweils acht Steuerstabelementen (control rod assemblies). Im Falle einer RESA werden nur die Abschaltelemente verwendet („*The shutdown bank is used in the event of a reactor trip and to maintain the reactor shutdown*“/NUS 20k). Der Einfall von 7 der 8 Abschaltelementen reicht nach Angaben in /NUS 20k/ aus, um den Kern abzuschalten.

7.2.3 Dampfabgabe über die Reaktorsicherheitsventile – RSV-SF1

Zur Verhinderung eines HD-Versagens der druckführenden Umschließung des RCS ist in einigen Ereignisabläufen eine Dampfabgabe über die RSVs notwendig. Vereinfachend wird davon ausgegangen, dass die RSVs bei Ausfall eines DHRS immer aufgrund von Druckspitzen oder kontinuierlichen Druckanstiegen angefordert werden. Öffnet mindestens eines der beiden RSVs im Störfallablauf ordnungsgemäß bei 143 bar bzw. 145 bar, dann ist damit ein erwünschter Druckabbau im RCS verbunden, Erfolgspfad für die Alternative 1. Für eine effiziente Funktion des DHRS müssen die RSVs bei einem reduzierten Druck von ca. 130 bar wieder schließen, damit der RCS insgesamt druckbeaufschlagt bleibt. Eine erfolgreiche Dampfabgabe über die RSVs ist mit der ein- oder mehrmaligen Öffnung mindestens eines der beiden RSVs verbunden, Alternative 2.

7.2.4 Absperrung eines Dampferzeuger-Bypasslecks – DE-SF1

Die Absperrung des Dampferzeuger-Bypasslecks ist erfolgreich, wenn der Dampferzeugerabschluss erfolgreich initiiert (automatisch oder durch die Betriebsmannschaft) und durchgeführt wird. Der Dampferzeugerabschluss des betroffenen Dampferzeugers besteht aus den FW- und den Speisewasser-Abschlüssen (über MSIV oder Backup-MSIV bzw. FWIV, Speisewasser-Regelventil oder Speisewasser-Rückschlagventile).

7.2.5 Druckentlastung des Reaktorkühlsystems bei niedrigen Temperaturen – LTOP-SF1

Im Fall eines Überdrucks des RCS bei niedrigen Temperaturen wird LTOP ausgelöst, wenn mindestens zwei der vier Drucksensoren den Überdruck im RCS messen und die Kühlmitteltemperatur im RCS richtig bestimmt wird (der zulässige Maximaldruck im RCS ist dabei eine temperaturabhängige Funktion). Die Druckentlastung ist erfolgreich, wenn die RVVs automatisch zeitnah angefordert werden und mindestens eines der drei RVVs aufgrund der Anforderung öffnet.

7.2.6 Notkühlung über die Notkühlsystem-Abblaseventile und die Notkühlsystem-Rücklaufventile – ECCS-SF1

Die Notkühlung ist erfolgreich, wenn mindestens eines der drei RVVs[21] und mindestens eines der beiden RRVs öffnen, Alternativen 1 und 2. Alternative 1 beschreibt die Anforderung im Fall eines bereits druckentlasteten RCS. Die Anforderung des ECCS erfolgt automatisch oder über die Betriebsmannschaft. Darüber hinaus muss der Naturumlauf zwischen RDB und Sicherheitsbehälter in Gang kommen und eine gewisse Mindestumlaufrate erzielt werden. Alternative 3 beschreibt die Mindestanforderung für eine Druckentlastung des RCS, dem Öffnen mindestens eines ECCS-Ventils, wobei die Notkühlung nicht erfolgreich zustande kommt (z. B. aufgrund eines Ausfalls des Naturumlaufes, dem Ausfall beider RRVs oder aller drei RVVs).

7.2.7 Blockieren aller Ventile der Notkühlung über den Schutz vor unbeabsichtigter Aktivierung – IAB-SF1

Das ECCS bietet eine Schutzfunktion vor unbeabsichtigter Aktivierung, das IAB. Löst das ECCS automatisch aus oder wird manuell bei Druckdifferenzen von über 90 bar zwischen RCS und Sicherheitsbehälter ausgelöst (z. B. im Normalbetrieb: 125 bar im RCS, 0 bar im Sicherheitsbehälter), so blockieren alle ECCS-Ventile. Der IAB ist erfolgreich, wenn alle fünf Ventile im Druckbereich > 125 bar nicht öffnen und erst nach Druckabbau ab ca. 69 bar Druckunterschied die RRVs bzw. ab ca. 62 bar die RVVs öffnen.

7.2.8 Absperrung der Einspeiseleitung und Entnahmeleitung des Volumenregelsystems – CVCS-SF1 und CVCS-SF2

Die Absperrung der CVCS-Einspeiseleitung bzw. -Entnahmeleitung ist erfolgreich, wenn das CIV der CVCS-Einspeiseleitung bzw. -Entnahmeleitung verfügbar ist und automatisch von der Lecküberwachungsinstrumentierung oder der Betriebsmannschaft aktiviert wird. Übersteigt die Differenzdurchflussrate (gemessen über Durchflusssensoren in den Leitungen) zwischen Einspeisung (CVCS-Einspeiseleitung und CVCS-Sprühleitung) und Entnahme (CVCS-Entnahmeleitung) eine festgelegte Differenz, so werden die CVCS-Einspeiseleitung (und damit auch die CVCS-Sprühleitung) und die CVCS-Entnahmeleitung automatisch gemeinsam abgesperrt. Die Absperrung kann auch durch

[21] Bedingung ist nach /NUS 20/ das erfolgreiche Öffnen nur eines RVV, obwohl für eine vollständige Nachzerfallswärmeabfuhr laut /NUS 20e/ zwei RVVs notwendig sind.

das Betriebspersonal über einen Sicherheitsbehälter-Abschluss veranlasst werden. Das Betriebspersonal wird neben der Alarmierung über die Lecküberwachungsinstrumentierung auch über hohe Strahlungswerte der abgepumpten Gase aus dem Sicherheitsbehälter alarmiert (im Fall eines KMV in den Sicherheitsbehälter) /NUS 20d/.

7.2.9 Wiederbespeisung des Reaktorkühlsystems durch das CVCS – CVCS-HM1

Das RCS kann nach Kühlmittelverlusten über das CVCS wieder befüllt werden (ein CVCS pro Modul). Eine erfolgreiche Wiederbespeisung setzt die Verfügbarkeit von elektrischer Energie (ELVS und mindestens einer von vier EDSS-Busse) und einer CVCS-Aufbereitungspumpe (zwei Pumpen vorhanden) voraus. Eine Handmaßnahme durch die Betriebsmannschaft ist notwendig, um die Sicherheitsbehälter- und Deionat-Abschlüsse rückgängig zu machen und mindestens eine CVCS-Aufbereitungspumpe in Betrieb zu nehmen. Eine Wiederbespeisung durch das CVCS ist erfolgreich, wenn die Betriebsmannschaft innerhalb eines maximalen Zeitbereichs die Handmaßnahme durchführt, mindestens eine CVCS-Aufbereitungspumpe, das Deionatsystem, das Boreinspeisesystem und die CVCS-Einspeiseleitung (oder die CVCS-Sprühleitung) zur Verfügung stehen.

Wird die Absperrung des Deionatsystems nicht rückgängig gemacht, so steht nur das Boreinspeisesystem (ein System für alle zwölf Module) mit maximal 95 m³ boriertem Kühlmittel zur Verfügung. Dieses Kühlmittelreservat reicht nicht für die Mindestanforderung der Maßnahme. Alternative 2 stellt etwas geringere Anforderungen (weniger Kühlmittel erforderlich, und die Pumpen werden nicht 72 h lang benötigt), da in einem solchen Anwendungsfall nur zeitweise in den Druckhalter gesprüht werden muss, um eine Überdruckversagen des RCS zu verhindern.

7.2.10 Deionat-Abschluss oder Verhinderung einer dauerhaften RCS-Überspeisung – CVCS-HM2

Die Absperrung des Deionatsystems ist erfolgreich, wenn das Schließen eines der beiden modulspezifischen Deionatabsperrventilen gelingt. Es wird angenommen, dass ein erfolgreicher Deionatabschluss die maximale Kühlmitteleinspeisemenge auf die gelagerten Kühlmittelmengen im Boreinspeisesystem begrenzt und keine weiteres Borgemisch angerührt wird. Das vollständige Auffüllen des Sicherheitsbehälter über das CVCS und damit ein mögliches Überdruckversagen kann damit verhindert werden. Die Absperrung

des Deionatsystems stellt die automatische Systemfunktion dar, die zur Störfallbeherrschung angefordert wird. Alternativ stehen der Betriebsmannschaft verschieden Möglichkeiten der Verhinderung einer dauerhaften Überspeisung zur Verfügung, beispielsweise über eine Änderung der Ventilstellung des CVCS-Dreiwegeventils oder die manuelle Außerbetriebnahme der CVCS-Aufbereitungspumpen oder das Stromloschalten der ELVS-Stromschienen. Aufgrund der vielen Möglichkeiten, die sich der Betriebsmannschaft bieten, soll für die Verhinderung der dauerhaften Überspeisung nur der menschliche Fehler berücksichtigt werden.

7.2.11 Fluten des Sicherheitsbehälter – CFDS-HM1

Das CFDS-Fluten (eine Redundanz des CFDS für sechs Module, nur der Sicherheitsbehälter eines Moduls kann gleichzeitig geflutet werden) des Sicherheitsbehälter ist erfolgreich, wenn eine der beiden CFDS-Pumpen zur Verfügung steht, die Maßnahme rechtzeitig von der Betriebsmannschaft eingeleitet wird, der Druck im Sicherheitsbehälter vor dem Fluten nicht zu hoch ist (wenige bar) und das entsprechende CIV anforderungsgemäß öffnet. Darüber hinaus muss das Reaktorbecken als Not- und Nachwärmesenke verfügbar sein. Das CFDS-Fluten des Sicherheitsbehälter ist eine Handmaßnahme. Die CIV werden nach dem Flutungsvorgang von der Betriebsmannschaft wieder geschlossen und die CFDS-Pumpe ausgeschaltet /NUS 20d/.

7.2.12 Drainage des Sicherheitsbehälter – CFDS-HM2

Nach einem kleinen Leck zwischen Reaktorbecken und Sicherheitsbehälter ist eine CFDS-Drainagefunktion erfolgreich, wenn die Durchführung der Handmaßnahme vor der Auslösung des ECCS durchgeführt und damit der Sicherheitsbehälter dauerhaft entwässert wird. Das CIV des CFDS muss dazu geöffnet werden. Die Mindestanforderung an die Handmaßnahme ist die Verfügbarkeit des Modulkontrollsystems, des nuklearen Drainagesystems und der erfolgreichen Inbetriebnahme einer der beiden CFDS-Pumpen. Das Kühlmittel wird über die Pumpen in das nukleare Drainagesystem gefördert. Der notwendige Sicherheitsbehälter-Druck zur Verhinderung der Kavitation in den CFDS-Pumpen (Kreiselpumpen) erfordert zusätzlich die erfolgreiche Inbetriebnahme des CES und das Öffnen der CES-CIV. Der Sicherheitsbehälter wird dann über eine CES-Pumpe leicht druckbeaufschlagt, was eine Kavitation der CFDS-Pumpen verhindert.

7.2.13 Notstrom über Gasturbinengenerator oder Dieselgeneratoren – ELVS-HM1

Es müssen entweder beide Notstromdieselgeneratoren oder ein Gasturbinengenerator funktionstüchtig sein, damit grundsätzlich Notstrom verfügbar ist. Zusätzlich müssen die Notstromversorger von der Betriebsmannschaft manuell gestartet mit den entsprechenden Stromschienen, EHVS bzw. ELVS, verbunden werden. Alle Generatoren sind empfindlich gegen externe Überflutung.

7.2.14 Wiederherstellung der externen Stromversorgung – EHVS-HM2

Die Wiederherstellung der externen Stromversorgung ist erfolgreich, wenn die externe Stromversorgung innerhalb 24h wieder verfügbar ist und die Batterien wieder aufgeladen werden. Reparaturarbeiten an Notstromdieselgeneratoren oder am Gasturbinengenerator werden nicht berücksichtigt.

7.2.15 Modulöffnung und Brennelententnahme – KRAN-HM1 und KRAN-HM2

Die Modulöffnung ist erfolgreich, wenn das Modul vollständig geöffnet im Brennelementwechselbecken steht. Die Brennelententnahme ist bereits erfolgreich, wenn die Naturumlaufkühlung für alle Brennelemente wiederhergestellt wurde. Wie viele Brennelemente dabei im Kern verbleiben und wie viele entnommen wurden ist nicht wesentlich.

7.3 Generelle Betrachtungen zu Transienten ohne Reaktorabschaltung (ATWS)

Für die Zulassung in den USA hat NuScale einige Basisrechnungen zum ATWS durchgeführt /NUS 20/. Die Ergebnisse zeigten /NUS 20/ folgend, dass

- der Druck im RCS nicht den maximal zulässigen Druck überschreitet, wenn mindestens ein RSV öffnet, unabhängig vom Erfolg der Initialisierungen des DHRS und des ECCS,
- der Druck im Sicherheitsbehälter nicht den Versagensdruckwert übersteigt,
- die Hüllrohrtemperaturen trotz der möglichen Rückkehr zur Kritikalität unterhalb 1200 °C bleiben und kein Kernschadenszustand eintritt.

Für die Kernauslegung gilt, dass sowohl die Temperatur des Moderators (das RCS-Kühlmittel im Kern) als auch die Temperatur des Kernbrennstoffs einen negativen Reaktivitätsrückwirkungskoeffizienten aufweisen. Der Kern wird demnach schnell unterkritisch nach einem Speisewasserausfall und einem damit verbundenen Temperaturanstieg im Primärkühlkreislauf (auch ohne Einfall der Abschaltstäbe). Der längerfristige ATWS ist wegen der zusätzlichen Wärme, die über die passiven Wärmeabfuhrsysteme (DHRS und ECCS) abgegeben werden muss, genauer zu betrachten.

Gründe für die ausreichende Kernkühlung sind der vergleichsweise kleine Kern, das große Verhältnis von Kühlmittel zu Leistung und die effizienten passiven Wärmeabfuhrsysteme DHRS und ECCS. Zu einer Rekritikalität kommt es erst nach der erfolgten Kopplung an die Not- und Nachwärmesenke (über das DHRS). Die stark-negative Temperaturreaktivitätsrückwirkung und das große Verhältnis von Kühlmittel zu Leistung sorgen dafür, dass sich die Spaltleistung an die Wärmeabfuhrkapazität anpasst und diese Kapazität nicht übersteigt. Die Spaltleistung kann demnach an die Not- und Nachwärmesenke abgegeben werden und der Kern ist gekühlt. Dies führt dazu, dass in den Ereignisablaufdiagrammen die Teildiagramme mit und ohne RESA (ATWS) gleich oder sehr ähnlich sind /NUS 20/.

7.4 Transienten und Reaktivitätsstörfälle

7.4.1 Allgemeine Transiente

Eine allgemeine Transiente beginnt mit der Anforderung einer RESA (dem Einfallen der Abschaltstäbe in den Kern). Die Anforderung kann unplanmäßig durch Fehlauslösung[22], ungewöhnlich großen Schwankungen in Anlagenmessgrößen oder nach einem Ausfall der Hauptwärmesenke und einem leichten Druckanstieg im Sekundärkühlkreis erfolgen. Eine RESA wird vom RTS automatisch unter den in Abschnitt 7.1 beschriebenen Bedingungen angefordert. Eine fehlausgelöste RESA kann durch ein gemeinsames Versagen mehrerer Messsensoren im RTS verursacht werden (dieser Fall soll hier aufgrund der geringen Eintrittswahrscheinlichkeiten nicht betrachtet werden).

[22] Es wird hier davon ausgegangen, dass das planmäßige Abfahren der Anlage (u. a. zum Tausch der Brennelemente) nicht durch eine RESA eingeleitet wird. Es gibt allerdings Regelwerke, die regelmäßige Tests der RESA fordern; entsprechende Tests können beim Abfahren der Anlage planmäßig durchgeführt werden, aber die genauen Bedingungen in der Anlage vor einem Test sind nicht bekannt.

Der Ereignisbaum als Ergebnis der Ereignisablaufanalyse ist in Abb. 7.1 dargestellt. Die erfolgreiche Auslösung der RESA führt in den oberen Teilbaum, die Pfade des unteren Teilbaumes repräsentieren ein ATWS. Bei erfolgter RESA kann die Nachzerfallswärme vollständig über mindestens eine Redundanz des DHRS abgeführt werden. Die Transiente wird beherrscht (Sequenz 1), falls beide Redundanzen verfügbar sind und der Druck im RCS nicht über den Ansprechdruck der RSVs ansteigt. Steht nur eine Redundanz des DHRS zur Verfügung oder tritt eine Druckspitze auf, so öffnet ein RSV (das erste Ventil öffnet bei 143 bar ± 1 %, das zweite Ventil würde erst bei 145 bar ± 1 % öffnen /NUS 20c/), und dieses Ventil sollte nach Druckabbau wieder vollständig schließen (Sequenz 2).

Schließt das Ventil nicht wie vorgesehen bei ca. 130 bar, wird im Folgenden das ECCS angeregt (durch Wasserstand im Sicherheitsbehälter zu hoch oder Druck im RCS zu niedrig), Sequenz 3. Fällt das ECCS aus, dann sollte eine Einspeisung durch das CVCS erfolgen (Sequenz 4), hierzu ist eine Handmaßnahme erforderlich.

Ein Fehlschlagen der Wiederbefüllung des RCS durch das CVCS bei gleichzeitiger Kühlung über das DHRS und das Ausdampfen über das offene RSV führt zu einem sinkenden Füllstand und zu einem Kernschadenszustand (Sequenzen 5 oder 6[23]).

Für den Fall, dass beide Redundanzen des DHRS unverfügbar sind, wird der Druck im Kühlkreislauf zum Ansprechen der RSVs führen. Die Wärmeabfuhr über den Sicherheitsbehälter erfolgt darauffolgend über die Aktivierung des ECCS, Sequenz 7. Fällt das ECCS aus, dann erfolgt die Wiederbespeisung durch eine Handmaßnahme über das CVCS (Sequenz 8 oder 11).

Bei gemeinsamem Ausfall von ECCS und CVCS kommt es zu einem Kernschadenszustand, druckentlastet in den Sequenzen 9, 10 oder 13 und druckbelastet bei über 130 bar in der Sequenzen 12. Im Fall eines gemeinsamen Ausfalls von DHRS und beiden RSVs kann die Nachzerfallswärme über den gefluteten Sicherheitsbehälter abgeführt werden, hierbei handelt es sich um eine Handmaßnahme der Betriebsmannschaft (Sequenz 14). Ist diese Handmaßnahme nicht erfolgreich, so kommt es zu einem HD-Versagen des RDB, Sequenz 15.

---

[23] Sequenz 6 berücksichtigt eine fehlgeschlagene Handmaßnahme. Falls die abgeschlossenen Ventile des CVCS von der Betriebsmannschaft geöffnet worden sind, aber die Maßnahme durch einen Systemausfall versagt und durch die geöffneten Ventile ein Sicherheitsbehälter-Bypass vorliegt.

Der untere Teilbaum in Abb. 7.1 (ab Sequenz 16) repräsentiert ein ATWS. Im Verlauf des Störfalls kommt es zur Anforderung des DHRS. Ein Kernschadenszustand wird verhindert, wenn eine Redundanz des DHRS verfügbar ist, das RSV im Verlauf der Transiente öffnet und die ECCS-Ventile öffnen (Sequenz 16) oder eine Einspeisung über das CVCS erfolgt (Sequenzen 17 und 20). Das Fehlschlagen der Einspeisung führt zu einem Kernschadenszustand, entweder im druckentlasteten RCS, Sequenzen 18, 19 oder 22, oder im druckbehafteten RCS, Sequenz 21 bei über 130 bar.

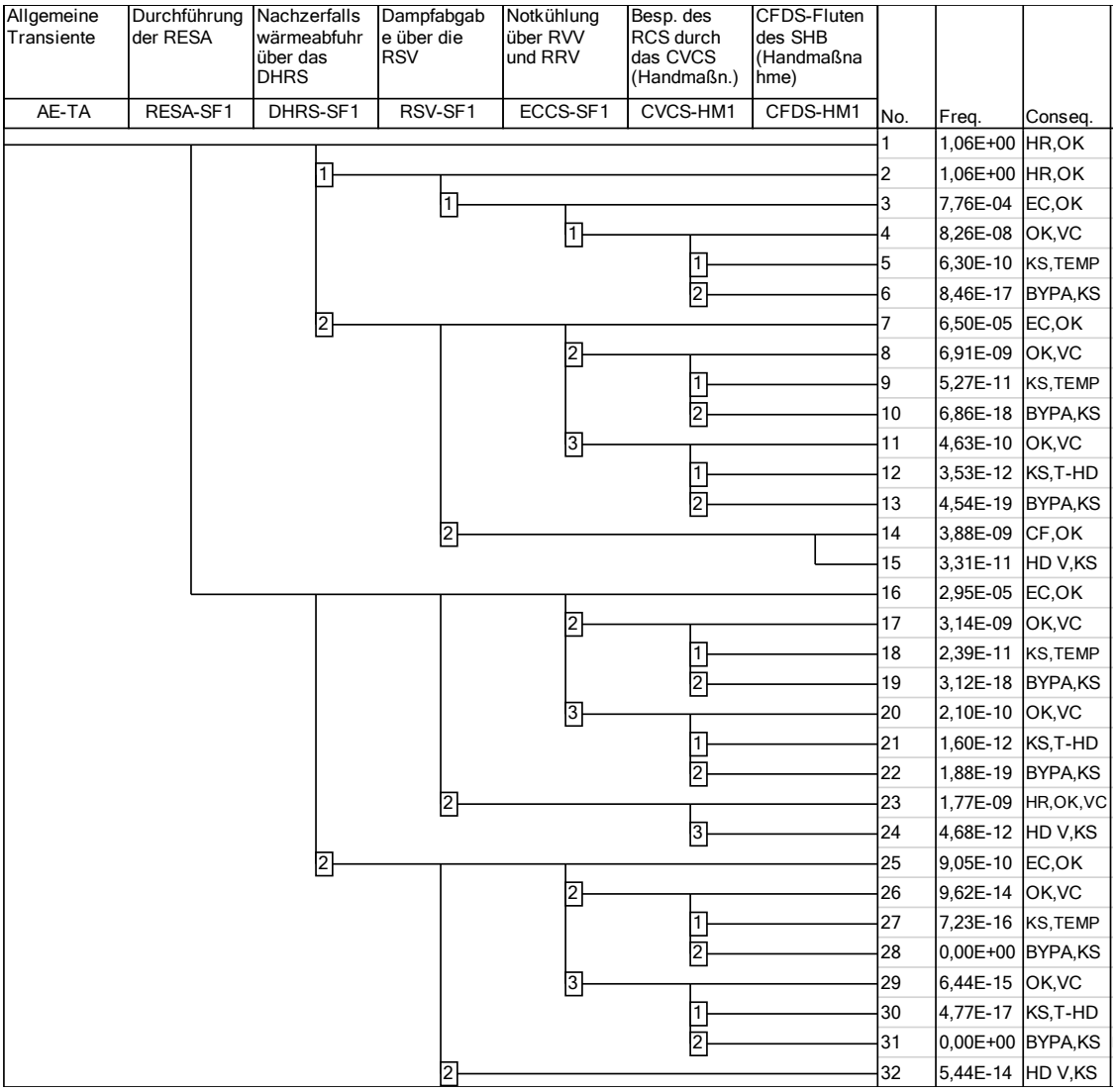


Abb. 7.1 Ereignisablaufdiagramm für allgemeine Transienten

Im Unterschied zur Ereignisbaumanalyse für den Fall mit RESA (Sequenz 2) wird im Fall eines ATWS die zusätzliche Wärmeabfuhr über den Sicherheitsbehälter nach Öffnen des RSVs benötigt. Der Grund dafür ist die höhere Kernwärmeabgabe im Transientenverlauf. Bleibt das RSV geschlossen, dann kann das Versagen des RCS durch Sprühen

und Kühlmittelentnahme des CVCS verhindert werden (Sequenz 23), ansonsten ist mit einem Versagen der druckführenden Umschließung des RCS zu rechnen (Sequenz 24).

Sind beide Redundanzen des DHRS unverfügbar, ergibt sich dennoch über das ECCS die Möglichkeit der Verhinderung eines Kernschadens, Sequenz 25, oder über die Einspeisung durch das CVCS, Sequenzen 26 oder 29. Versagt die Wiederbespeisung, so ergibt sich ein Kernschadenszustand (Sequenzen 27, 28 und 31 zeigen einen druckentlasteten Fall und Sequenz 30 den Hochdruckfall bei über 130 bar). Der Ausfall beider Redundanzen des DHRS und der gleichzeitige Ausfall beider RSVs hat ein Versagen der druckführenden Umschließung des Kühlkreislaufes zur Folge (Sequenz 32).

7.4.2 Fehlausfahren der Steuerstäbe

Der Reaktivitätsstörfall ‘Fehlausfahren der Steuerstäbe‘“ soll abdeckend für alle Reaktivitätsstörfälle mit positivem Reaktivitätseintrag betrachtet werden. Folgende Randbedingungen des Kerns führen dabei zu den niedrigsten kritischen Wärmeflussverhältnissen /NUS 20b/:

- anfängliche Kernleistung bei 70 %,
- Kerninventar am Zyklusende,
- hohe mittlere Kühlmitteltemperatur,
- niedrige Kerndurchflussrate,
- hohe Wärmeleitfähigkeiten im Kern (die Wärmeleitfähigkeit wird beispielsweise reduziert durch einen erhöhten Abbrand oder eine Oxidschicht auf den Hüllrohren).

Darüber hinaus werden folgende konservative Annahmen getroffen:

- Das Abschaltelement (bestehend aus 24 einzelnen Abschaltstäben) mit größter Reaktivitätswirkung verbleibt außerhalb des Kerns während der RESA (die Abschaltbank umfasst insgesamt acht Abschaltelemente),
- Verzögerung der RESA um zwei Sekunden,
- maximale Dauer für das Einfallen der Abschaltstäbe nach Auslösen der RESA,
- maximale Ausfahrgeschwindigkeit des fehlerhaft ausfahrenden Steuerstabelementes,

– maximale Reaktivitätswirkung des ausfahrenden Steuerstabelementes (insgesamt sind acht Steuerelemente vorhanden) bei minimaler Temperaturreaktivitätsrückwirkung im Kern.

Die Störfallbeherrschung setzt die Auslösung der RESA und eine ausreichende Nachzerfallswärmeabfuhr voraus. Dieser Sachverhalt wird mit den Untersuchungen in /NUS 20b/ begründet. In einer deterministischen Rechnung zeigt sich eine kontinuierliche Abnahme der Sicherheit gegenüber dem Filmsieden (kritische Heizflächenbelastung) bis zum Zeitpunkt der RESA nach 132 s, Abb. 7.2. Unter der Annahme, dass nach Ausfall der RESA sich der Abwärtstrend des Indikators weiter fortsetzt, so ist ein Beginn des Filmsiedens im Kern nach ca. 140 s mit einer gewissen Wahrscheinlichkeit zu befürchten (MCHFR = 1,3, eine Sicherheitsmarge von 30 % wurde hier berücksichtigt, um Unsicherheiten abzudecken). Eine Filmsieden hätte einen schnellen Temperaturanstieg im Kern zur Folge. Der erzeugte Dampf im Kern bewirkt eine negative Reaktivitätsrückwirkung auf den Kern. Ob dieser leistungsmindernde Effekt ausreicht, um den Temperaturanstieg im Kern noch vor Eintritt eines Kernschadens zu stoppen, kann hier nicht geklärt werden. Ein Kernschadenszustand nach einem zusätzlichen Ausfall der RESA soll in der weiteren Analyse aber postuliert werden. Das entsprechende Ereignisablaufdiagramm für Reaktivitätsstörfälle ist in Abb. 7.3 gezeigt.

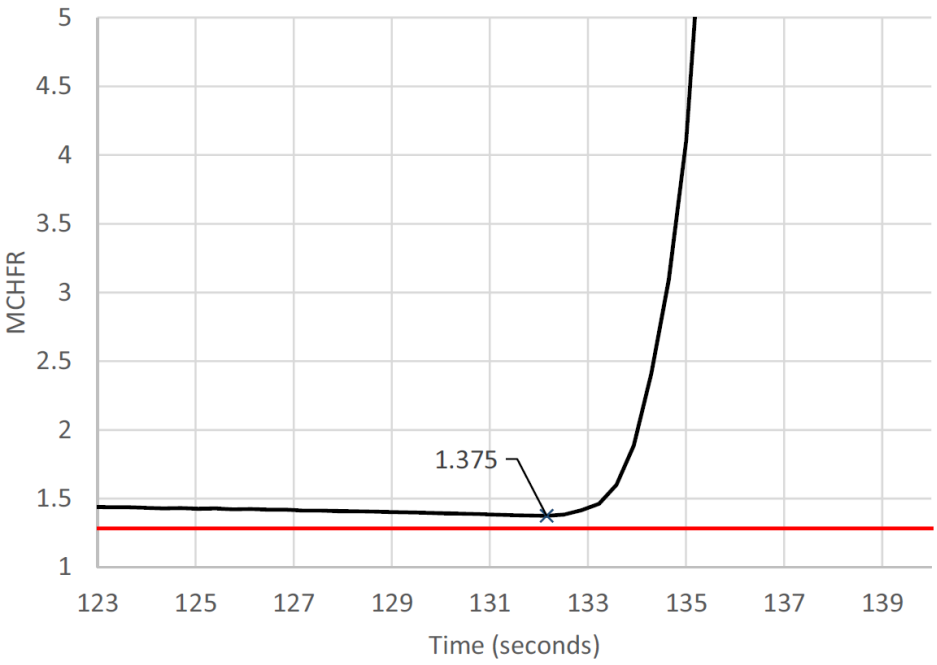


Abb. 7.2 Kritische Heizflächenbelastung bzgl. dem Übertritt zum Filmsieden für den Fall eines Steuerstabfehlfahrens, aus /NUS 20b/

Nach der RESA wird die Nachzerfallswärme an das DHRS abgegeben und die RSVs könnten im Transientenverlauf zeitweise öffnen (Sequenz 1). Für den Fall eines offenstehenden RSV wird durch Wasserstand im Sicherheitsbehälter zu hoch oder Druck im Kühlkreislauf zu niedrig das ECCS angeregt (Sequenz 2).

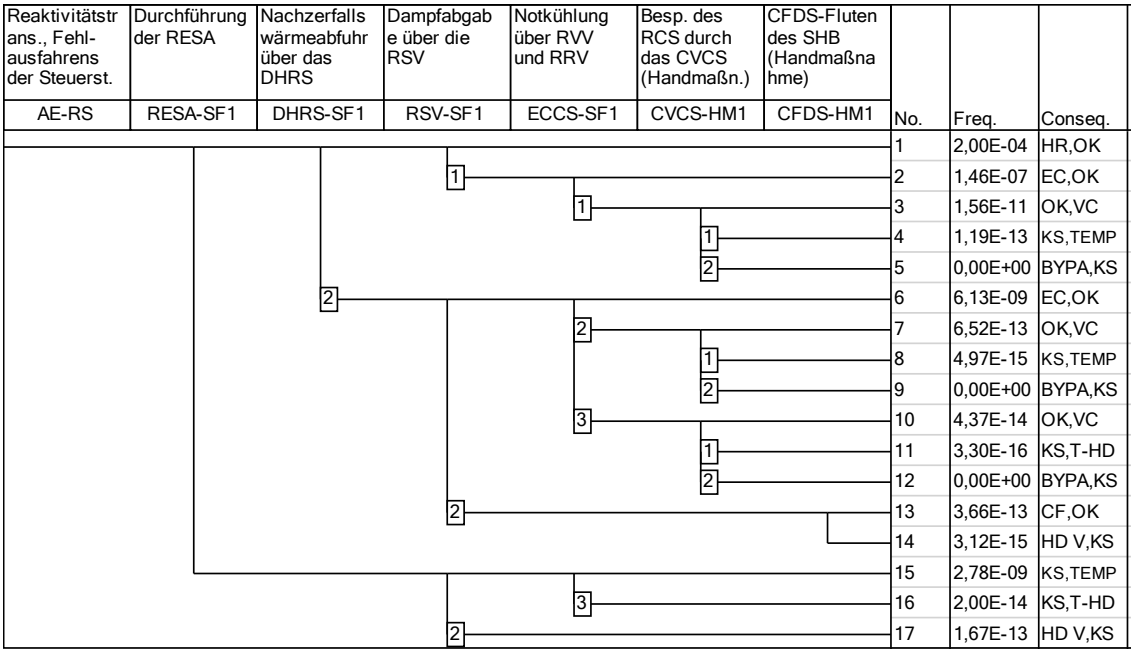


Abb. 7.3 Ereignisablaufdiagramm für Reaktivitätsstörfälle mit fehlerhaft eingebrachter Reaktivität

Fällt das ECCS aus, sollte über eine Handmaßnahme eine Wiederbefüllung des RCS mit dem CVCS erfolgen (Sequenz 3). Das Fehlschlagen dieser Maßnahme führt in den Kernschaden (Sequenzen 4 und 5). Bei Unverfügbarkeit beider Redundanzen des DHRS steigt der Druck im Kühlkreislauf bis zum Ansprechdruck der RSVs an. Die Nachzerfallswärmeabfuhr erfolgt über das ECCS (Sequenz 6).

Schlägt die Aktivierung des ECCS fehl, dann kann die Wiederbespeisung mittels einer Handmaßnahme durch das CVCS erfolgen (Sequenz 7 oder 10). Ein Ausfall beider Systeme, ECCS und CVCS, führt zum Kernschaden, entweder druckentlastet (Sequenzen 8, 9 oder 12) oder druckbelastet bei über 130 bar in Sequenz 11.

Sollten das DHRS und beide RSVs gemeinsam ausfallen, so kann die Nachzerfallswärme über ein Fluten des Sicherheitsbehälter erfolgen (Sequenz 13). Erfolgt diese Handmaßnahme nicht, ist mit dem HD-Versagen des RDB zu rechnen (Sequenz 14).

Falls die RESA nicht zur Verfügung steht, ist mit einem Voranschreiten des Reaktivitätsstörfalls zu rechnen (Sequenz 15). Ein sehr schneller Eingriff der Betriebsmannschaft wäre erforderlich, um möglichst hochkonzentrierte Borsäure in den Primärkühlkreislauf über das CVCS einzuspeisen. Aber auch diese Maßnahme würde erst verzögert Wirkung zeigen (Rohrleitungslängen und Dauer bis zu einer Durchmischung im Primärkühlkreislauf). Sind die RSVs zusätzlich nicht verfügbar, so ist mit einem Versagen der druckführenden Umschließung zu rechnen (Sequenz 17) oder bei Unverfügbarkeit aller ECCS-Ventile, der Kernschaden unter HD-Bedingungen (Sequenz 16).

Reaktivitätsstörfälle unter Anfahrbedingungen werden konservativ und abdeckend in /NUS 20b/ untersucht. Der Grenzwert für die Aktivierung der RESA ist auf 25% der nominalen Leistung im Leistungsbetrieb abgesenkt, so kann trotz schnellerem Anstieg das Maximum der Leistung niedrig gehalten werden. Die entsprechenden Ereignispfade ergeben sich analog zum Leistungsbetrieb und sind durch diesen abgedeckt.

7.4.3 Ausfall der externen Stromversorgung

Ein Ausfall der externen Stromversorgung kann mehrere Ursachen haben. Ein Ausfall im EHVS oder in der Umspannanlage führt in allen Modulen in die RESA. Ein Spannungsabfall im Netz wird aber führt allerdings zunächst in einen Lastabwurf auf Eigenbedarf und bei Erfolg dieser Maßnahme in die Beherrschung des Szenarios (Sequenz 1, der Ereignisablaufanalyse in Abb. 7.4).

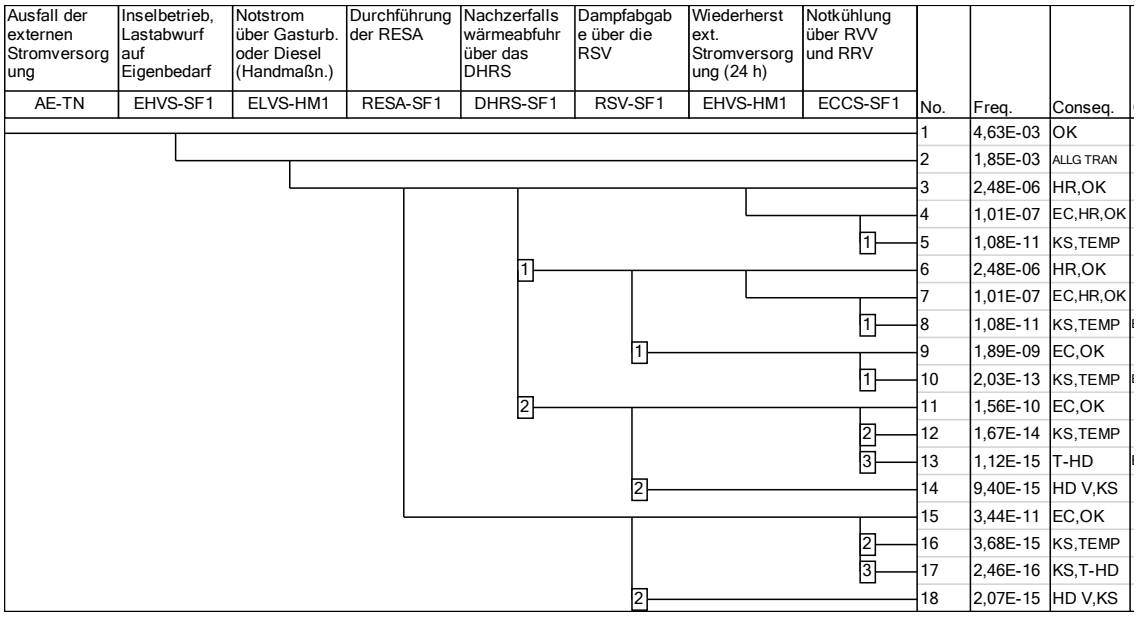


Abb. 7.4 Ereignisablaufdiagramm für den Ausfall der externen Stromversorgung

Kommt es zur RESA, so stehen im weiteren Ablauf entweder der Gasturbinengenerator oder beide Notstromdieselgeneratoren zur Notstromversorgung zur Verfügung (Sequenz 2), kann der Störfall auf den Ereignisbaum einer allgemeinen Transiente, Abschnitt 7.4.1, zurückgeführt werden. Fällt die interne Notstromversorgung vollständig aus (Sicherheitsbehälter), ist der Ereignisbaum ähnlich dem einer allgemeinen Transienten mit drei Unterschieden:

- Für die Ereignispfade mit RESA, Nachzerfallswärmeabfuhr und geschlossenem RSVs muss die externe Stromversorgung innerhalb von 24 h wiederhergestellt werden (Sequenzen 3, 6 oder 11), ansonsten wird das ECCS stromlos gefahren und damit aktiviert (Spannung im ELVS über 24 h zu niedrig), Sequenzen 4 oder 7. Der Grund für die Unterbrechung der Batteriestromversorgung für das ECCS ist Strom zu sparen, damit genügend Energie aus der Batterie für die Überwachung der Anlage für insgesamt 72 h nach externem Stromausfall bleibt /NUS 20e/. Öffnen mit der Aktivierung des ECCS nicht mindestens ein RVV und ein RRV oder kommt der Naturumlauf nicht in Gang, so ist mit einem Kernschaden zu rechnen, Sequenzen 5, 8, 12, 13, 16 oder 17.
- Das CVCS steht ohne Stromversorgung nicht zur Verfügung.
- Das Fluten des Sicherheitsbehälters kann ohne Stromversorgung nicht durchgeführt werden.

Fällt die externe Stromversorgung während eines Brennelementwechsels aus, Mode 5 POS2 bis POS5, so wird die Nachzerfallswärme über den gefluteten (POS2, POS3 & POS5) oder geöffneten (POS4) Sicherheitsbehälter an das Reaktorbecken abgegeben. Es ist mit keinen Kernschaden zu rechnen. Während POS1 wird der Sicherheitsbehälter über das CFDS geflutet. Bei einem Ausfall der externen Stromversorgung wird dieser Vorgang unterbrochen.

7.4.4 Ausfall des Gleichstromnetzes EDSS

Ein Ausfall des EDSS (mindestens zwei der vier EDSS-Busse) führt zur Auslösung der RESA, Aktivierung der Nachzerfallswärmeabfuhr, Sicherheitsbehälterabschluss mit Dampferzeuger- und CVCS-Abschluss. Das Ergebnis der Ereignisablaufanalyse ist in Abb. 7.5 gezeigt.

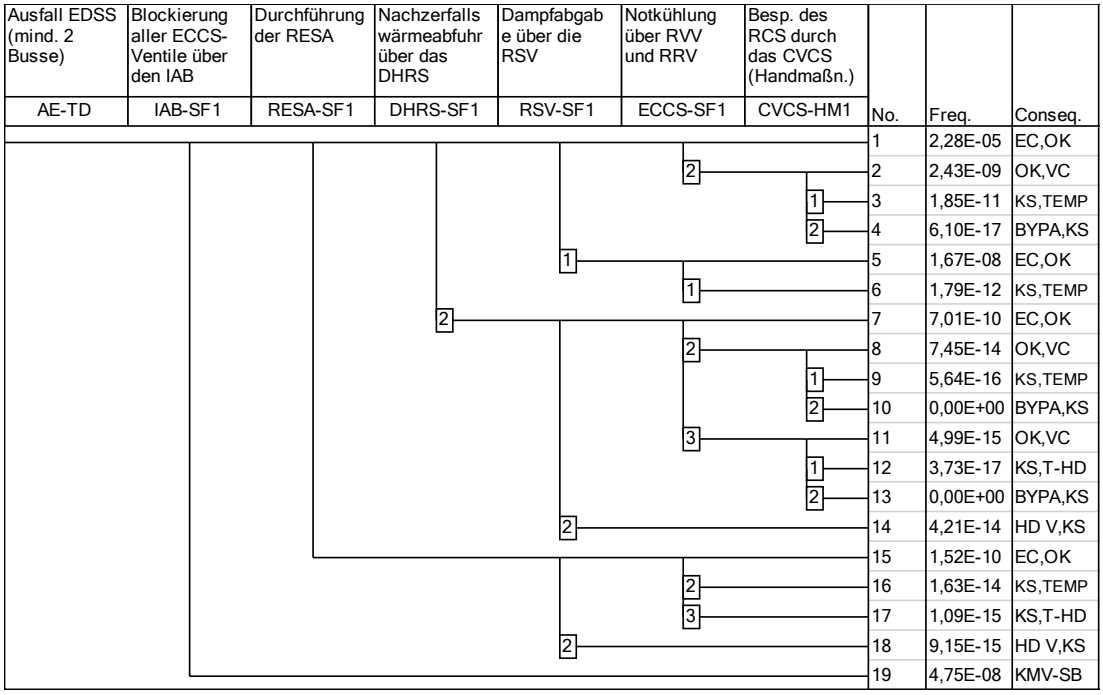


Abb. 7.5 Ereignisablaufdiagramm für den Ausfall der Gleichspannungsversorgung

Das ECCS wird durch den EDSS-Ausfall aktiviert, aber durch den IAB zunächst blockiert, bis der Druckunterschied zwischen RCS und Sicherheitsbehälter unterhalb 65 bar gefallen ist. Versagt der IAB an einem Ventil, so wird der Störfall im Weiteren als KMV in den Sicherheitsbehälter unter Berücksichtigung der Unverfügbarkeit der Gleichspannung (Sequenz 19). Für andere Sequenzen sinkt der Druckunterschied zwischen RCS und Sicherheitsbehälter aufgrund eines Druckabbaus im RCS über das DHRS (Sequenzen 1 bis 4) oder durch Dampfabgabe an den Sicherheitsbehälter (Sequenzen 5 bis 13).

Das CVCS kann über eine Handmaßnahme durch die Betriebsmannschaft aktiviert werden, sofern mindestens ein Bus des EDSS zur Verfügung steht (CVCS-HM1). Ist die RESA erfolgt, eine Redundanz des DHRS verfügbar[24], schließt das RSV nach der Anforderung wieder und läuft die Notkühlung über das ECCS planmäßig an, dann wird ein Kernschadenszustand verhindert (Sequenz 1). Schlägt die Notkühlung fehl, dann kann mit Hilfe des CVCS (mind. ein Bus des EDSS benötigt) der RCS nachgefüllt werden (Sequenz 2). Eine Unverfügbarkeit der Einspeisung führt in den Kernschaden (Sequenzen 3 oder 4). Schließt das durch einen Druckanstieg im RCS angeforderte RSV fehlerhaft nicht, dann kommt die Notkühlung durch den Druckverlust früher zum Einsatz und

[24] Aufgrund des Ausfalls von mindestens zwei EDSS-Bussen kann eine Redundanz des DHRS nicht regulär angefordert werden

die Nachzerfallswärme kann erfolgreich abgeführt werden (Sequenz 5). Ein Ausfall der Notkühlung hat einen Kernschaden zur Folge. Der Ausfall des DHRS führt zum Ansprechen der RSVs. Die Druckabgabe an den Sicherheitsbehälter hat das Öffnen der ECCS-Ventile zur Folge (Sequenz 7). Öffnen die ECCS-Ventile fehlerhaft nicht, so sollte mit dem CVCS nachgespeist werden (Sequenzen 8 oder 11).

Wird das CVCS nicht aktiviert oder steht nicht zur Verfügung, dann ergibt sich ein Kernschaden, druckentlastet (Sequenzen 9, 10 und 13) oder druckbelastet (130 bar, Sequenz 12). Öffnen die RSVs fehlerhaft nicht, so kommt es zu einem HD-Versagen der druckführenden Umschließung (Sequenz 14). Für den Fall eines ATWS kann der Kernschaden mit Hilfe des ECCS und dem Ansprechen der RSVs verhindert werden (Sequenz 15), ansonsten ist mit einem Kernschaden (druckentlastet: Sequenz 16, druckbeaufschlagt: Sequenz 17) oder einem Hochdruckversagen des RCS (Sequenz 18) zu rechnen.

Kommt es zu einem Ausfall der Gleichspannungsversorgung während eines Brennelementwechsels (Mode 5 POS2 bis POS5), so wird die Nachzerfallswärme über den gefluteten oder geöffneten Sicherheitsbehälter an das Reaktorbecken abgegeben. Es ist mit keinen Kernschaden zu rechnen.

7.4.5 Leitungsleck im Sekundärkühlkreis

Ein Leitungsleck/-bruch im Sekundärkühlkreis, entweder im Speisewasserbereich oder im Frischdampfbereich, führt zur Auslösung der RESA aufgrund von

- hohem Sicherheitsbehälterdruck (Frischdampf-Rohrlecks innerhalb des Sicherheitsbehälters),
- niedrigem Frischdampfdruck oder hoher Reaktorleistung (Frischdampf-Rohrlecks außerhalb des Sicherheitsbehälters) oder
- hohem Druck im RCS (Leck in einer Speisewasserleitung).

Die Ereignisablaufanalyse zeigt einen ähnlichen Ereignisablauf im Vergleich zu allgemeinen Transienten, Abb. 7.6. In der Analyse wurde berücksichtigt, dass aufgrund des Kühlmittelverlustes in den Sicherheitsbehälter, die Möglichkeit zum Fluten des Sicherheitsbehälter über das CFDS nicht mehr gegeben ist. Darüber hinaus kann im Fall eines ATWS mit Nachzerfallswärmeabfuhr und geöffnetem RSV der Kernschadenszustand

nicht durch ein Sprühen durch das CVCS verhindert werden. Konservativ betrachtet steht maximal eine Redundanz des DHRS zur Verfügung (die Redundanz des nicht betroffenen Dampferzeugers), dies entspricht im Modell der Alternative 3 der Systemfunktion DHRS-SF1. Es besteht nämlich die Möglichkeit, dass der betroffene Dampferzeuger nicht vom Leck abgetrennt werden kann oder zu wenig Kühlmittel im Dampferzeuger zurückbleibt, um die Nachzerfallswärmeabfuhr über das DHRS zu gewährleisten. Darüber hinaus sind beide Redundanzen der Dampferzeuger in der Sammelleitung verbunden und trennen sich erst wieder in der Speisewasserleitung. Zu Störfallbeginn besteht die Gefahr, dass auch die zweite Redundanz der Nachzerfallswärmeabfuhr aufgrund des Kühlmittelverlusts nicht zur Verfügung steht, speziell bei Leitungslecks im nicht-redundanten Teil des sekundären Kühlsystems (z. B. Bruch der Sammelleitung oder der gemeinsamen Speisewasserleitung).

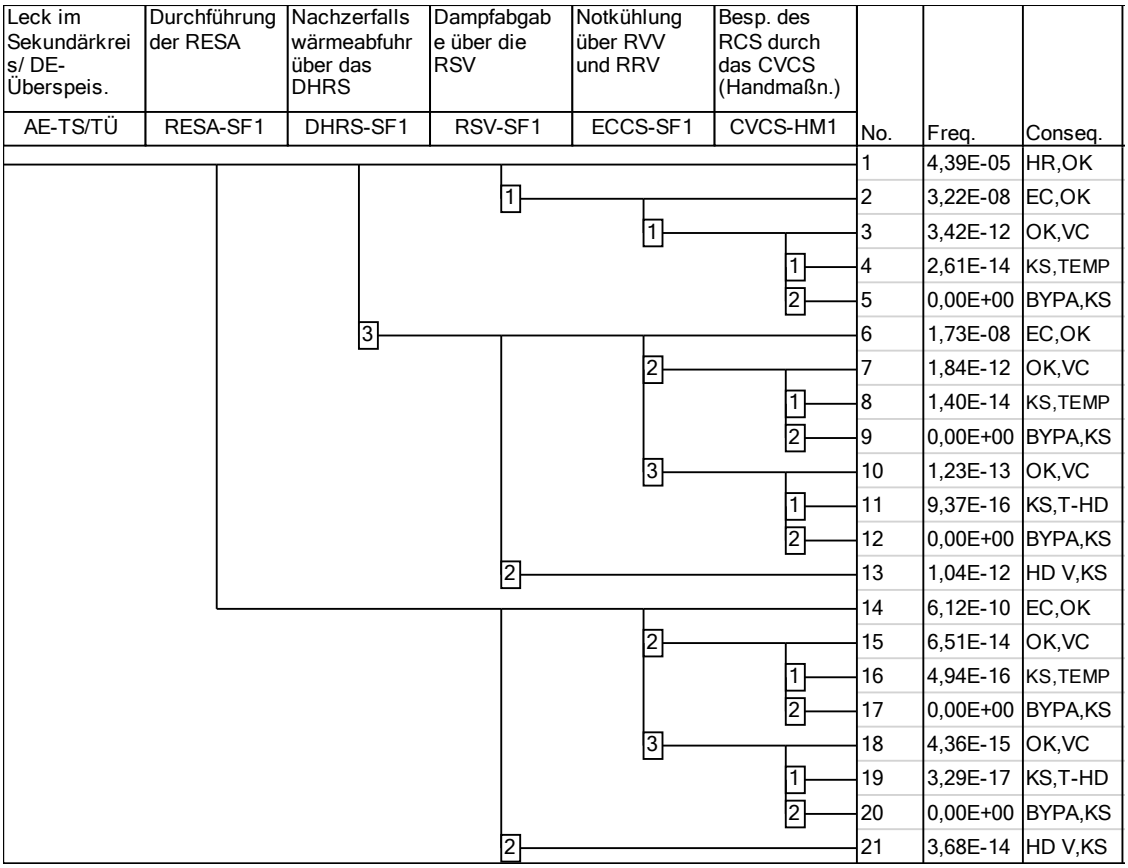


Abb. 7.6 Ereignisablaufdiagramm zu einem Leitungsleck im Sekundärkühlkreis

7.4.6 Dampferzeugerüberspeisung

Der Störfall der *Dampferzeugerüberspeisung* ist bei einer normalen Überspeisungsrate auf die Ereignisablaufanalyse zur allgemeinen Transienten zurückzuführen. Ist der

Vorgang der Überspeisung sehr rasch, so gefährdet der Anstieg des Dampferzeugerfüllstandes die Verfügbarkeit der betroffenen Redundanz oder beider Redundanzen des DHRS. In diesem Fall ist die Ereignisablaufanalyse zum Leitungsleck im Sekundärkühlkreis anzuwenden (konservativer Fall).

7.4.7 Überspeisung durch das CVCS

Dieser Störfall unterscheidet sich vom Störfall einer fehlerhaft heizenden Druckhalterheizung (betrachtet als KMV in den Sicherheitsbehälter, Abschnitt 7.5.1) in dem Punkt, dass der Füllstand im RCS durch die Einspeisung des CVCS immer weiter ansteigt. Der Störfall geht mit erfolgreichem Abschluss der CVCS-Einspeiseleitung bzw. CVCS-Sprühleitung[25] in eine allgemeine Transiente über (Sequenz 1 in Abb. 7.7), anderenfalls kommt es zu einer anhaltenden Überspeisung. Dieser Fall überschreitet die Untersuchungen der beherrschten Störfälle /NUS 20b/. Die RESA wird ausgelöst durch Druck oder Füllstand im Druckhalter zu hoch. Die CVCS-Aufbereitungspumpen sind Verdrängerpumpen und können bis zu einem Druck von 155 bar jeweils maximal 1,3 l/s (die Pumpen können mit variabler Drehzahl betrieben werden) einspeisen /NUS 20d/; dieser Druck liegt oberhalb des Ansprechdrucks der RSVs (143 bar bzw. 145 bar).

Die Nachzerfallswärme kann zunächst über das DHRS, dann über das ECCS und zuletzt über den gefüllten Sicherheitsbehälter abgegeben werden. Kann die dauerhafte Überspeisung des RCS über das CVCS nicht verhindert bzw. die Einspeisemenge nicht begrenzt werden, so droht der Sicherheitsbehälter durch einen aufgeprägten Druck von über 90 bar zu versagen (Sequenzen 4, 6, 9, 11, 16 oder 18)[26]. Falls das CVCS dauerhaft überspeist und hierfür auch die Kühlmittelreserven des Deionatsystems (600 m³) verfügbar sind, so ist die Integrität des Sicherheitsbehälter entsprechend gefährdet.

---

[25] Es wird angenommen, dass das CVCS-Abschlusssignal nicht von der Betriebsmannschaft überschrieben werden kann, da der Grund für die Auslösung weiter bestand hat, ansonsten käme eine Zuschaltung der CVCS-Entnahmeleitung als Möglichkeit zur Störfallbeherrschung in Frage.

[26] Der Sicherheitsbehälter kann über die Kühlmittelreserven im Boreinspeisesystem (maximal 95 m³) nicht vollständig aufgefüllt werden (das Deionatsystem ist abgesperrt), allerdings ist von einem steigenden Dampfdruck bei fehlender Nachwärmeabfuhr auszugehen.

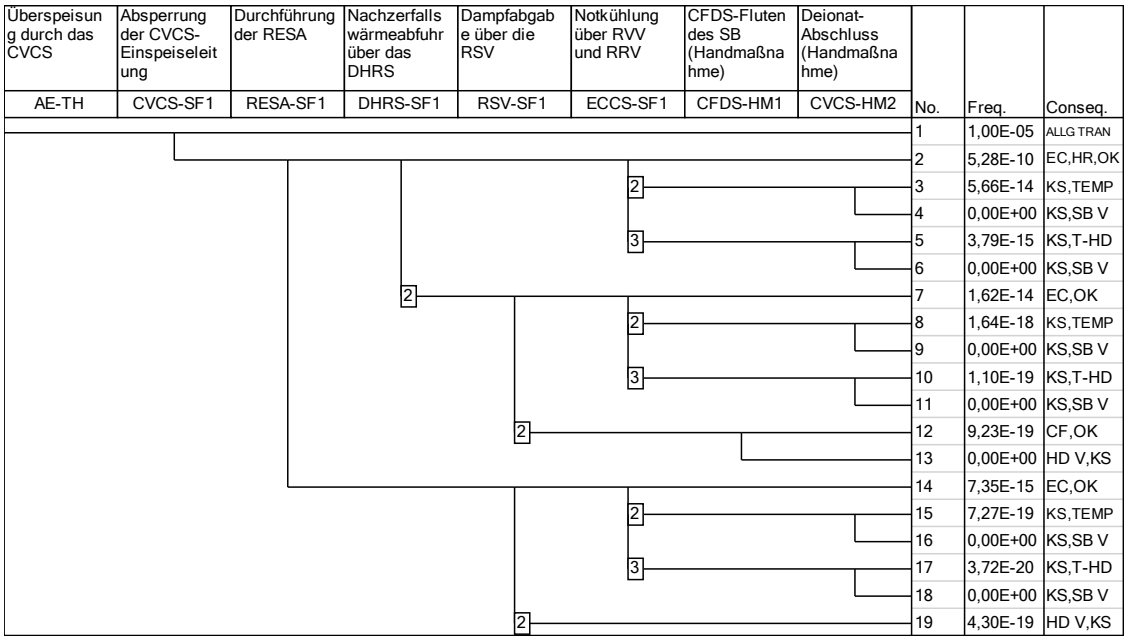


Abb. 7.7 Ereignisablaufdiagramm für das auslösende Ereignis einer Überspeisung des RCS

Ein Sicherheitsbehälterversagen setzt voraus, dass das Deionatsystem fehlerhaft nicht abschließt und die Betriebsmannschaft die CVCS-Pumpen nicht außer Betrieb nehmen oder manuelle Absperrventile schließen kann, um damit die weitere Einspeisung zu unterbinden[27]. Die Kühlmittelreserven im Boreinspeisesystem (95 m³) reichen nicht aus, um den Sicherheitsbehälter vollständig mit Kühlmittel zu füllen. Darüber hinaus ist durch die fehlerhafte Kühlmitteleinspeisung nicht mit einem Druckanstieg im Sicherheitsbehälter zu rechnen. Die Kühlleistung des ECCS führt zu einem längerfristigen Druckabbau von ca. – 0,5 kPa/s, abgeschätzt über das Ergebnis einer Simulation von NuScale (siehe Abb. 7.8).

Für Einspeiseraten von bis zu 2,5 l/s, die maximal durch das CVCS eingespeist werden könnten, kann über das ideale Gasgesetz konservativ ein Beitrag zur Druckveränderung im Sicherheitsbehälter von + 0,1 kPa/s bis + 0,2 kPa/s je nach Füllstand im Sicherheitsbehälter abgeschätzt werden. Es ergibt sich damit immer noch effektiv ein Druckabfall von mindestens – 0,3 kPa/s, sofern die Kühlmittelreserven des Deionatsystems nicht eingespeist werden. Bei einer Unverfügbarkeit des ECCS (Sequenzen 3, 8, 15 oder mit

[27] Die Möglichkeiten zum Stop der CVCS-Pumpen sind vielfältig und es bleibt ausreichend Zeit diese Möglichkeiten umzusetzen, > 24 h, dazu zählen der Abschluss manueller Ventile, die entsprechenden ELVS-Stromschienen außer Betrieb zu setzen oder die Pumpen manuell abzuschalten.

druckbeaufschlagtem RCS die Sequenzen 5, 10 oder 17) ist ein Kernschaden anzunehmen, da aufgrund der Fehlfunktion des CVCS nicht davon ausgegangen werden kann, dass die Einspeiserate dauerhaft genügend hoch ist, um den Kern ausreichend zu kühlen. Das ECCS hingegen liefert ausreichend kondensiertes Kühlmittel über die RRV nach (Sequenzen 2, 7 und 14).

Öffnen die RSVs fehlerhaft nicht, so stoppt die Einspeisung des CVCS bei 155 bar im RCS, der Sicherheitsbehälter bleibt dabei evakuiert und das ECCS wird nicht in Betrieb genommen. Die Nachzerfallswärme kann durch ein CFDS-Fluten des Sicherheitsbehälter an das Reaktorbecken abgegeben werden (Sequenz 12). Steht keine ausreichende Wärmeabfuhr bei geschlossenen RSVs zur Verfügung, so ergibt sich ein Hochdruckversagen des RCS (Sequenzen 13 und 19).

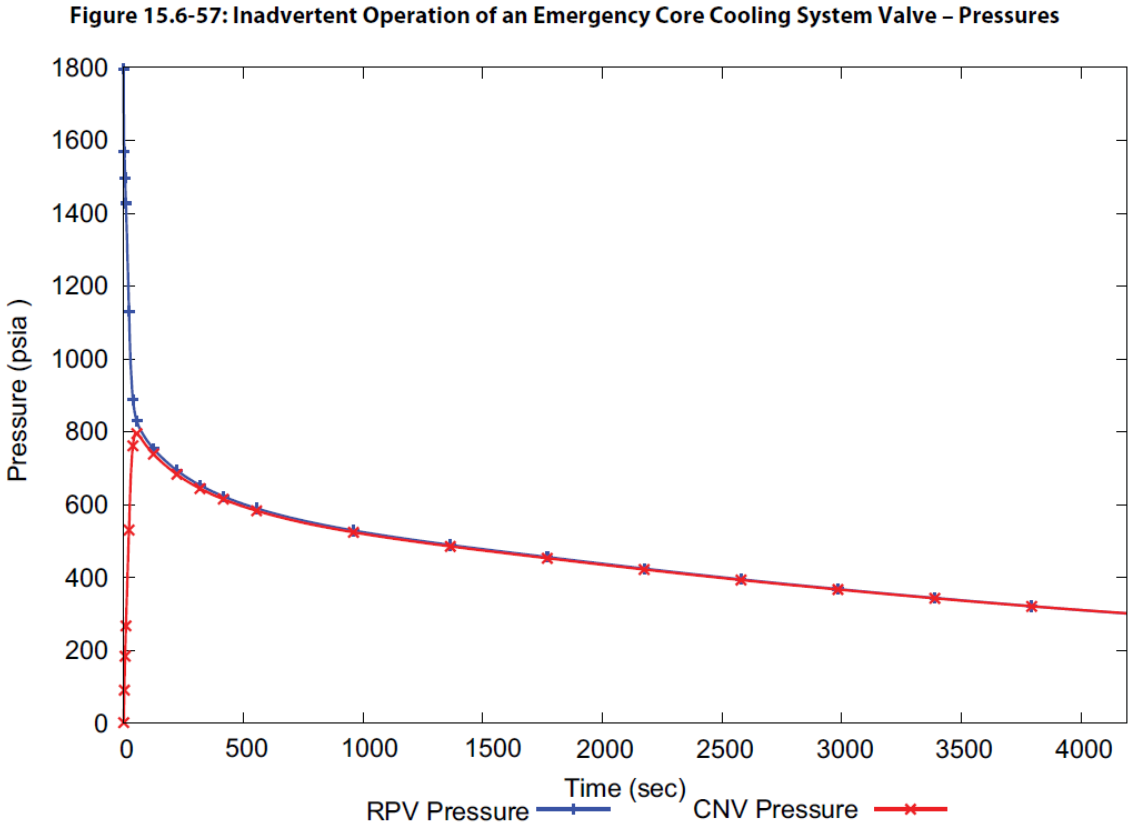


Abb. 7.8 Kühlleistung des ECCS nach erfolgter Druckentlastung des RCS /NUS 20b/

7.4.8 Ausfall von Komponentenhilfssystemen

Infolge eines Ausfalls von Komponentenhilfssystemen (z. B. Ausfall des Komponentenkühlwassers, der Luftzufuhr oder verschiedener Stromschienen wie EHVS, EMVS oder ELVS, siehe u. a. /DOY 20/) fallen das CVCS und das CFDS aus. Die RESA wird

entweder aufgrund niedriger Batterieladespannung oder hohem Frischdampf-Druck im Sekundärkühlkreis nach Abschluss (z. B. aufgrund niedriger Batterieladespannung) ausgelöst /NUS 20/. Das Ereignisablaufdiagramm, Abb. 7.9, ergibt sich analog zu allgemeinen Transienten unter Berücksichtigung der Systemausfälle:

- CVCS,
- CFDS.

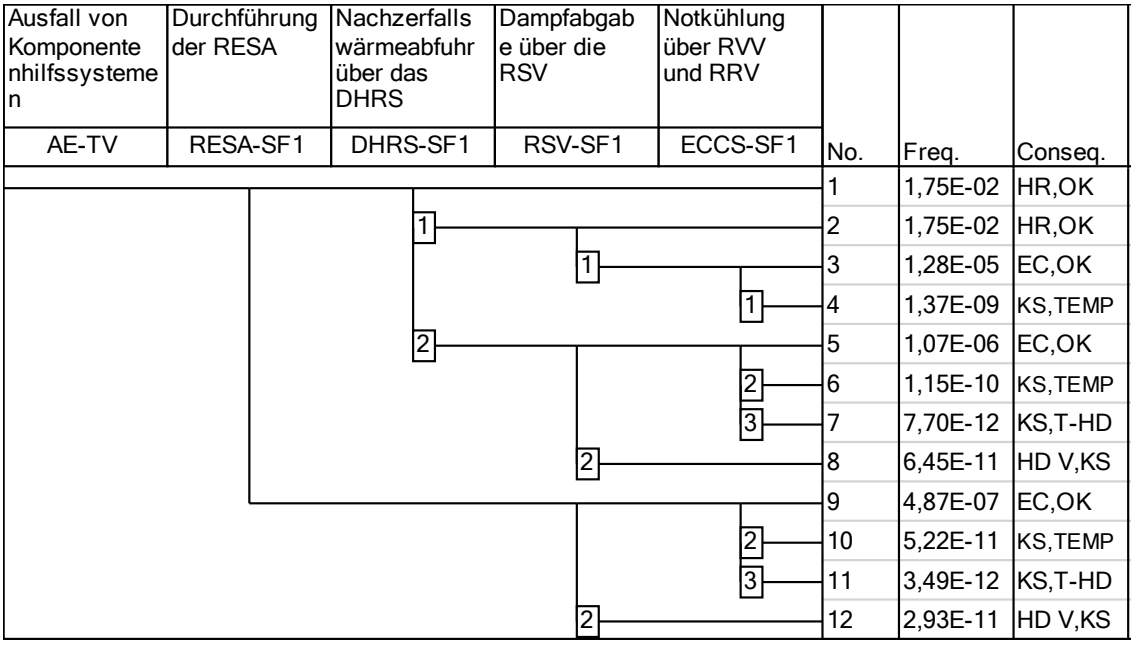


Abb. 7.9 Ereignisablaufdiagramm für den Ausfall von Komponentenhilfssystemen

7.4.9 Kleines Leck zwischen Reaktorbecken und Sicherheitsbehälter

Ein kleines Leck zwischen Reaktorbecken und Sicherheitsbehälter führt zu einem Eindringen von Beckenwasser in den Sicherheitsbehälter. Die RESA wird aufgrund eines hohen Druckes im Sicherheitsbehälter ausgelöst (Druck größer als 0,7 bar). Die Betriebsmannschaft kann über die Inbetriebnahme der CFDS-Drainagefunktion[28] versuchen, das einströmende Kühlmittel abzupumpen, um das Auslösen des ECCS ab einer

[28] Die CFDS-Drainagefunktion setzt einen kleinen Überdruck im SB voraus, der über das CES erzeugt wird. Ist das Leck zu groß, so kann möglicherweise kein genügender Überdruck im SB erzeugt werden, um eine Kavitation der CFDS-Pumpen zu verhindern.

Füllstandsmarke von 6 m zu verhindern[29]. Je nach Größe des Lecks bleibt dafür möglicherweise nur wenig Zeit. Die Ereignisablaufanalyse ist in Abb. 7.10 dargestellt.

Stehen beide Redundanzen des DHRS zur Verfügung, kommt es im Verlauf der Transiente nicht zum Ansprechen eines RSVs und kann die Auslösung des ECCS verhindert werden (über eine Drainage durch das CFDS), so wird die Nachzerfallswärme dauerhaft über das DHRS abgeführt (Sequenz 1). In dieser Sequenz kommt es zu keinem Kühlmittelaustausch zwischen RCS und Sicherheitsbehälter. Löst das ECCS aus, so wird das CVCS zur Kühlung benötigt (Sequenz 2). Dabei kann von keiner vollständigen Nachzerfallswärmeabfuhr über das ECCS aufgrund des Ein- oder Ausströmens von Kühlmittel über das Leck ausgegangen werden.

Öffnet ein RSV und gibt Dampf in den Sicherheitsbehälter ab, so kann dennoch mit einer erfolgreichen CFDS-Drainage die Auslösung des ECCS verhindert werden, Sequenz 5, ansonsten muss Kühlmittel zur Kernkühlung über das CVCS nachgespeist werden (Sequenz 6). Schließt das RSV nicht oder fallen beide Redundanzen des DHRS aus, muss auch Kühlmittel über das CVCS nachgespeist werden (Sequenzen 9 und 12).

Wird kein Kühlmittel nachgespeist, so ergibt sich ein Kernschaden (Sequenzen 3, 4, 7, 8, 10, 11, 13 oder 14). Ist das DHRS nicht funktionsfähig und die RSVs öffnen nicht, so kann der Sicherheitsbehälter geflutet werden, um die Nachzerfallswärme über den Sicherheitsbehälter abzugeben (Sequenz 15). Ein Hochdruckversagen der druckführenden Umschließung ergibt sich, sollte auch das Fluten des Sicherheitsbehälter nicht erfolgen (Sequenz 16).

Falls die RESA nicht erfolgreich ist, eine Redundanz des DHRS arbeitet, ein RSV öffnet und das Kühlmittelinventar ergänzt wird, dann wird ein Kernschadenszustand verhindert (Sequenz 17). Öffnet kein RSV, so muss gesprüht werden, um ein Versagen der druckführenden Umschließung zu verhindern (Sequenz 20). Ohne Nachzerfallswärmeabfuhr kann der Kern über das Einspeisen durch das CVCS gekühlt werden (Sequenz 22), falls ein RSV öffnet. Ansonsten kommt es zum Kernschaden (Sequenzen 23 und 24) oder zu einem Versagen der druckführenden Umschließung, falls kein RSV öffnet (Sequenz 25).

[29] Alternativ zur SB-Drainage über das CFDS wäre ein Absperren des ECCS durch die Betriebsmannschaft denkbar, um sicher zu stellen, dass keines der ECCS-Ventile fehlerhaft öffnet. Allerdings ist die Möglichkeit der Absperrung des ECCS nach den Angaben in der Systembeschreibung, /NUS 20e/, nicht vorgesehen.

Aufgrund der Aktivierung des ECCS ist der RCS für alle Kernschadensendzustände druckentlastet.

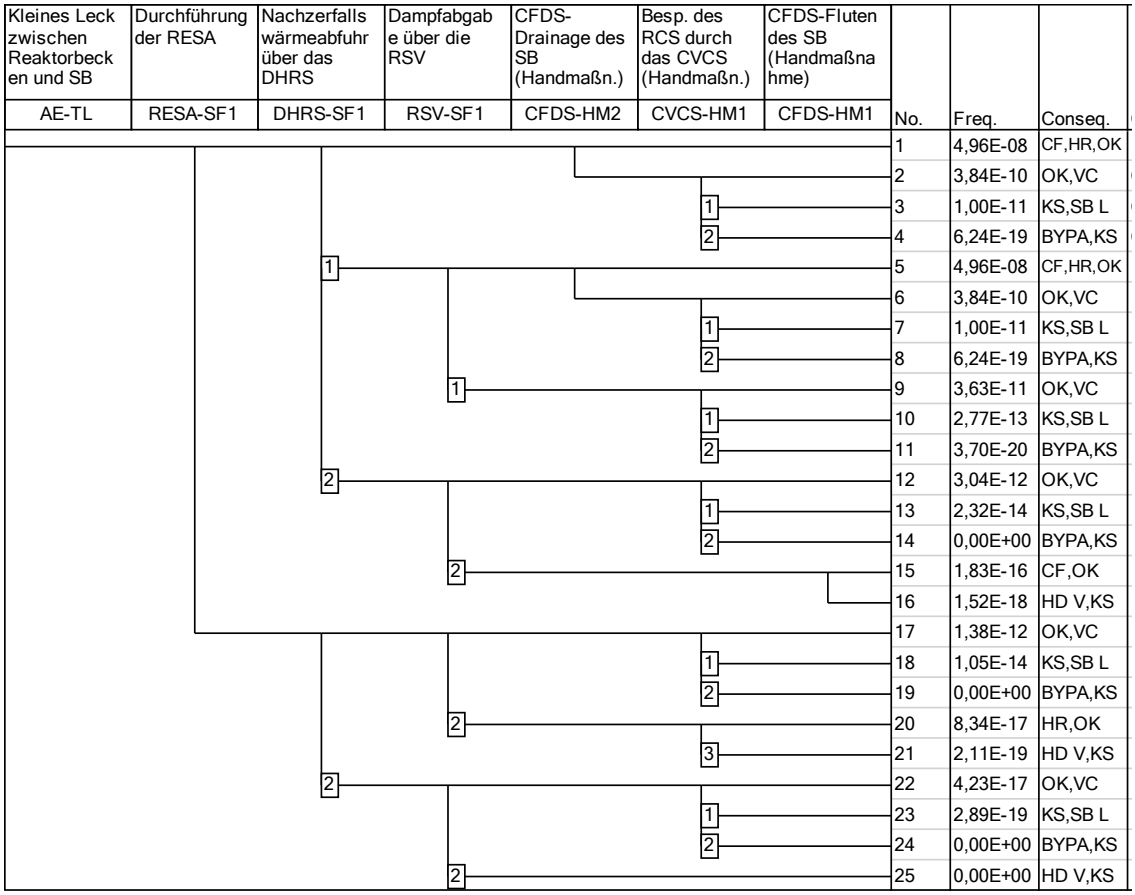


Abb. 7.10 Ereignisablaufdiagramm Sicherheitsbehälterleck

Im Zuge eines Brennelementwechsels ist der Sicherheitsbehälter während der Betriebszustände POS2, POS3 und POS5 geflutet und druckbeaufschlagt. Daraus ergibt sich ein erhöhtes Risiko für ein Leck in der Sicherheitsbehälterhülle. Die Wärmeabfuhr der Nachzerfallsleistung erfolgt über den gefluteten Sicherheitsbehälter in das Reaktorbecken. Kommt es zu einem Leck, so ist mit einer leichten Veränderung des Wärmetransports zwischen RCS und dem Reaktorbecken als Not- und Nachwärmesenke über den Sicherheitsbehälter zu rechnen. Infolgedessen wird sich auch der Naturumlauf im RCS und die Aufwärmspanne über den Kern leicht anpassen. Ein Kernschaden ist nicht zu erwarten.

7.4.10 Funktionales Versagen des RCS-Naturumlaufs

Infolge eines funktionalen Versagens des Naturumlaufs, z. B. durch einen Verlust der Unterkühlung im Steigrohr, kommt es zu einer RESA und zu einem Dampferzeuger-

Abschluss aufgrund der zu niedrigen Umlaufrate des Primärkühlkreislaufs. Ist der Umlauf auch für die veränderten Bedingungen gestört, dann ist mit einem Druckanstieg im RCS zu rechnen. ECCS und CVCS wären für die Störfallbeherrschung viel zu spät verfügbar und es kommt zu einem Brennelementschaden. Stabilisiert sich der Naturumlauf erfolgreich nach der RESA, so orientiert sich der weitere Ereignisbaum, Abb. 7.11, an der allgemeinen Transienten. Der Druckverlauf im RCS führt dabei mit großer Wahrscheinlichkeit zu einem Ansprechen der RSVs.

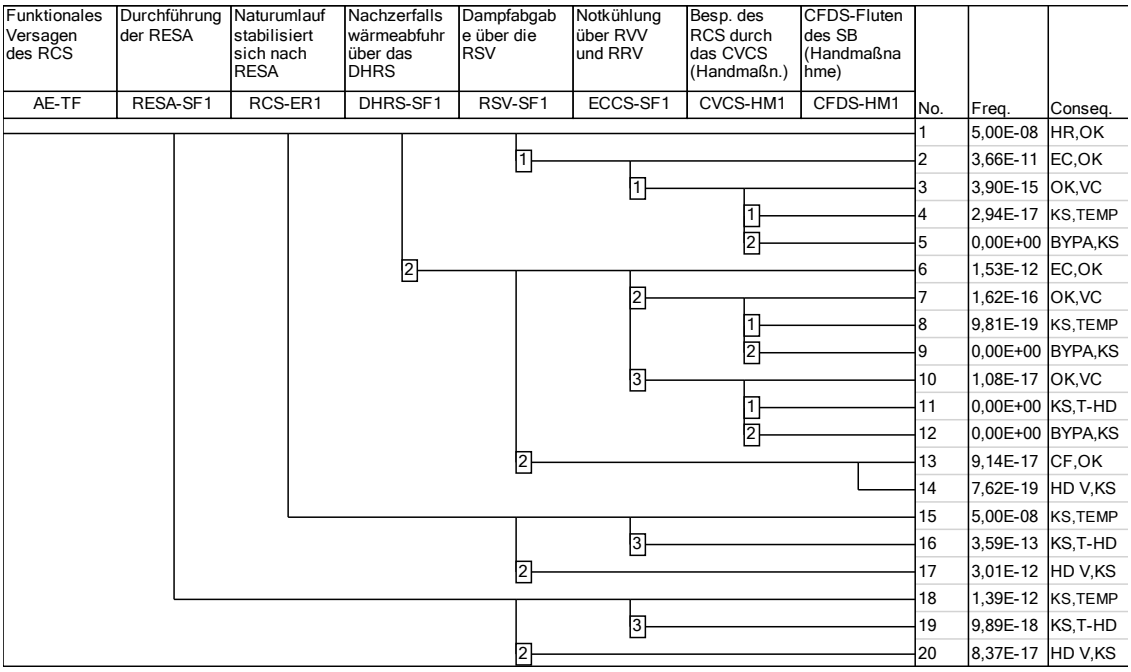


Abb. 7.11 Ereignisablaufdiagramm zum funktionalen Versagen des RCS

Versagt der Naturumlauf im RCS während eines Brennelementwechsels, Mode 5 POS2 bis POS5, so kann durch eine zeitnahe Entladung des Kernes ein Durchfluss und eine Kühlung über das Reaktorbecken wiederhergestellt werden. Hierfür bedarf es zunächst einer Modulöffnung. Stabilisiert sich der Naturumlauf durch diese Maßnahme allerdings nicht, so müssen die einzelnen Brennelemente aus dem Kern entnommen werden (Sequenz 2). Es ergibt sich das Ereignisablaufdiagramm in Abb. 7.12.

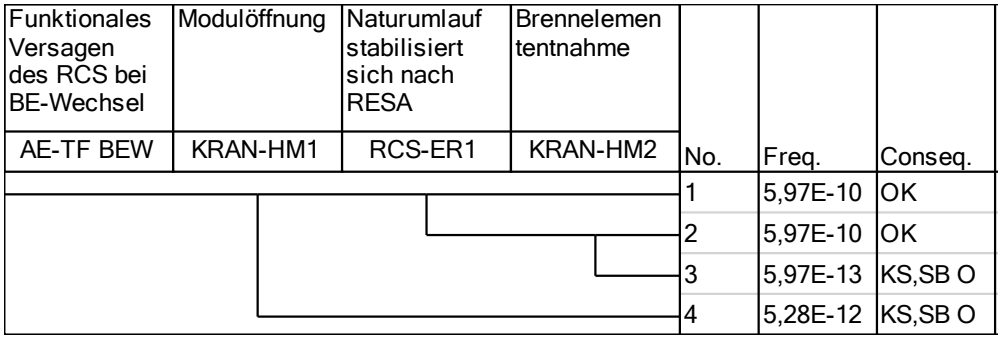


Abb. 7.12 Ereignisablaufdiagramm nach funktionalem Versagen des RCS während eines Brennelementwechsels

7.5 Kühlmittelverluststörfälle

In diesem Abschnitt werden die Ereignisabläufe von KMV aus dem RCS in den angrenzenden Sicherheitsbehälter, siehe Abschnitt 7.5.1, sowie von KMV im angeschlossenen CVCS, vgl. Abschnitte 7.5.2, 7.5.3 und 7.5.4, ein Dampferzeuger-Bypassleck in Abschnitt 7.5.5 und die fehlerhafte Aktivierung des ECCS, das in einen zeitlich verzögerten KMV führt, in Abschnitt 7.5.6 beschrieben.

7.5.1 Kühlmittelverlust in den Sicherheitsbehälter

Ein KMV in den Sicherheitsbehälter unterscheidet sich vom Leck in das Reaktorgebäude dadurch, dass die Funktion des RSVs für die Störfallbeherrschung nicht relevant ist, bzw. durch das Leck umgangen wird (für einen vollständigen Sicherheitsventilersatz ist im Dampfbereich ein äquivalenter Leckquerschnitt, Durchmesser von 7,6 cm /NUS 20c/, erforderlich). Das Ergebnis der Ereignisablaufanalyse ist in Abb. 7.13 gezeigt. Der Störfall wird unabhängig vom Erfolg der RESA über die Wärmeabfuhr durch das ECCS (Sequenz 1) oder über eine Wiederbespeisung des RCS durch das CVCS beherrscht (Sequenz 2). Die Sequenzen 3 und 4 führen nach Ausfall des ECCS und der Einspeisung durch das CVCS in den Kernschaden.

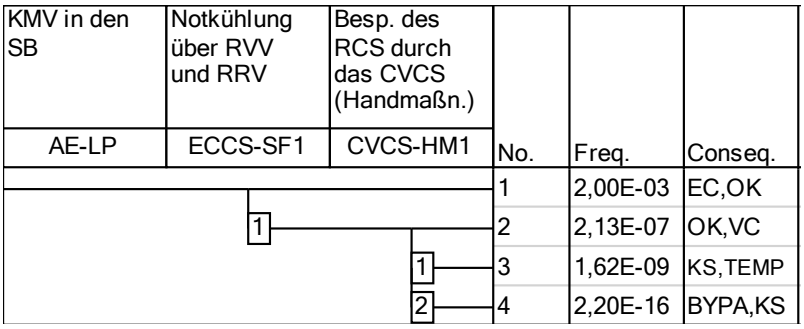


Abb. 7.13 Ereignisablaufdiagramm zum KMV in den Sicherheitsbehälter

7.5.2 Leck der CVCS-Einspeiseleitung in den Sicherheitsbehälter

Ein Leck in der CVCS-Einspeiseleitung ist ein besonderes Leck zwischen RCS und Sicherheitsbehälter. Für dieses auslösende Ereignis reicht das ECCS aus, um den Störfall zu beherrschen (Sequenz 1 in Abb. 7.14). Fällt das ECCS aus, so kann über Sprühen des CVCS in Verbindung mit einer Stabilisierung des Naturumlaufes im RCS (über die Kühlung durch das DHRS), ein Kernschaden verhindert werden (Sequenz 2). Der Ausfall des Sprühens oder des DHRS führt in den Kernschaden (Sequenzen 3, 4 oder 5).

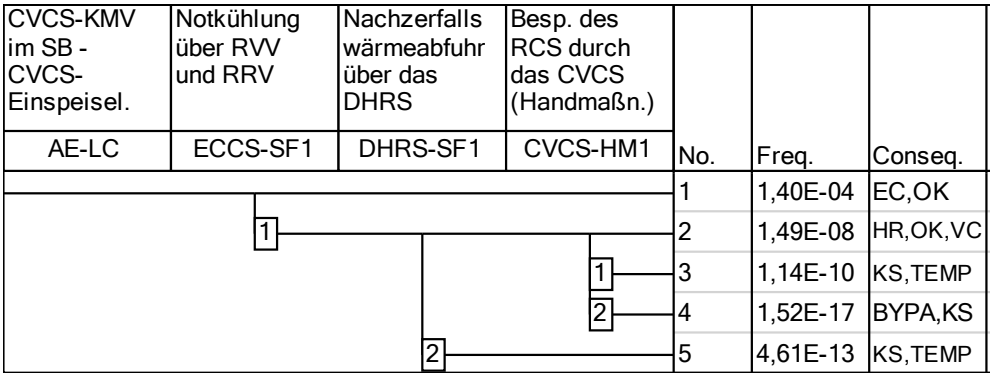


Abb. 7.14 Ereignisablaufdiagramm zum KMV der CVCS-Einspeiseleitung in den Sicherheitsbehälter

7.5.3 Leck der CVCS-Einspeiseleitung in das Reaktorgebäude

Im Unterschied zu Lecköffnungen in den Sicherheitsbehälter sind Lecks aus dem RCS in das Reaktorgebäude nur an Zuleitungen von angeschlossenen Systemen möglich und hierfür kommt nur das CVCS in Betracht. Ein entsprechendes Leck kann über das zugehörige Ventil des Sicherheitsbehälter-Abschlusses abgesperrt werden. Das Ventil schließt nach erfolgter Detektion des Lecks automatisch, kann allerdings auch manuell aktiviert werden.

Die Ereignisablaufanalyse (vgl. Abb. 7.15) beginnt mit der Auslösung der RESA.

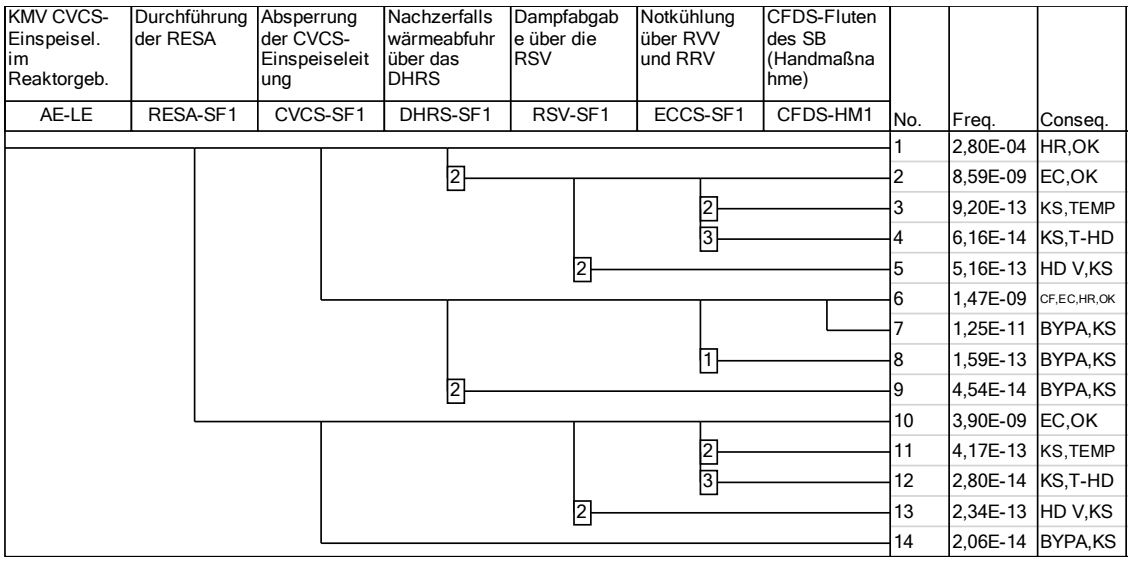


Abb. 7.15 Ereignisablaufdiagramm zum auslösenden Ereignis eines Lecks der CVCS-Einspeiseleitung in den Sicherheitsbehälter

Nach erfolgreicher RESA, Absperrung der CVCS-Einspeiseleitung und Nachzerfallswärmeabfuhr über mindestens eine Redundanz des DHRS ist der Störfall erfolgreich beherrscht (Sequenz 1). Steht das DHRS nicht zur Verfügung, so werden die RSVs angefordert, und nach einer teilweisen Befüllung des Sicherheitsbehälter wird das ECCS automatisch angefordert (Sequenz 2).

Steht das ECCS nicht zur Verfügung, kann aufgrund der Absperrung der CVCS-Einspeiseleitung kein Kühlmittel nachgespeist werden. Es ergibt sich ein Kernschaden (druckentlastet in Sequenz 3 oder druckbelastet in Sequenz 4). Öffnet keines der RSVs, ist ein Hochdruckversagen der druckführenden Umschließung zu erwarten (Sequenz 5).

Schlägt bereits die Absperrung der CVCS-Einspeiseleitung fehl, wird für die Störfallbeherrschung eine alternative Einspeisung benötigt, um das abfließende Kühlmittel nachzuspeisen. Das CFDS kann über ein (geregeltes) Fluten des Sicherheitsbehälter die Nachspeise von Kühlmittel leisten. Der Störfall wird beherrscht, wenn Kühlmittel über das CFDS in den Sicherheitsbehälter eingespeist wird und das DHRS und das ECCS verfügbar sind (Sequenz 6). Der Ausfall eines der Systeme führt in den Kernschaden mit Sicherheitsbehälter-Bypass (Sequenzen 7, 8 oder 9).

Im Fall eines ATWS ist die Absperrung der CVCS-Einspeiseleitung, die Funktion eines RSV und das ECCS erforderlich (Sequenz 10). Schlägt die Notkühlung über das ECCS fehl, so ist mit einem Kernschaden zu rechnen (Sequenz 11 für druckentlastet und Sequenz 12 für Drücke über 130 bar im RCS). Sind beide RSVs unverfügbar, so kommt es zu einem Versagen der druckführenden Umschließung (Sequenz 13). Ein Kernschaden mit Sicherheitsbehälter-Bypass ist auch zu erwarten für den Fall ATWS+Ausfall der Absperrung der CVCS-Einspeiseleitung (Sequenz 14).

7.5.4 Leck der CVCS-Entnahmeleitung in das Reaktorgebäude

Ein alternativer KMV in das Reaktorgebäude ergibt sich durch ein Leck der CVCS-Entnahmeleitung. Das Ereignisablaufdiagramm ist in Abb. 7.16 dargestellt.

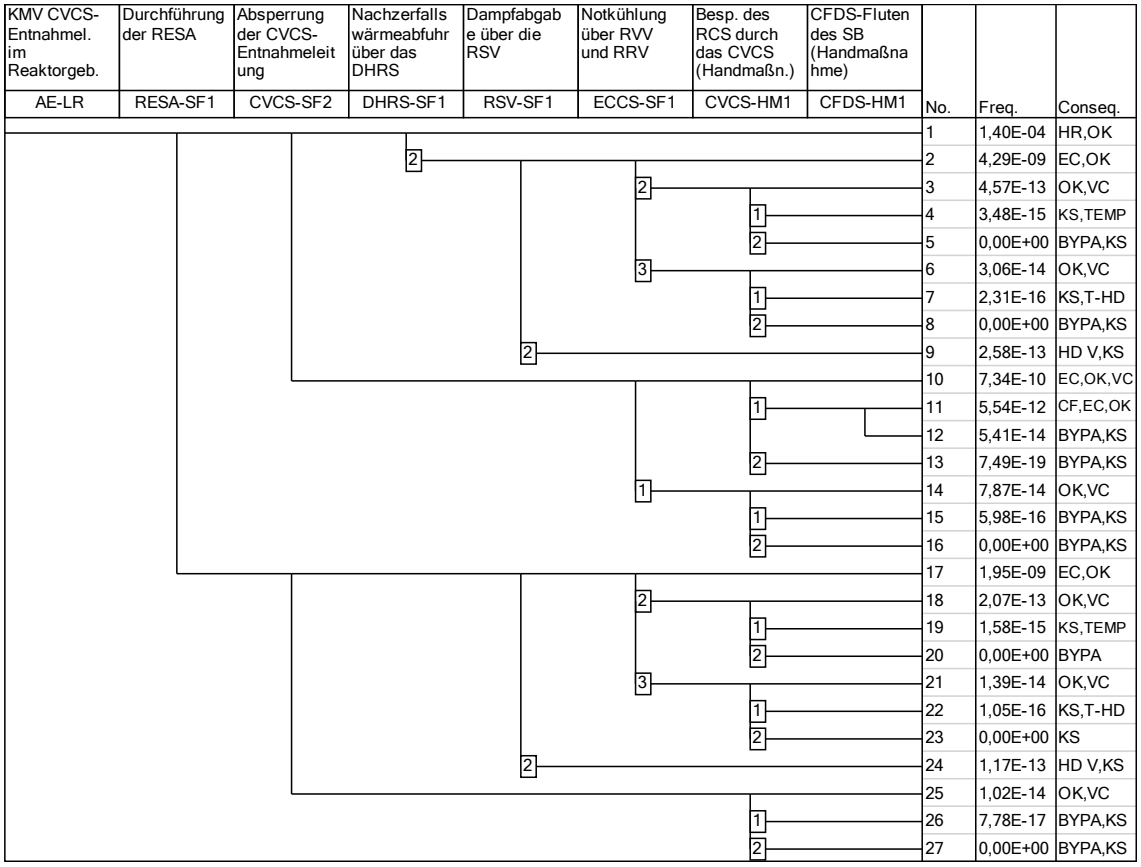


Abb. 7.16 Ereignisablaufdiagramm zum auslösenden Ereignis eines Lecks der CVCS-Entnahmeleitung in den Sicherheitsbehälter

Für dieses auslösende Ereignis steht die CVCS-Einspeiseleitung für eine Wiederbespeisung des RCS zur Verfügung (sofern diese nicht von einem Ausfall gemäß CVCS-T01

betroffen ist). Für die Störfallbeherrschung sind eine RESA, die Absperrung der CVCS-Entnahmeleitung und eine Redundanz des DHRS ausreichend (Sequenz 1).

Der Ausfall des DHRS hat zur Folge, dass mindestens ein RSV öffnet und das ECCS aktiviert wird (Sequenz 2). Das Fehlschlagen der Notkühlung über das ECCS kann über eine Einspeisung durch die CVCS-Einspeiseleitung des CVCS ausgeglichen werden (Sequenzen 3 oder 6). Fällt die Einspeisung durch das CVCS komplett aus, so kommt es zum Kernschaden (druckentlastet in den Sequenzen 4, 5 oder 8, druckbelastet in Sequenz 7).

Defekte RSVs führen in ein Versagen der druckführenden Umschließung (Sequenz 9). Bei Nicht-Absperrung der CVCS-Entnahmeleitung, aber erfolgreicher Notkühlung über das ECCS und Kühlmittel-Nachspeisung durch das CVCS (Sequenz 10) oder das Fluten des Sicherheitsbehälter über das CFDS (Sequenz 11) wird ein Kernschaden verhindert. Das Versagen beider Einspeisemöglichkeiten hat einen Kernschaden mit Sicherheitsbehälter-Bypass zur Folge (Sequenzen 12 oder 13).

Ohne ECCS reicht die Einspeisung durch das CVCS aus (aufgrund der Annahme eines „kleinen“ Lecks), um den Abfluss durch das Leck zu überspeisen (Sequenzen 14). Keine Einspeisung hat auch hier einen Kernschaden mit Sicherheitsbehälter-Bypass zur Folge (Sequenzen 15 und 16). Im Fall eines ATWS reicht die Kombination der Absperrung der CVCS-Entnahmeleitung und erfolgreiche Nachzerfallswärmeabfuhr über das DHRS nicht für die Störfallbeherrschung aus.

Die Sequenzen 17 bis 24 ergeben sich analog zu den Sequenzen 2 bis 9 unabhängig von der Verfügbarkeit der DHRS. Bei Fehlschlagen der Absperrung der CVCS-Entnahmeleitung ist beim ATWS die Einspeisung von Kühlmittel über das CFDS in den Sicherheitsbehälter für die Störfallbeherrschung nicht ausreichend, entsprechend ergeben sich nur die Möglichkeiten der Einspeisung über das CVCS (Sequenz 25) oder ein Kernschaden mit Sicherheitsbehälter-Bypass (Sequenzen 26 und 27).

7.5.5 Dampferzeuger-Bypassleck

Für das auslösende Ereignis eines Dampferzeuger-Bypasslecks kann davon ausgegangen werden, dass nur ein einzelnes Sekundärkühlkreis-Kühlrohr betroffen ist. Der Grund für die Betrachtung eines Lecks in nur einem Kühlrohr (Querschnitt von 10 bis 15 cm /NUS 20c/) und nicht in mehreren Kühlrohren liegt im Aufbau des Dampferzeugers.

Typischerweise fließt in einem DWR das RCS-Kühlmittel durch die Heizrohre, im SMR von NuScale fließt hingegen das Speisewasser des Sekundärkühlkreises durch die Rohre (in diesem Fall mit kühlender Wirkung). Das Kühlmittel des RCS wird für die Wärmeabgabe um die Kühlrohre herumgeleitet. Der höhere Druck im RCS lastet damit auf der Außenfläche der Kühlrohre, im Fall eines Dampferzeuger-Bypasslecks kommt es zu einem Versagen nach innen, umliegende Kühlrohre sind in der Folge nicht von diesem Implosions-Ereignis betroffen /NUS 20/.

Das Ereignisablaufdiagramm in Abb. 7.17 kann analog zum Diagramm in Abb. 7.16 für das Leck in der CVCS-Entnahmeleitung verstanden werden. Einzige Unterschiede ergeben sich durch die andere Art der Absperrung des Dampferzeuger-Bypasslecks durch die Dampferzeuger-Absperrung DE-SF1 und eine höhere Ausfallwahrscheinlichkeit für das DHRS DHRS-SF1, da bereits eine Redundanz leckbedingt nicht zur Verfügung steht. Eine Umgehung des Sicherheitsbehälter ist grundsätzlich auch möglich, wenn der Dampferzeuger-Bypassleckabschluss nicht erfolgt.

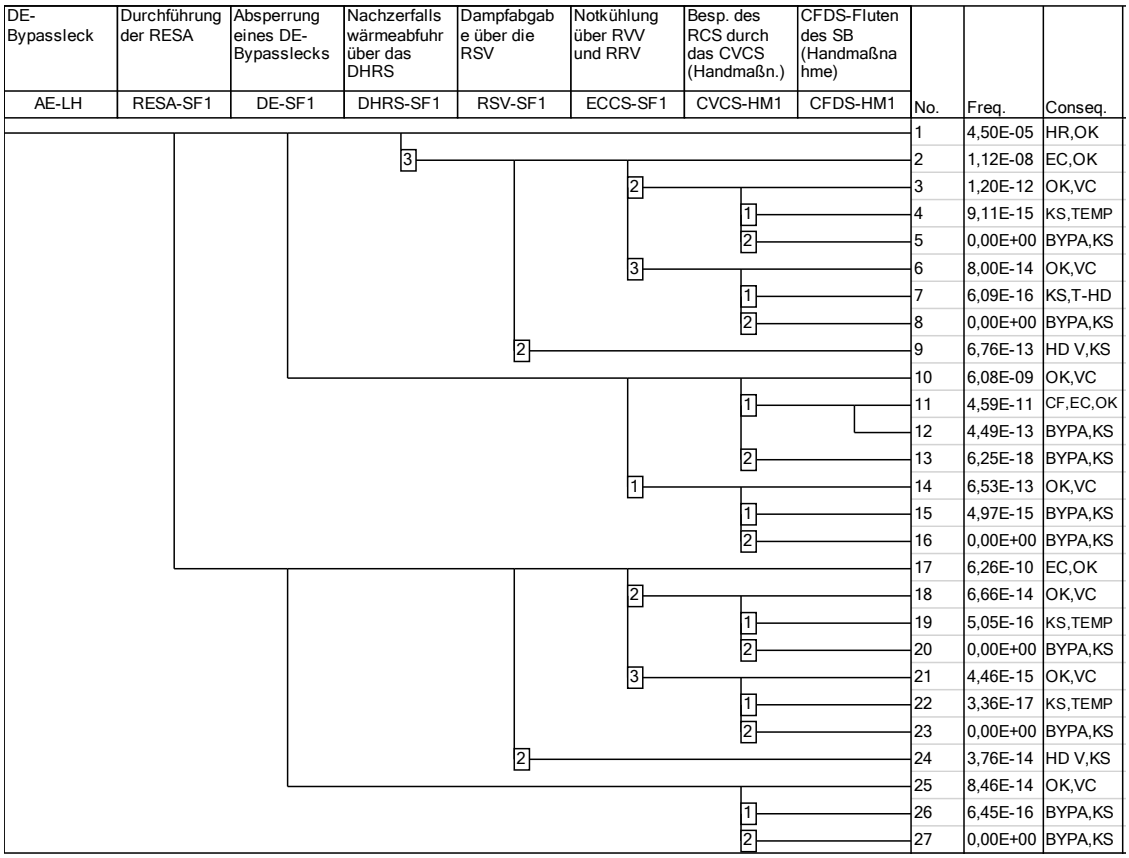


Abb. 7.17 Ereignisablaufdiagramm zum Dampferzeuger-Bypassleck

7.5.6 Fehlerhafte Aktivierung des Notkühlsystems ECCS

Eine fehlerhafte Aktivierung des ECCS wird zunächst mit Hilfe des IAB verhindert. Öffnet eines der ECCS-Ventile fehlerhaft durch ein Versagen es IAB, so kommt es zu einem KMV in den Sicherheitsbehälter, Sequenz 26 in Abb. 7.18. Dieser Fall wird in Abschnitt 7.5.1 näher untersucht.

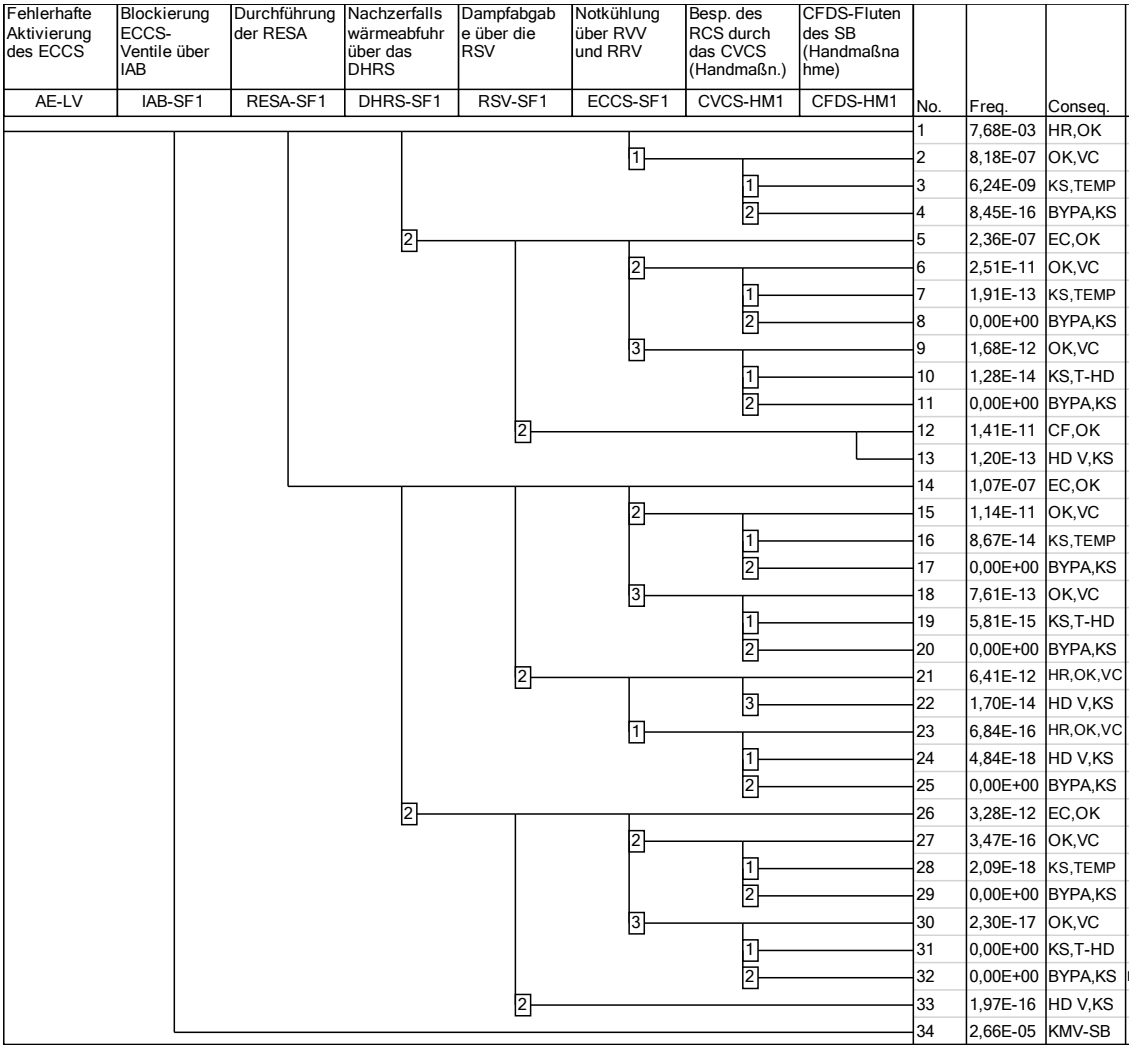


Abb. 7.18 Ereignisablaufdiagramm zur fehlerhaften Aktivierung des ECCS

Ist dies nicht der Fall, so wird der Störfall analog zu einer allgemeinen Transiente betrachtet, mit der Ausnahme, dass die ECCS-Ventile nach erfolgtem Druckabbau im RCS öffnen. Gemeinsame Ausfälle des ECCS und CVCS führen in den Kernschaden, Sequenzen 3, 4, 7, 8, 10, 11, 16, 17, 19, 20, 22, 24, 25, 28, 29, 31 und 32. Ein erfolgreicher Einsatz des DHRS reicht für die Störfallbeherrschung aufgrund der Auslösung des ECCS nicht aus. Für den Erfolg nach einem Versagen beider RSVs ist ein Druckhalter-Sprühen notwendig (Sequenz 21).

7.6 Ereignisse im Nichtleistungsbetrieb

Entsprechend Tab. 6.5 sind einige auslösende Ereignisse auch für den Nichtleistungsbetrieb möglich. Die Betrachtungen in Abschnitt 7.4 können mit einigen kleinen Anpassungen bzw. Berücksichtigungen der unterschiedlichen System-Ausfallhäufigkeiten auch für den Nichtleistungsbetrieb verwendet werden. Insbesondere befinden sich Erläuterungen zum Nichtleistungsbetrieb in den Abschnitten 7.4.3, 7.4.4, 7.4.9 und 7.4.10.

Anpassungen der System-Ausfallwahrscheinlichkeiten gelten für:

- RTS-T01: Für die unterkritischen Zustände POS1-POS6 wird keine RESA benötigt.
- DHRS-T01 bis DHRS-T04: Das DHRS wird für die Zustände POS2-POS5 nicht benötigt, die Nachzerfallswärmeabfuhr ist gesichert, damit wird ein Ausfall nicht unterstellt.
- CFDS-T01: Der Sicherheitsbehälter ist in den Zuständen POS2-POS5 bereits geflutet, somit wird ein Ausfall nicht unterstellt.
- ECCS-T01 und ECCS-T03: Die ECCS-Ventile werden bei geflutetem Sicherheitsbehälter POS2-POS5 nicht benötigt. Somit wird ein Ausfall nicht unterstellt.
- RCS-T01 und RCS-T02: Für alle druckentlasteten Zustände POS2-POS6 ist nicht mit einem Ansprechen der RSVs zu rechnen und ein HD-Versagen der druckführenden Umschließung wird in Abschnitt 7.6.2 gesondert betrachtet.
- CVCS-T01: Bei einem gefluteten Sicherheitsbehälter, POS2-POS5 ist das CVCS nicht verfügbar, eine Kühlmittelentnahme oder Einspeisung ist für die Störfallbeherrschung weder möglich noch nötig.

7.6.1 Fall eines Moduls in den Betriebs- oder Brennelementbeladebereich

In den Anlagen- bzw. Modulbetriebszuständen POS3 und POS5 ist als auslösendes Ereignis der Fall des Reaktormoduls in den Betriebs- oder Brennelementbeladebereich möglich. Der Fall eines Moduls ist ein sekundäres auslösendes Ereignis, das auf Ereignisse wie beispielsweise eine zu hohe Brückengeschwindigkeit, eine Überladung des Krans oder eine zu hohe Geschwindigkeit des Hebezuges folgt /NUS 20/. Fällt das Modul auf die Seite, so ist mit einer Freilegung des Kerns und in Folge mit einem Kernschaden zu rechnen. Im Betriebsbereich wird das Modul nur 30 cm angehoben und es besteht die Möglichkeit, dass das Modul den Fall unbeschadet und aufrecht übersteht.

Im Brennelementwechselbecken gibt es eine höhere Wahrscheinlichkeit für das Fallen auf die Seite des Moduls aufgrund der höheren Modulanhebungen. Konservativ ist für jeden Fall eines Moduls in die waagrechte Position mit einem Kernschaden und einem Versagen des Sicherheitsbehälter auszugehen, der Kernschadensendzustand ist damit der Schwerwiegendste: Sicherheitsbehälterversagen. Dagegen führt der Fall eines teilweise geöffneten Moduls im Brennelementbeladebereich während des Betriebszustandes POS4 zu keinem Kernschaden, da Beckenwasser über die geöffneten ECCS-Ventile weiterhin zirkulieren kann und damit die Kernkühlung sichergestellt ist /NUS 20/.

Des Weiteren kann der Fall des oberen Behälterteils des Sicherheitsbehälter auf das Modul während der Modulöffnung oder -schließung nur einen mechanischen Schaden an den Brennelementen verursachen, eine sehr geringe Freisetzung an Spaltprodukten könnte folgen /NUS 20/. Eine Behinderung der Kernkühlung wird nicht angenommen /NUS 20/. POS4 wird demnach aufgrund des geringen Freisetzungspotenzials von höchstens mechanischen Schäden an einzelnen Brennelementen nicht weiter untersucht.

Ein Risiko für mehrere Module ergibt sich nur für den Fall eines Moduls in den Betriebsbereich. Entsprechend der Ausführungen in der NuScale-PSA /NUS 20/ sind drei Szenarien denkbar, diese Szenarien mit zwei oder drei beteiligten Reaktormodulen sind in Abb. 7.19 veranschaulicht:

- Das betroffene Modul fällt entlang der Mitte des Reaktorbeckens, trifft dabei kein anderes Modul und kommt horizontal zur Ruhe,
- Das betroffene Modul berührt ein anderes Modul auf Höhe der Plattform, beide Module werden beschädigt (die drei Fälle auf der linken Seite in Abb. 7.19).
- Das betroffene Modul trifft ein anderes Modul auf Höhe der Plattform. Der Fuß des fallenden Moduls gleitet über den Boden des Reaktorbeckens und trifft auf ein drittes Modul (gezeigter Fall auf der rechten Seite in Abb. 7.19).

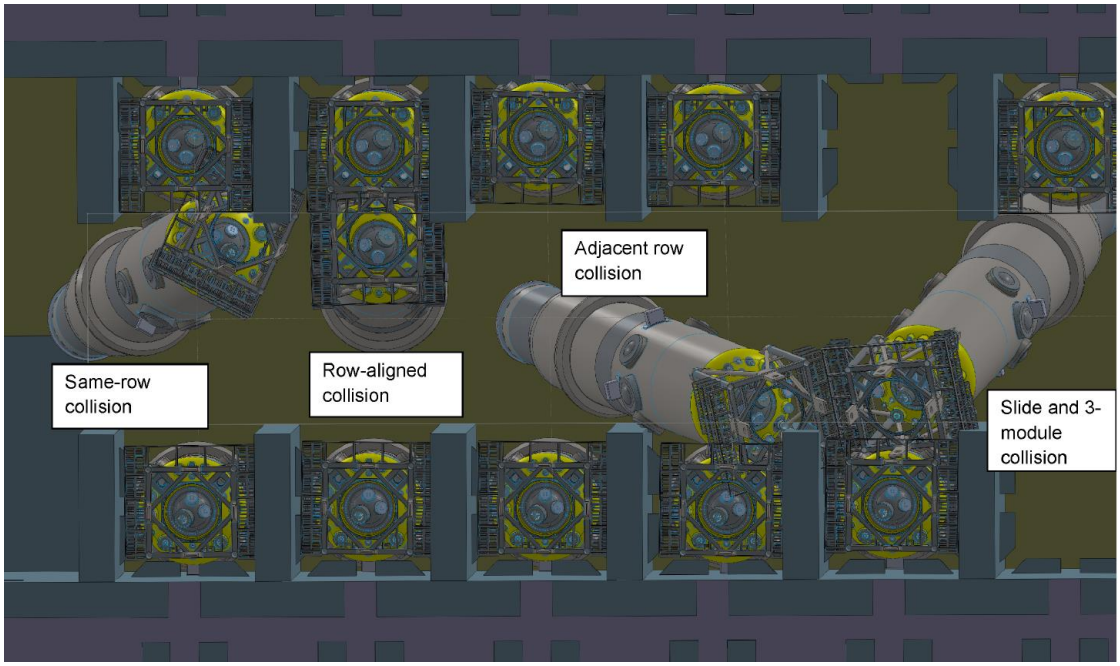


Abb. 7.19 Mögliche Fallszenarien für Reaktormodule im Betriebsbereich /NUS 20/

Mit einem Kernschaden ist für alle waagerecht zum Liegen kommenden Module zu rechnen, da ein Ausfall aller Systeme mit Naturumlauf sehr wahrscheinlich ist. Nach Experteneinschätzung ist mit Kernschäden in teilweise aufrechtstehenden Modulen nicht zu rechnen /NUS 20/. Die Aufprallgeschwindigkeiten sind auch zu gering, um eine Beschädigung des Sicherheitsbehälter zu verursachen. Die getroffenen Module bleiben höchstwahrscheinlich in den Modulbuchten in (nahezu) aufrechter Position.

7.6.2 Überdruck im kalten Reaktorkühlsystem RCS

Kommt es in der Abkühl- oder Aufwärmphase (POS2 oder POS6) während eines Brennelementwechsels zu einem fehlerhaften Druckanstieg im RCS (z. B. durch eine fehlerhafte Heizung im Druckhalter), dann wird ab einer bestimmten temperaturabhängigen Druckgrenze der LTOP aktiv und fordert die Öffnung der RVVs an. Ein Versagen des LTOP hat ein HD-Versagen der druckführenden Umschließung zur Folge.

Überdruck im kalten RCS	Druckentlastung des RCS bei niedrigen Temperature			
AE-NÜ	LTOP-SF1	No.	Freq.	Conseq.
		1	1,20E-07	OK
		2	1,21E-10	HD V,KS

Abb. 7.20 Ereignisablaufdiagramm zum Überdruck im RCS

8 System- und Fehlerbaumanalysen

Ein besonderes Merkmal von SMRs sind die verschiedenen passiven Systeme, die zum Einsatz kommen. Passive Systeme gelten meist als besonders zuverlässig, da auf den Einsatz von aktiven Elementen, z. B. Pumpen, in den Systemen verzichtet wird. Die Zuverlässigkeit der passiven Systeme des NuScale-SMR wird in Abschnitt 8.1 diskutiert, allerdings sind für die Quantifizierung der Zuverlässigkeit weitere thermohydraulische Zuverlässigkeitsanalysen notwendig.

In Abschnitt 8.2 werden die Fehlerbaumanalysen beschrieben, die zur Bestimmung der Systemausfallwahrscheinlichkeiten herangezogen werden. Diese Fehlerbäume sind die Basis für die Verzweigungswahrscheinlichkeiten der Ereignisablaufanalysen aus Kapitel 7. Abschnitt 8.3 beschreibt die System- und Fehlerbaumanalysen für Handmaßnahmen, darunter der Einsatz des CVCS zur Kühlmitteleinspeisung und das CFDS zur Sicherheitsbehälterflutung.

8.1 Zuverlässigkeit passiver Systeme

Passive Systeme können entsprechend /IAE 91/ (siehe auch /BEC 17/) in vier Kategorien eingeteilt werden:

A Passive Komponenten ohne strömende Flüssigkeiten, bewegliche Objekte, Kraftübertragung oder Energiespeicherung. In diese Kategorie fallen physikalische Barrieren, wie Brennstoffhülle, druckführende Umschließung, Rohre und Behälter. Entsprechende Systeme des NuScale-Reaktors sind die Brennstoffhüllrohre, das RCS und der Sicherheitsbehälter, Details finden sich in Abschnitt 8.1.8.

B Das System verwendet strömende Flüssigkeiten basierend auf physikalischen Gegebenheiten. In diese Kategorie fallen Naturumlaufkühlsysteme. Es wird nicht zwischen Einphasen- und Zweiphasen-Naturumläufen unterschieden. Der NuScale Reaktor besteht aus drei Systemen der Kategorie B: Der Primärkühlkreislauf, das DHRS und das ECCS, sofern die Aktivierung des DHRS und des ECCS separat betrachtet werden. Die genannten Systeme mit Naturumlauf sind in Abschnitt 8.1.1 näher analysiert.

C Das System beinhaltet bewegliche mechanische Komponenten, allerdings ohne elektronische Steuerungslogik und die Funktion hängt nicht von einer externen Stromversorgung ab. In diese Kategorie fallen die RSVs zum Schutz der Integrität

des RCS vor einem Überdruck im Leistungsbetrieb und das IAB. Diese Systeme werden in Abschnitt 8.1.6 bzw. Abschnitt 8.1.7 untersucht.

D Die Kategorie D ist gekennzeichnet von der Möglichkeit zur aktiven Ansteuerung der passiven Komponenten, die Energieversorgung für die Funktion der Komponente muss aus einem Speichermedium verfügbar sein. In diese Kategorie fallen unter anderem das DHRS und das ECCS des NuScale-Reaktors unter Berücksichtigung der Systemaktivierung. Die Systemfehlerbäume sind in den Abschnitten 8.2.2 und 8.2.3 analysiert.

8.1.1 Systeme mit Naturumlauf im NuScale-Reaktor

Der Naturumlauf folgender Systeme soll genauer betrachtet werden:

- der Primärkühlkreislauf im Leistungs- und im Nachzerfallswärmeabfuhrbetrieb,
- der DHRS-Kreislauf nach erfolgreicher Aktivierung des DHRS und
- der Notkühlkreislauf nach erfolgreicher Aktivierung des ECCS.

Der Primärkühlkreislauf ist ein Einphasennaturumlauf. Beim Notkühlkreislauf und dem DHRS-Kreislauf handelt es sich um Zweiphasennaturumläufe.

8.1.2 Notwendige Schritte zur Durchführung einer Zuverlässigkeitsbestimmung der Systeme mit Naturumlauf

Die Untersuchung soll auf der Methode des APSRA beruhen (nähere Informationen in /BEC 17/ bzw. /NAY 07/). Die Methode besteht aus acht Schritten, wie in Abb. 8.1 gezeigt.

Im ersten Schritt werden die passiven Systeme und deren Funktionalität genauer untersucht. Die entsprechenden Systembeschreibungen finden sich in den Abschnitten 3.2.2 und 3.2.4.

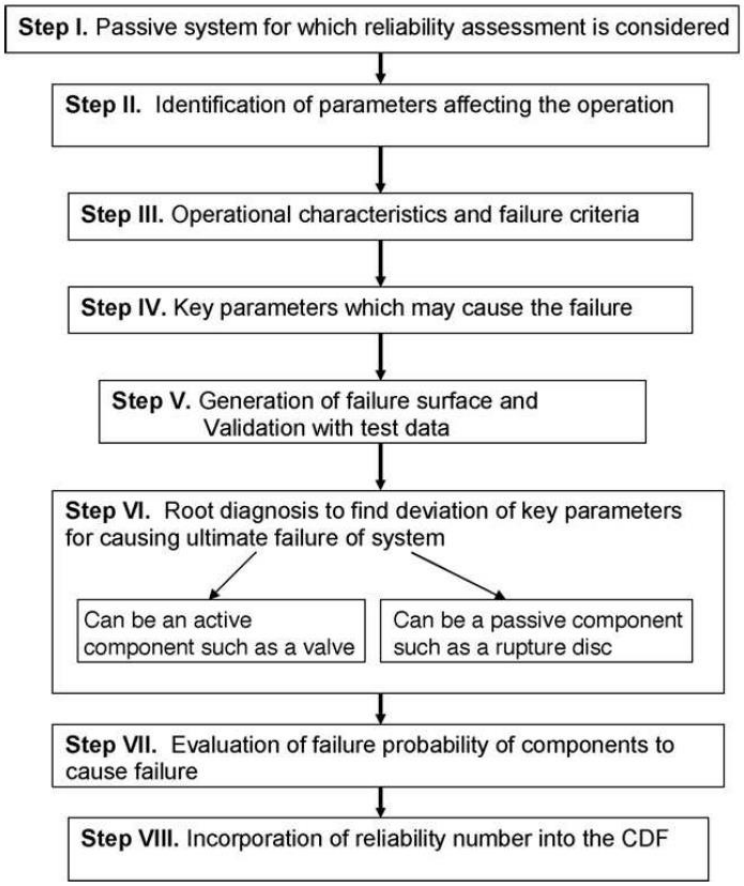


Abb. 8.1 Schritte zur Durchführung einer Zuverlässigkeitsanalyse eines passiven Systems über APSRA /NAY 07/

Der dritte Schritt besteht in der Festlegung auf Ausfallkriterien der Systeme mit Naturumlauf. Als Ausfallkriterium kommt die nicht vollständig abgeführte Nachzerfallswärme (bzw. im Fall eines Ausfalls der RESA oder einer Rekritikalität nach Ausfall eines Steuerstabs die nicht vollständig abgeführte Reaktorleistung) in Betracht. Innerhalb der ersten Sekunden (bis ca. 100 s nach Störfalleintritt) darf im DHRS allerdings die abgeführte Leistung geringer ausfallen, bis zur Stabilisierung der Umlaufrate. Die Kernleistung muss nach der Einschwingphase für 72 h vollständig abgeführt und der Druck und die Temperatur im RCS absinken. Dies gilt auch für den Fall eines ATWS.

Die Kernleistung einer möglichen Rekritikalität nach Ausfall eines Abschaltstabes hängt von der Moderatortemperatur ab und ist in Abb. 8.2 gezeigt, /BOT 18/. Die erzeugte Leistung kann entweder durch das ECCS oder das DHRS abgeführt werden. Die Moderatortemperaturen sind für den Betrieb des ECCS geringer als für das DHRS, da der RCS über die ECCS-Ventile druckentlastet wurde.

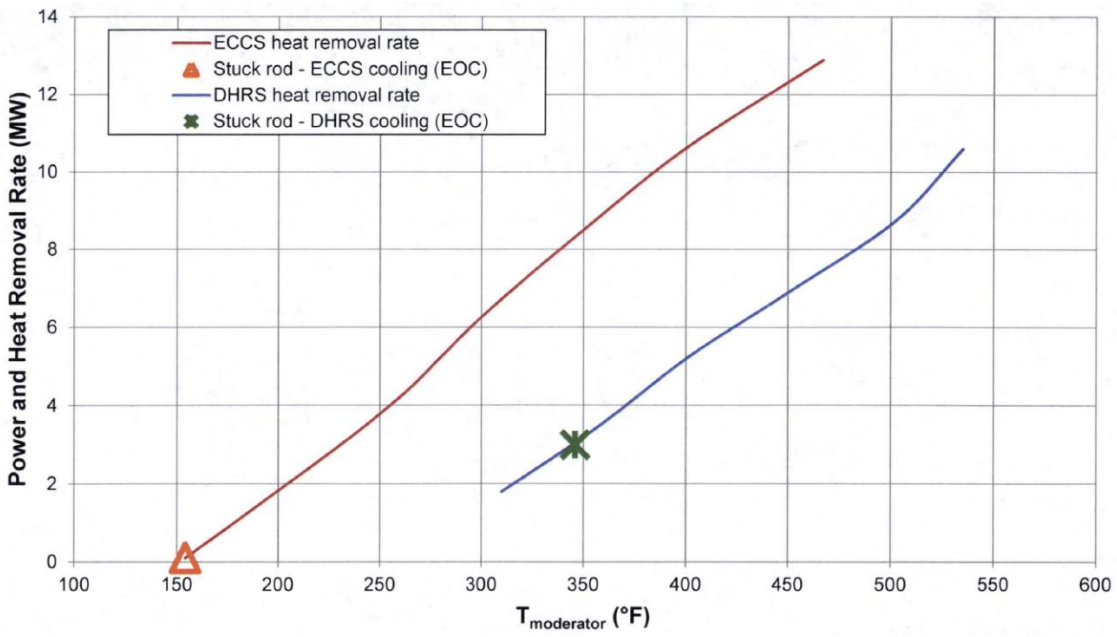


Abb. 8.2 Kernleistung und Kühlleistung des DHRS und ECCS im Fall einer Rekritikalität mit fehlerhaft nicht eingefallen Steuerstab höchster Kritikalität, nach /BOT 18/

Im vierten Schritt werden die Hauptparameter bestimmt, die ein Versagen verursachen könnten. Das Ergebnis dieser Parameteranalyse ist in Tab. 8.1 gezeigt. Hier wurden die Parameterlisten von FMEA und Hazop aus /IAE 14/ als Grundlage verwendet und auf die Anwendbarkeit für die Naturumläufe des NuScale-Reaktors untersucht. Ein Zusammenspiel der Faktoren Ventilausfälle, Kühlmittelinventar und Vorhandensein nichtkondensierbarer Gase (möglicher Ausfall der Füllstandssensoren) könnte in diesem Zusammenhang besonders interessant sein. Die Variation dieser Parameter innerhalb der Unsicherheitsbänder in einer Unsicherheitsanalyse können die Basis für die Abtastung der Versagensoberfläche sein. Die verschiedensten Kombinationen aus Ventilausfällen stellen diskrete Größen der Analyse dar. Die Durchführung von thermohydraulischen Unsicherheitsanalysen erfordert eine genaue Detailkenntnis der Systeme, die in der veröffentlichten Unterlagen nicht ausreichend gegeben ist.

Tab. 8.1 Ursachen für Systemausfälle von Naturumläufen

Ursachen, Parameter	Auswirkungen, Parameter	Anwendbarkeit auf NuScale	Zu untersuchen?
Leitungsversagen, Lecks, Versagen der Umschließung, Risse	Ausfall einer Redundanz des Systems, Verminderung der Kühlleistung durch Verlust an Kühlmittel, Durchflussrate verringert; möglicher Druckaufbau im DHRS bei Dampferzeuger-Bypasslecks und Kühlmittelabfluss aus dem RCS.	Als auslösendes Ereignis zu betrachten, ansonsten System gegen maximale Systemdrücke bis 145 bar ausgelegt, Lecküberwachung ist redundant vorhanden (DHRS), Lecks im ECCS nicht möglich und im Primärkühlkreislauf aufgrund hoher Druckauslegung nur bedingt möglich.	Nein
Verstopfung einer oder mehrerer Leitungen	Ausfall oder verminderte Kühlleistung des DHRS, Verstopfung der RRV kann in einen Ausfall des ECCS führen.	Verstopfungen sind vergleichbar mit Ausfällen von Ventilen, allerdings viel unwahrscheinlicher, da nur aufgrund eines Komponentenversagens mit Materialeintrag möglich, z. B. dem Versagen der Umschließung oder eines Ventils. Das Kühlmittel wird im Betrieb gereinigt und die Systemfunktionen regelmäßig überprüft, eine zehnprozentige Verstopfung wird konservativ in die Sicherheitsanalysen mit einbezogen. Verstopfen könnten insbesondere die Sekundärkühlrohre der Dampferzeuger oder die RRV	Ja, Verstopfung der Dampferzeugerrohre wird in NuScale-Analysen berücksichtigt. Darüber hinaus sollten Ventilausfälle berücksichtigt werden.
Oberflächenrauhigkeit aufgrund chemischer Prozesse	Erhöhte Druckverluste im DHRS, niedrigere Wärmestromdichten	Die Kühlmittelchemie wird sauerstoffarm eingestellt. Im DHRS erfolgt der wesentliche Teil der Druckverluste an der Düse, im ECCS sind keine Rohre vorhanden und Druckverluste ergeben sich im Wesentlichen an den Ventilen. Der RCS wird nicht wesentlich durch erhöhte Oberflächenrauhigkeiten gestört.	Nein
Thermische Schichtung des Reaktorbeckens	Höhere Temperaturen an der Sekundärseite der Wärmetauscher	Konservative NuScale-Analysen verwenden hohe Reaktorbeckentemperaturen von 93 °C, der maximale Unsicherheitsbereich ist damit abgedeckt.	Nein

Ursachen, Parameter	Auswirkungen, Parameter	Anwendbarkeit auf NuScale	Zu untersuchen?
Anteil nicht-kondensierbarer Gase im System	Zusätzliche Druckverluste (zusätzliche Modellunsicherheiten) und verminderte Kondensationsraten von Frischdampf, Durchflussraten geringer, Druckaufbau, niedrige Wärmestromdichten.	Die erfolgreiche Entlüftung des DHRS wird mit Füllstandssensoren überwacht (maximal 0,422 kg nicht-kondensierbare Gase bleiben unentdeckt). Die gelöste Konzentration von nicht-kondensierbaren Gasen im Kühlmittel wird überwacht und ist weit unter der Löslichkeitsgrenze. Druckverluste durch die nicht-kondensierbaren Gase sind aufgrund des Zweiphasenbetriebes nicht zu erwarten. Der Sicherheitsbehälter wird im Betrieb vakuumisiert und die nicht-kondensierbaren Gase im RCS werden im Betrieb entfernt.	Ja, wird in den NuScale-Analysen berücksichtigt; zusätzlich ist ein möglicher Ausfall der Füllstandsüberwachung zu analysieren.
Wärmeverluste	Zusätzliche Wärmeverluste reduzieren die Umlaufrate des Systems, Durchflussraten fallen dadurch geringer aus.	Das ECCS verfügt über keine Rohrleitungen, Wärmeverluste zwischen RCS und Sicherheitsbehälter an der RCS-Außenhülle können die Umlaufraten im RCS und ECCS beeinflussen. Im DHRS sind die Wärmeverluste zwischen Rohrleitungen und Sicherheitsbehälter oder Rohrleitungen und Reaktorgebäude zu beachten (hauptsächlich in der Frischdampf-Leitung).	Ja
Unsicherheit in den Anlagenparametern Reaktorleistung, Nachzerfallsleistung bzw. Rückwirkungskoeffizienten, Temperatur im RCS	Niedrige Reaktorleistungen können sich auf die Umlaufraten im ECCS und RCS auswirken. Niedrige Temperaturen im RCS können sich negativ auf die Umlaufrate im DHRS auswirken	NuScale-Analysen verwenden Reaktorleistungen von 102 % und Nachzerfallsleistungen von 120 % gegenüber dem Standard ANS 1973. Es ist nicht klar, ob der obere Maximalwert bzgl. der Parameterunsicherheit immer konservativ ist. Allerdings gibt es darüber hinaus NuScale-Analysen für den Teillastbetrieb	Ja, wird berücksichtigt in NuScale-Analysen.
Unsicherheit in den Anlagenparametern bzgl. Ventilöffnungszeiten	DHRS: Wasserinventar und Druck im Sekundärkühlkreis sind betroffen mit Auswirkungen auf den Wärmeübergang und die Durchflussrate.	Die Dampferzeuger-Abschlussventile (für Frischdampf und Speisewasser) schließen anforderungsgemäß innerhalb von 7 Sekunden nach Initiierung. Durch den gleichzeitigen Abschluss von Frischdampf und Speisewasser kann das Inventar in den Dampferzeuger näherungsweise erhalten werden. Die Leitungen des DHRS sind vorgefüllt.	Ja
Unsicherheit im Anlagenparameter Reaktordruck	Möglicher Einfluss auf den Reaktorkühlkreislauf und die Wärmeübertragung im Dampferzeuger (mit Relevanz für das DHRS)	Das ECCS arbeitet druckentlastet (d. h. Druckangleich zwischen RCS und Sicherheitsbehälter) und das DHRS reduziert den Druck im RCS nach und nach, eine Druckentlastung ist nicht vorgesehen	Ja

Ursachen, Parameter	Auswirkungen, Parameter	Anwendbarkeit auf NuScale	Zu untersuchen?
Unsicherheit in den Anlagenparametern Füllstand im Druckhalter und (sekundärseitiger) Füllstand im Dampferzeuger	Auswirkungen auf den Reaktorkühlkreislauf (Relevanz für das DHRS) und das Wasserinventar für das ECCS. Zu niedrige und zu hohe Wasserinventare können sich negative auf die Wärmeübergänge auswirken und auch einen Einfluss auf die Umlaufraten haben.	Das Kühlmittel im RCS teilt sich nach Öffnen der RSVs oder Aktivierung des ECCS zwischen RCS und Sicherheitsbehälter auf. Bei einem zu geringen Inventar besteht die Gefahr, dass es zu einer Kernabdeckung kommt. Ein zu großes Kühlmittelinventar reduziert die Kondensationsfläche für den Wärmeübergang zwischen Sicherheitsbehälter und Reaktorbecken.	Ja, dies wird in NuScale-Analysen berücksichtigt.
Unsicherheit in den Anlagenparametern der Druckverlustbeiwerte	Die Druckverlustbeiwerte beeinflussen die Durchflussrate im Primärkühlkreislauf, im ECCS und im DHRS.	Die Unsicherheiten in den Druckverlustbeiwerten müssen untersucht werden und können auch von der Reynoldszahl abhängen. Im ECCS ist der Druckverlust von den Beiwerten in den Ventilen abhängig, im DHRS im Wesentlichen von den Beiwerten der Düsen.	Ja, dies wird in NuScale-Analysen berücksichtigt.
Unsicherheit im Anlagenparameter Reaktorbeckentemperatur	Eine hohe Reaktorbeckentemperatur führt zu einem schlechteren Wärmeübergang im DHRS-Kondensator.	Eine hohe Reaktorbeckentemperatur ist für das ECCS und das DHRS als konservativ anzusehen. Eine konservativ hohe Temperatur von 93°C wird in den NuScale-Analysen verwendet.	Ja, dies wird in NuScale-Analysen berücksichtigt.
Ablagerungen	Dicke der Ablagerungen auf den Wärmeübergangsflächen	Ablagerungsfaktoren 3 E-04 m²*K/W (DHRS-Kondensatoroberfläche), 6 E05 m²*K/W (Dampferzeuger-Wärmeübergangsfläche). Die Wärmeübergangsflächen an der Außenhülle des RCS und im Sicherheitsbehälter sind sehr groß. Im Sicherheitsbehälter kondensiert Dampf, hier sind keine kurzfristen Ablagerungen zu erwarten, im Kernbereich kann es zu Borsäure-Niederschlägen kommen.	Ja, dies wird in NuScale-Analysen berücksichtigt.

Ursachen, Parameter	Auswirkungen, Parameter	Anwendbarkeit auf NuScale	Zu untersuchen?
Unsicherheit in den Anlagenparametern bzgl. Wärmeübergangskoeffizienten für Kondensation und Verdampfung an den Oberflächen Kühlmittel-Wärmetauscher	Die Wärmeübergangskoeffizienten hängen auch von den Füllstände im Dampferzeuger (DHRS) und Sicherheitsbehälter (ECCS) und von der Reaktorbecken-temperatur ab. Darüber hinaus ergibt sich eine Unsicherheit des Modellparameters für den Wärmeübergang. Experimente über den gesamten Bereich der Parameterunsicherheiten können helfen die Modellunsicherheiten gering zu halten.	Die Wärmeübergangskoeffizienten der NuScale-Analysen sind an den experimentellen KAIST- und NIST-1 HP-03 SET-Ergebnissen validiert (siehe /NUS 20f/ und /KIM 00/), Borsäure-Niederschläge im Kernbereich könnten den Wärmeübergang aus den Brennstäben verschlechtern	Ja, dies wird in NuScale-Analysen berücksichtigt.
Unsicherheit im Anlagenparameter Reaktorbeckenfüllstand	Der Füllstand im Reaktorbecken kann im Störfallverlauf leicht absinken, die Wärmeübergangsfläche der Sicherheitsbehälter-Außenwand kann dadurch leicht abnehmen.	Das Reaktorbecken siedet 61 h nach Störfalleintritt. Ein Einfluss des Reaktorbeckenfüllstandes auf die Funktion der Kühlsysteme ist gering im Fall des ECCS und die Kondensatoren des DHRS sind genügend weit unter Wasser.	Nein

Die nächsten Schritte V bis VII basieren auf den thermohydraulischen Unsicherheitsanalysen und deren Bestimmung der Versagensoberfläche in Abhängigkeit von den Hauptparametern. Diese Ergebnisse liefern die Grundlage zur Bestimmung der Ausfallrate des ECCS bzw. des DHRS.

8.1.3 Naturumlauf des Nachzerfallswärmeabfuhrsystem

NuScale hebt als Abhängigkeiten für die Kühlleistung des DHRS folgende Einflussfaktoren hervor /NUS 20c/ und /NUS 20/:

- Temperatur im RCS – Der Wärmetransport des DHRS steigt mit zunehmender Temperatur im RCS
- Kühlmittelinventar (bedroht durch Leckstörfälle oder falsche Abstimmung der Ventil-Verschlusszeiten) – ein hoher Füllstand und ein niedriger Füllstand können sich negativ auf die Wärmeübergänge auswirken. Ein niedriger Füllstand führt dazu, dass die Wärmeübergangsflächen im Dampferzeuger nicht vollständig befeuchtet werden. Ein hoher Füllstand verringert die Frischdampf-Bildung im Damperzeuger und die Kondensation im DHRS-Kondensator aufgrund verringertem Kontakt zum Frischdampf.
- Ansammlung nicht-kondensierbarer Gase – Nicht-kondensierbare Gase können den Wärmeaustausch im DHRS-Kondensator verringern. Die maximale Menge an nicht-kondensierbaren Gasen ist 0,422 kg in einer Redundanz des DHRS, ansonsten wird die Betriebsmannschaft über die Ansammlung der nicht-kondensierbaren Gase im DHRS informiert.
- Wassertemperatur im Reaktorbecken – Die Wassertemperatur im Reaktorbecken kann den Flächenwärmeübergangskoeffizient im DHRS-Kondensator beeinflussen.
- Druckverluste – Die Druckverluste an den Düsen dominieren die Durchflussrate und damit den Wärmetransport im System, (zusätzliche) Druckverluste im System (z. B. bei Ausfall eines der beiden Auslöseventile) beeinflussen nur bedingt die Durchflussraten.
- Speisewasser-Druck – Der Speisewasser-Druck hängt vom Höhenunterschied zwischen der Unterkante der DHRS-Kondensatoren und der Unterkante der Dampferzeuger ab.

Darüber hinaus ist ein Einfluss folgender Systemgrößen zu erwarten:

- (Kühlmittel-)Temperatur,
- Wärmeübertragung (Wärmeübergangskoeffizienten zwischen Kühlmittel und Kühlflächen) in DHRS-Kondensator und Dampferzeuger,
- Blockierte Leitungen im Dampferzeuger,
- RCS-Systemgrößen für die Wärmeabgabe an die Dampferzeuger:
  - Umlaufrate (hängt auch von den Größen im DHRS ab),
  - Temperatur (wie oben erwähnt),
  - Druck (insbesondere nach einer Druckentlastung nach Aktivierung des ECCS sinkt die Wärmeabgabe an das DHRS),
  - Kühlmittelinventar (der Druckhalter sollte nicht leerlaufen, ansonsten kommt Dampf in den Primärkühlkreislauf und gefährdet dessen Naturumlauf),
  - Menge und Position von nicht-kondensierbaren Gasen im RCS,
  - Druckverluste im RCS,
  - Kernleistung: Nachzerfallsleistung bzw. Spalt- und Nachzerfallsleistung im Fall eines ATWS.

Die NuScale-Analysen ergeben für die Ausfallrate einer Redundanz des DHRS einen Wert von 4 E-06 innerhalb von 72 h /NUS 20/ und ein GVA beider Redundanzen aufgrund der Verstopfung beider Dampferzeuger mit 2,57 E-06 innerhalb von 72 h. Eine typische stabilisierte Durchflussrate durch das DHRS (> 100 s nach einem Ausfall der externen Stromversorgung) beträgt etwa 2 kg/s bei 82 bar /NUS 20b/ (Randbedingung ist ein maximaler Druck im RCS). Für diesen Fall beträgt die angenommene Temperatur im Reaktorbecken 93 °C, die maximale Temperatur im RCS ungefähr 300 °C bei einer Durchflussrate von 150 kg/s (nach ca. 200 s erreicht, zuvor kleinere Werte bei etwa 50 kg/s) und einem Druck von 120 bar (mit fallender Tendenz). Für diese Störfallbeherrschung werden beide Redundanzen des DHRS als funktionstüchtig angenommen.

8.1.4 Naturumlauf des Not- und Nachkühlsystems ECCS

NuScale untersucht in Sensitivitätsanalysen zum ECCS die nachfolgend aufgeführten, einflussreichen Parameter /NUS 19/:

- Nachzerfallsleistung, Variation zwischen 0 % und 120 % der nominellen Nachzerfallsleistung,
- Temperatur im Reaktorbecken, Variation zwischen 18 °C und 99 °C,
- Füllstandshöhe im Reaktorbecken, Variation zwischen 14 m und 21 m,
- Einfluss durch nicht-kondensierbare Gase,
- Druckhalterfüllstände (anfängliches RCS-Inventar), Variation bis 20 % des nominellen Füllstands,
- Dampfexpansion bei Durchströmung der RVVs mit einem Expansionsfaktor von Y = 0,7,
- Gleichzeitiger Betrieb des DHRS,
- ein RVV oder ein RRV öffnet nicht.

Kühlmittelverluste durch ein Leck am Sicherheitsbehälter (1 cm Füllstandshöhenverlust im Sicherheitsbehälter und 3 cm im RCS innerhalb 24 h) wurden berücksichtigt, aber zeigten keinen wesentlichen Einfluss auf die Kühlleistung des ECCS. Darüber hinaus hebt NuScale als Abhängigkeiten für die Kühlleistung des ECCS folgende Einflussfaktoren hervor /NUS 20e/ und /NUS 20/:

- Borsäure-Niederschlag im Kernbereich,
- Kühlmittelverluste sowie
- Ansammlungen von Schmutz (debris accumulation), die u. a. zu höheren Druckverlusten und schlechteren Wärmeübergängen führen. Insbesondere muss eine Hüllrohrtemperatur von unter 430 °C eingehalten werden, um schnelle Korrosionsprozesse im Kernbereich zu verhindern. Konservativ wird eine maximale Menge Schmutz von 16 kg angenommen. Schmutzansammlungen können die Funktion der RRV gefährden.

Die Ausfallrate des ECCS wird in /NUS 20/ mit 1 E-07 innerhalb von 72 h angegeben. Durchflussraten durch die einzelnen RVVs liegen im Bereich von 0,2 kg/s bis 5 kg/s mit einem hohen Wert zu Beginn der Notkühlung /NUS 19/. Die Durchflussraten durch die RRV liegen entsprechend der geringeren Redundanz um einen Faktor 1,5 höher. Wichtig im Zusammenhang mit dem ECCS ist auch, dass es zu einer ungleichmäßigen Verteilung der Borsäure über das gesamte Kühlmittel kommt. Die Borsäure sammelt sich

dabei im Kernbereich an und ist im Sicherheitsbehälter verdünnt. Dieser Effekt reduziert die Gefahr einer möglichen Rekritikalität während eines ATWS.

8.1.5 Naturumlauf im Reaktorkühlsystem RCS

Der Naturumlauf im RCS liegt bei maximal 68,5 kg/s im Nachkühlbetrieb /NUS 20c/. Im Leistungsbetrieb bei 100 % Leistung liegt die Durchflussrate zwischen 539 kg/s und 651 kg/s mit einem Mittelwert von 587 kg/s. Als Ausfallmechanismus für den Naturumlauf im RCS kommt ein Verlust an Kühlmittelinventar und ein Verlust der Unterkühlung in der Steigleitung (loss of subcooling in the riser) /NUS 20k/ in Betracht. Ein Verlust der Unterkühlung in der Steigleitung kann auf einen Druckverlust im RCS (blowdown) oder einen starken Temperaturanstieg im Kern, hier ist ein Störfall aufgrund zusätzlicher eingebrachter Reaktivität (reactivity insertion accident) zu denken, zurückzuführen sein.

8.1.6 Reaktorsicherheitsventile

Die RSVs sind in jedem Modul zweifach redundant (2 x 100 %) vorhanden und unabhängig voneinander installiert. Die RSVs werden benötigt, um den RDB vor einem Überdruckversagen zu schützen. Die Ventile sind beschrieben in /NUS 20c/. Eines der beiden Ventile öffnet bei 143 bar, das andere bei 145 bar. Der Ventildurchmesser beträgt ungefähr 8 cm am Anschluss des RDB und 10 cm am Anschluss des Sicherheitsbehälter. Die RSVs werden über federbelastete Steuerventile geschalten, welche beim jeweiligen Ansprechdruck im RDB auslösen und beim Unterschreiten eines Schließdrucks wieder schließen (Hysterese). Die RSVs sind passiv und können nicht aktiv geöffnet werden. Eine Funktionsprüfung der RSVs erfolgt alle fünf Jahre, jedes fünfte Ventil wird außerdem nach zwei Jahren geprüft. Die folgenden Abbildungen Abb. 8.3 und Abb. 8.4 zeigen die Fehlerbäume für die Ausfälle für Wiederschließen des angesprochenen Ventils und das Öffnungsversagen beider Ventile bei Ansprechdruck.

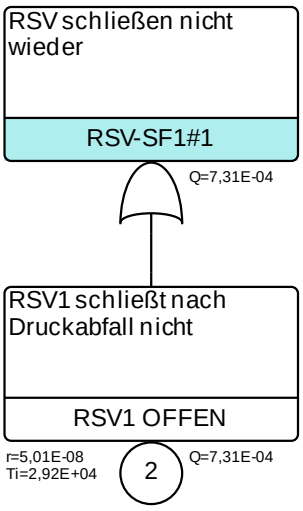


Abb. 8.3 Fehlerbaum der RSVs zur Druckbegrenzung des RCS

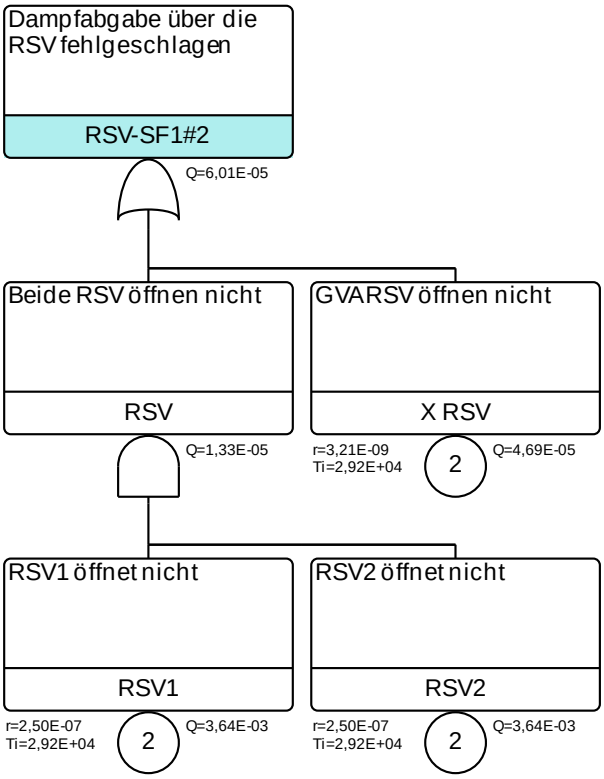


Abb. 8.4 Schließung der RSVs nach einem Druckabbau im RDB

8.1.7 Schutz vor unbeabsichtigter Aktivierung des Notkühlsystems

Alle ECCS-Ventile sind mit einer Auslöseblockierung ausgestattet, dem IAB, der eine unbeabsichtigte Öffnung der ECCS-Ventile verhindert. Der IAB ist in jedem Ventil unabhängig vorhanden. Bei Aktivierung des ECCS spannt sich eine Feder über den Druck

zwischen RCS und Sicherheitsbehälter. Wird eine Druckdifferenz von 90 bar überschritten, so verhindert eine Scheibe die Entlüftung der Kontrollkammern und damit die Öffnung der Ventile bis zu einem Druckabfall unter ca. 65 bar. Der Fehlerbaum für den IAB ist in Abb. 8.5 gezeigt. Ein GVA des IAB mehrerer ECCS-Ventile führt genau wie ein Einzelfehler zum Ausfall der Sicherheitsfunktion, hat aber eine wesentlich geringere Wahrscheinlichkeit und wird deshalb vernachlässigt. Ein Ausfall zweier EDSS-Busse verhindert die Öffnung der zugehörigen ECCS-Ventile.

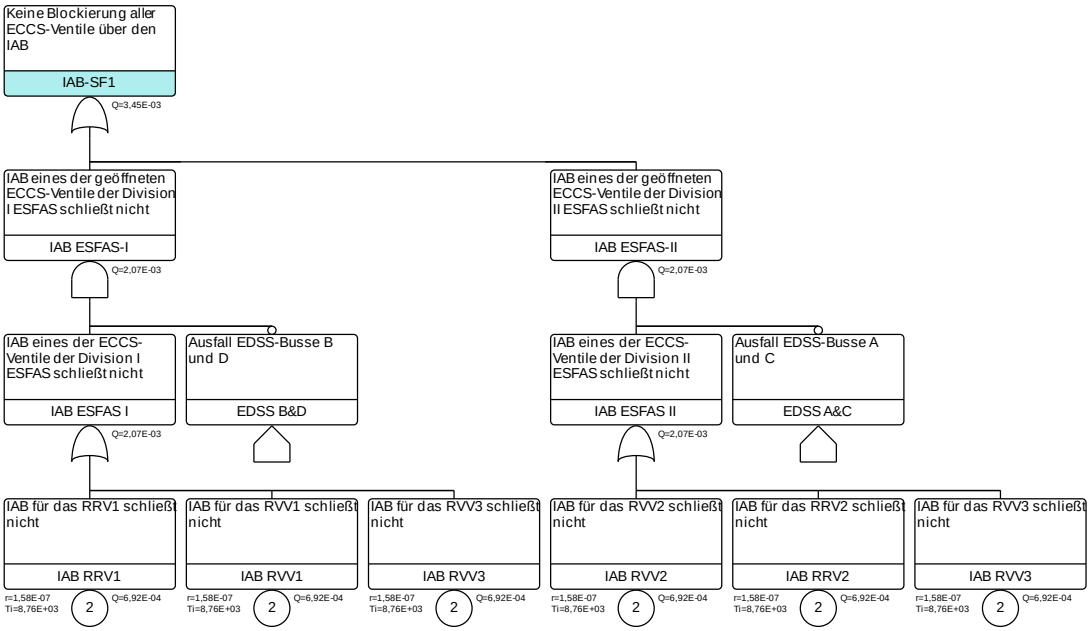


Abb. 8.5 Fehlerbaum für den IAB

8.1.8 Spaltprodukt-Barrieren

Im SMR von NuScale gibt es die drei klassischen Barrieren eines DWR, die Hüllrohre, die druckführende Umschließung des RCS und der Sicherheitsbehälter.

Hüllrohre

Die Integrität der Hüllrohre ist bei allen betrachteten auslösenden Ereignissen über eine Verletzung des Temperaturkriteriums ‘Temperatur kleiner 1.200 °C‘ gefährdet oder über einen Absturz schwerer Lasten während eines Brennelementwechsels.

Druckführende Umschließung des RCS

Die druckführende Umschließung wird durch das Öffnen eines RSVs bei Drücken über 143 bar durchlässig, sowie durch das Öffnen mindestens eines ECCS-Ventils bei Aktivierung des ECCS, durch einen KMV oder durch ein Überdruckversagen bei Drücken von mehr als 174 bar.

Integrität des Sicherheitsbehälters

Die Integrität des Sicherheitsbehälters kann bei Drücken über 90 bar nicht gewährleistet werden. Im Fall eines Lecks im CVCS außerhalb des Sicherheitsbehälters wird die Sicherheitsbehälterbarriere umgangen, wenn der Sicherheitsbehälterabschluss nicht erfolgt. Bei einem Dampferzeuger-Bypassleck ohne Isolierung des betroffenen Dampferzeugers ist auch von einem Sicherheitsbehälter-Bypass auszugehen. Außerdem ist die Integrität des Sicherheitsbehälters für den Störfall ‘Leck zwischen Reaktorbecken und Sicherheitsbehälter‘ verletzt.

8.2 Fehlerbaumanalysen

8.2.1 Ausfall der RESA

Eine RESA wird vom RTS entsprechend den Kriterien in Abschnitt 7.1 ausgelöst. Der Ausfall beider RTS-Redundanzen wird im Fehlerbaum, Abb. 8.6, zusammenfassend betrachtet (Basisereignis: Ausfall des Reaktorschutzsystems). Die Sensorik hat eine Ausfalltoleranz von zwei der vier Sensoren, die aufgrund niedriger Ausfallraten in der Analyse nicht explizit betrachtet werden (Basisereignis: Ausfall der RESA-Anregung). Die beweglichen Teile des RTS, acht Abschalt- und acht Regelelemente, werden im Fehlerbaum berücksichtigt. GVA von drei oder mehr Abschalt- bzw. Regelelementen führt in ein ATWS. Im Fall eines Ausfalls der elektrischen Energieversorgung fallen die Stäbe durch Entregung der Haltemagnete selbsttätig ein. Deshalb ist die RESA-Anregung im Fehlerbaum über binären Hausevents mit der Funktion der elektrischen Energieversorgung verknüpft.

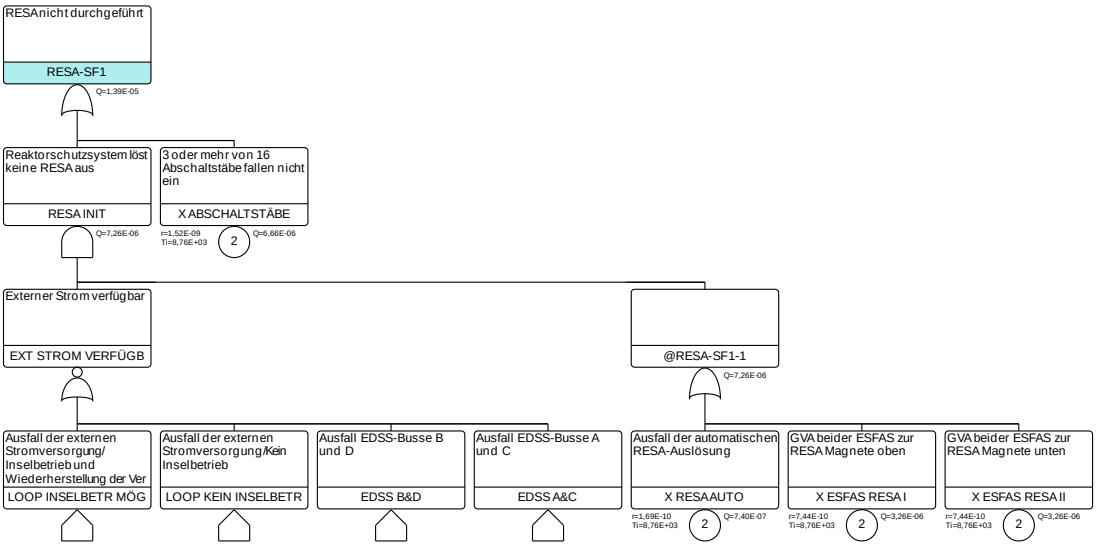


Abb. 8.6 Fehlerbaum der RESA

8.2.2 Ausfall des Nachwärmeabfuhrsystems

Der Fehlerbaum für eine Redundanz des DHRS ist in Abb. 8.7 gezeigt. Der Fehlerbaum zur Initiierung des Dampferzeuger-Abschlusses befindet sich in Abb. 8.9. Für die Funktion des DHRS sind fünf Faktoren entscheidend:

- erfolgter Frischdampf-Abschluss des Dampferzeugers mit mindestens einem von zwei Ventilen,
- erfolgter Speisewasser-Abschluss des Dampferzeugers mit mindestens einem von drei Ventilen (FWIV, Speisewasserregelventil und Speisewasserrückschlagventil),
- Öffnung mindestens eines der beiden parallel angeordneten DHRS-Auslöseventile,
- eine vorangegangene erfolgreiche Entlüftung des DHRS,
- Erreichen einer Mindestumlaufrate des Naturumlaufs für eine ausreichende Wärmeabfuhr (hierfür ist mit einer Stabilisierungsphase von ca. 100 s zu rechnen).

Der Abschluss der Dampferzeuger erfolgt typischerweise zusammen mit dem Sicherheitsbehälterabschluss (siehe Abb. 8.9) kann jedoch auch manuell durchgeführt werden oder nach Detektion eines Dampferzeuger-Bypasslecks erfolgen. Der Dampferzeugerabschluss besteht aus dem Frischdampf-Abschluss und dem Speisewasserabschluss durch Schließen von zwei in Reihe angeordneten Abschlussarmaturen. Für den Speisewasserabschluss sind zusätzlich Rückschlagventile berücksichtigt. Die DHRS-Auslöseventile sind zweifach redundant. Für die Stabilität und eine ausreichende Umlaufrate des

Naturumlaufes sind die Faktoren der ausreichenden Entlüftung des Systems und die richtige Menge an Kühlmittel im System (nach einem Leckstörfall oder einem fehlerhaften Dampferzeugerabschluss) wichtig. Es wird angenommen, dass das Öffnen nur eines Auslöseventils keinen Einfluss auf die Umlaufrate und Stabilität des Naturumlaufs hat, da die Druckverluste im Wesentlichen an der durchflusslimitierenden Düse anfallen.

Die Entlüftung und das Befüllen der Leitungen des DHRS wird vor dem Leistungsbetrieb über die Speisewasserpumpen von den Speisewasserleitungen durchgeführt. Die Ansammlung von nicht-kondensierbaren Gasen wird durch vier Füllstandssensoren pro Redundanz hinter den Auslöseventilen mit jeweils zwei Sensoren pro Auslöseventil überwacht. Ein Alarmsignal in der Warte zeigt eine unzureichend gefüllte Leitung an. Das DHRS ist während des Brennelementwechsels nicht verfügbar. Wasserschlag und resonante Schwingungen können nach /NUS 20c/ nicht auftreten.

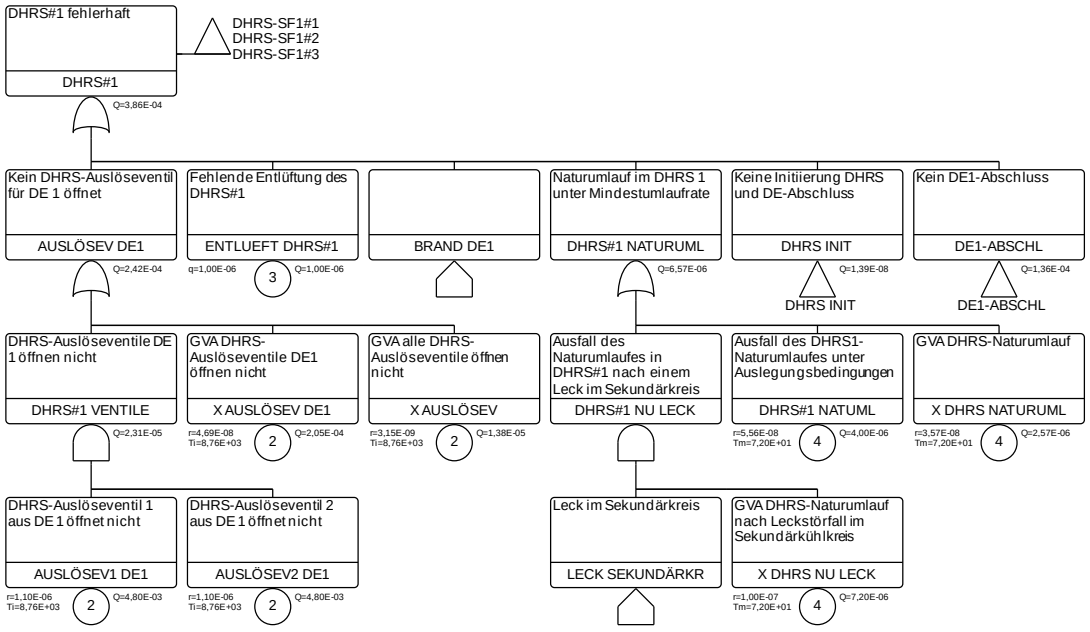


Abb. 8.7 Funktion des DHRS für den DE1

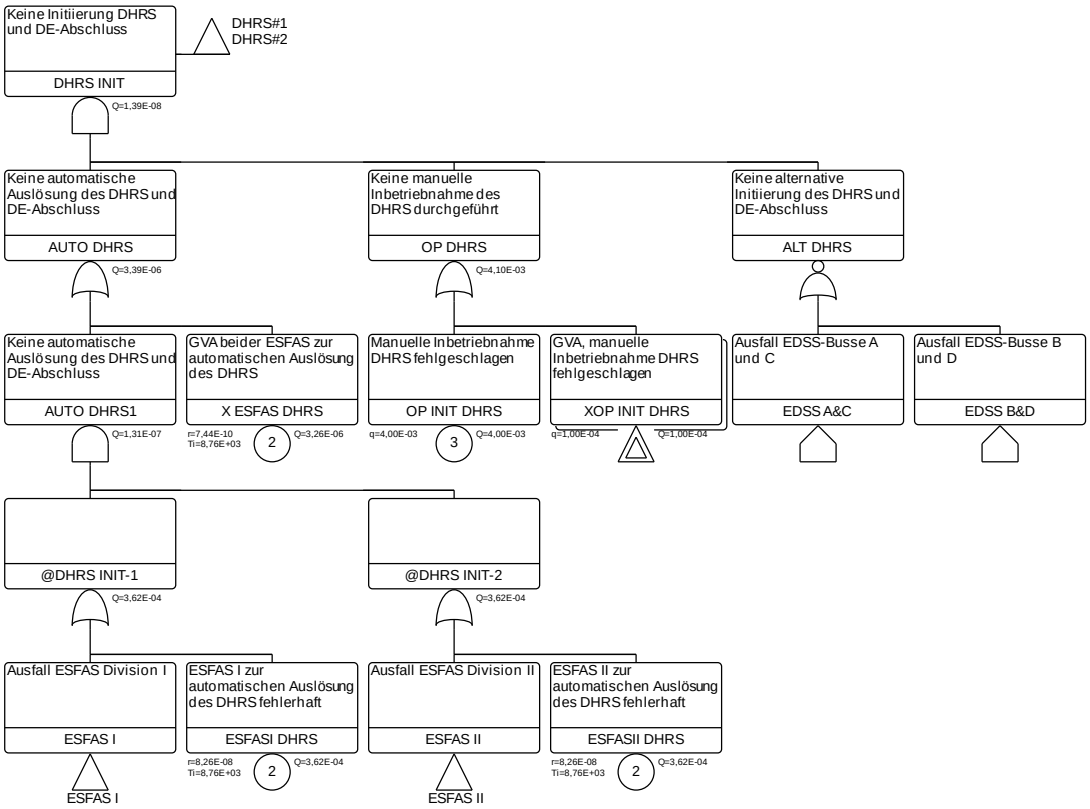


Abb. 8.8 Fehlerbaum zur Initiierung des DHRS

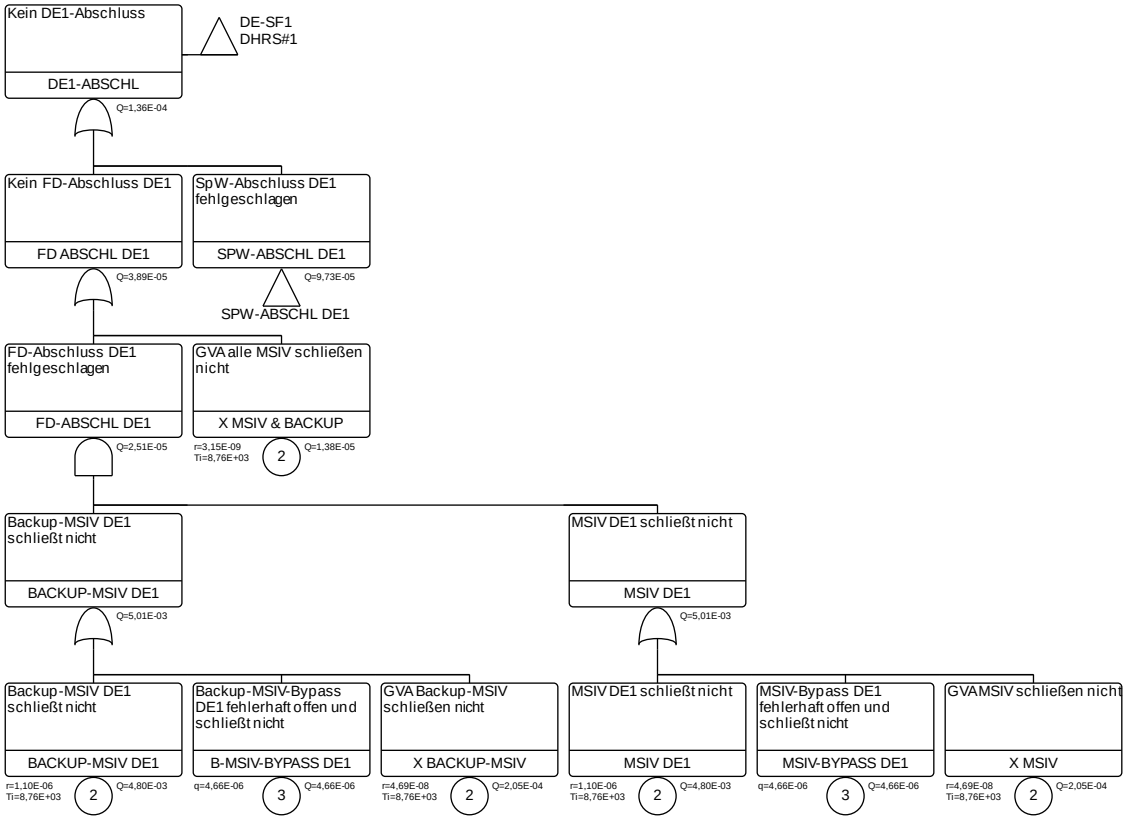


Abb. 8.9 Fehlerbaum zum Abschluss des DE1

Die Ausfälle der Systemfunktion ergeben sich entsprechend den Mindestwirksamkeitsbedingungen unter Berücksichtigung eines oder beider Systeme entsprechend den Ereignisbaumanalysen wie Abb. 8.10 dargestellt.

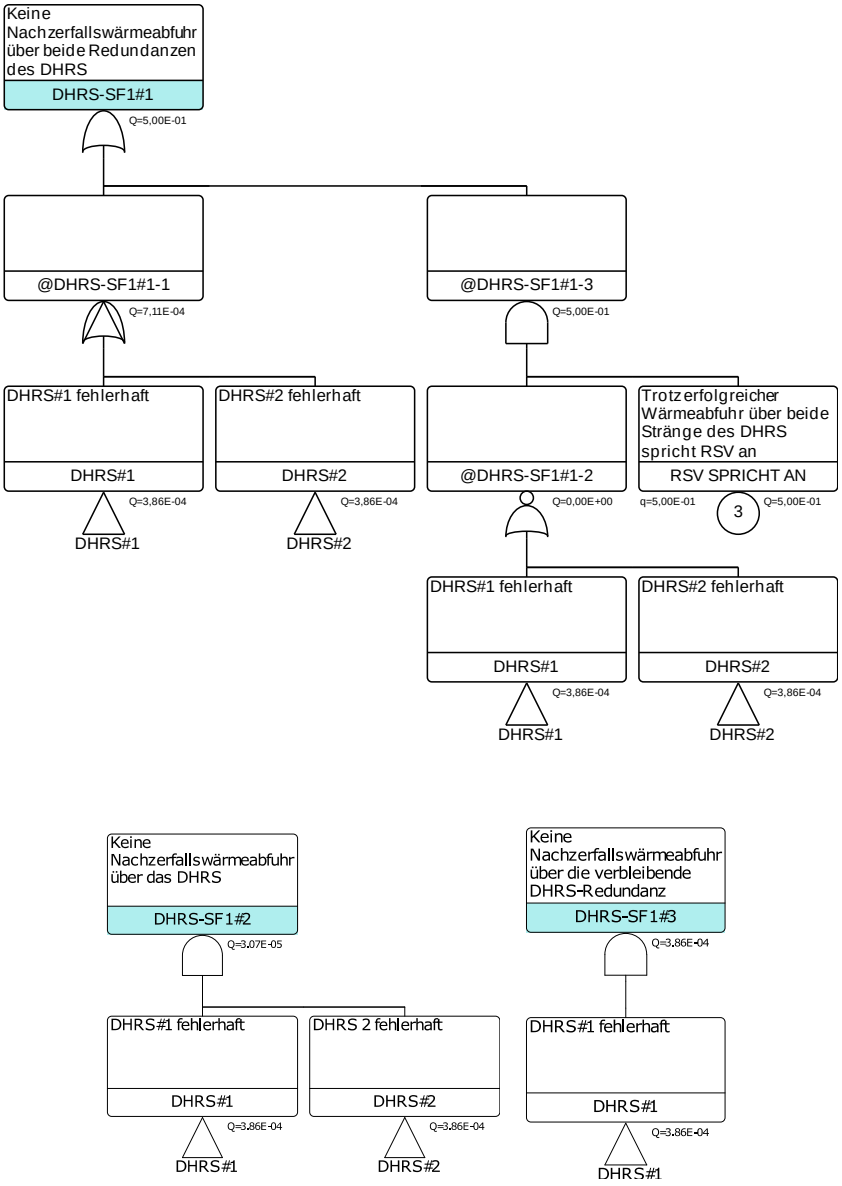


Abb. 8.10 Ausfallverknüpfungen der Systemfunktionen DHRS-SF1

8.2.3 Ausfall des Not- und Nachkühlsystems ECCS

Für eine erfolgreiche Notkühlung über das ECCS (Funktionsereignis ECCS-SF1#1) ist das Öffnen mindestens eines Ventils der drei RVVs und eines der beiden RRVs sowie das Anlaufen des ECCS-Naturumlaufs erforderlich. Für das ECCS ergibt sich ein Zweiphasen-Naturumlauf zwischen RCS und Sicherheitsbehälter. Ein höheres Ausfallrisiko

für den Naturumlauf ist bei Ausfall einzelner ECCS-Ventile zu erwarten, da die Druckverluste im Naturumlauf hauptsächlich an den Ventilen anfallen und höhere Durchströmraten bei Redundanzausfällen an den übrigen Ventilen entstehen. Die Wärmeabfuhr hängt u. a. von der Dampfabgaberate (Massendurchsatz) über die RVVs ab, die im Gleichgewicht der Kühlmittelrückflussrate über die RRVs in der Wasserphase entspricht. Die Umlaufrate im ECCS ist entsprechend von der Verfügbarkeit der systemrelevanten RVVs und RRVs abhängig.

DHRS und ECCS werden in einigen Transientenverläufen gleichzeitig verwendet und es strömt ein Teil des Kühlmittels im RCS über den Primärteil der Dampferzeuger und den Rückströmraum zurück in den Kern. Die Nachzerfallswärme des Kerns wird entsprechend für eine gewisse Zeit in Teilen über das DHRS und gleichzeitig über das ECCS abgegeben. Ein Ausfall des ECCS ergibt sich durch KMV-Störfälle, dieser Ausfall ist entsprechend in den Ereignisablaufanalysen berücksichtigt und fehlt im Fehlerbaum zum ECCS.

Darüber hinaus ist es für das ECCS wichtig, dass die ECCS-Ventile nach einem Druckabbau im RCS passiv öffnen, eine Eigenschaft, die in den Systemfunktionen ECCS-SF1#1 und ECCS-SF1#2 berücksichtigt wurde (siehe dazu Abb. 8.11). Im Fehlerbaum ECCS-SF1#3 fehlt diese Möglichkeit, da für Transienten, die diesen Fehlerbaum berücksichtigen, kein ausreichender Druckabbau im RCS über DHRS oder RCS-Leckage vorliegt. Für eine Druckentlastung des RCS im Leistungsbetrieb reicht das Öffnen eines beliebigen ECCS-Ventils aus, entsprechend der Systemfunktion ECCS-SF1#3 in Abb. 8.11.

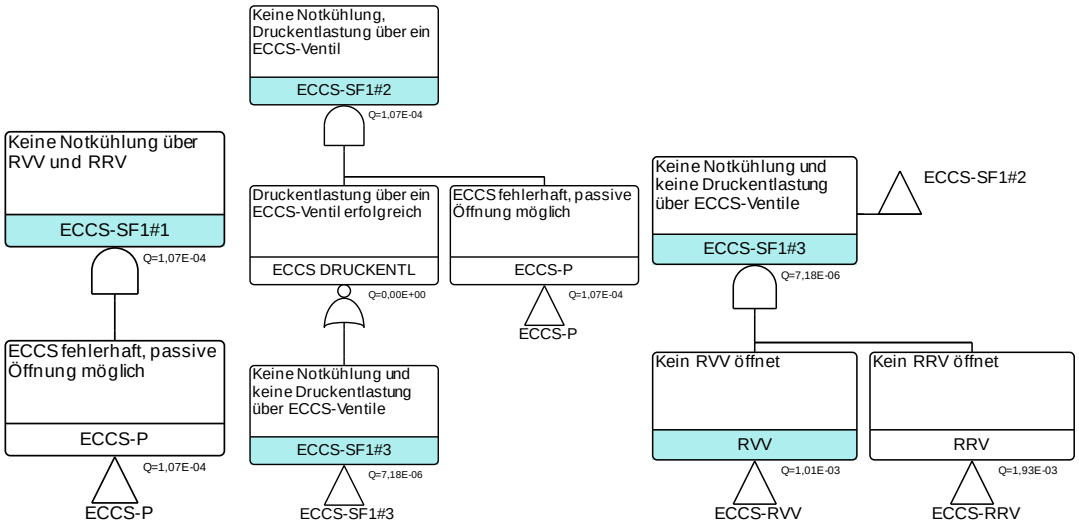


Abb. 8.11 Systemfunktionen für den Einsatz des ECCS in den Ereignisablaufanalysen

Der weiterführende Fehlerbaum zu ECCS ist in Abb. 8.12 gezeigt. Hier ist auch die höhere Ausfallrate für den Naturumlauf bei einem Ausfall von Redundanzen berücksichtigt. Außerdem ist für eine reibungslose Funktion des ECCS ein Abschluss des CES notwendig und mindestens eine Redundanz des ESFAS.

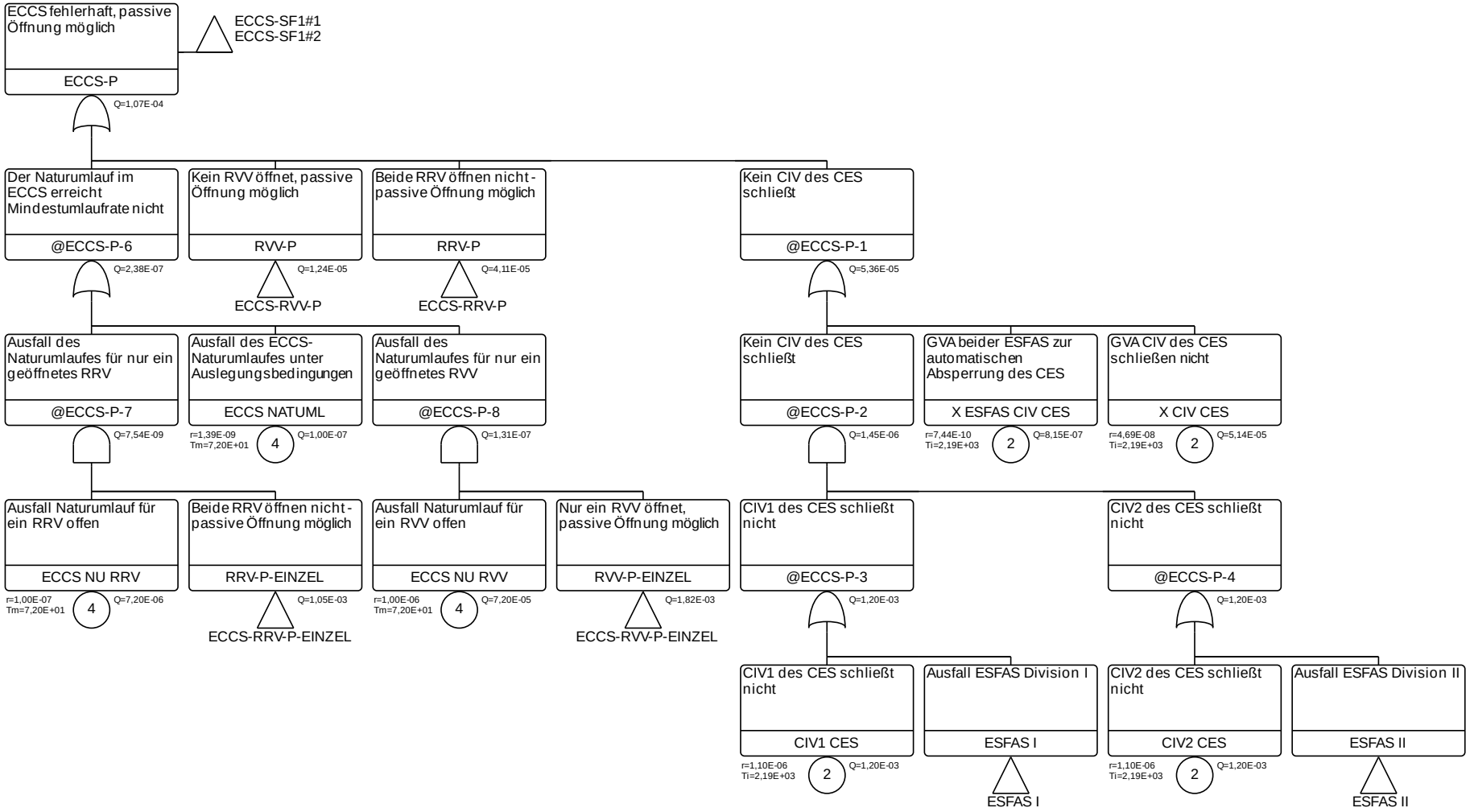


Abb. 8.12 Fehlerbaum zum Ausfall des ECCS

Abb. 8.13 zeigt die Ausfalllogik der RRVs für Fälle mit der Möglichkeit einer passiven Öffnung der Ventile im Verlauf der Transiente.

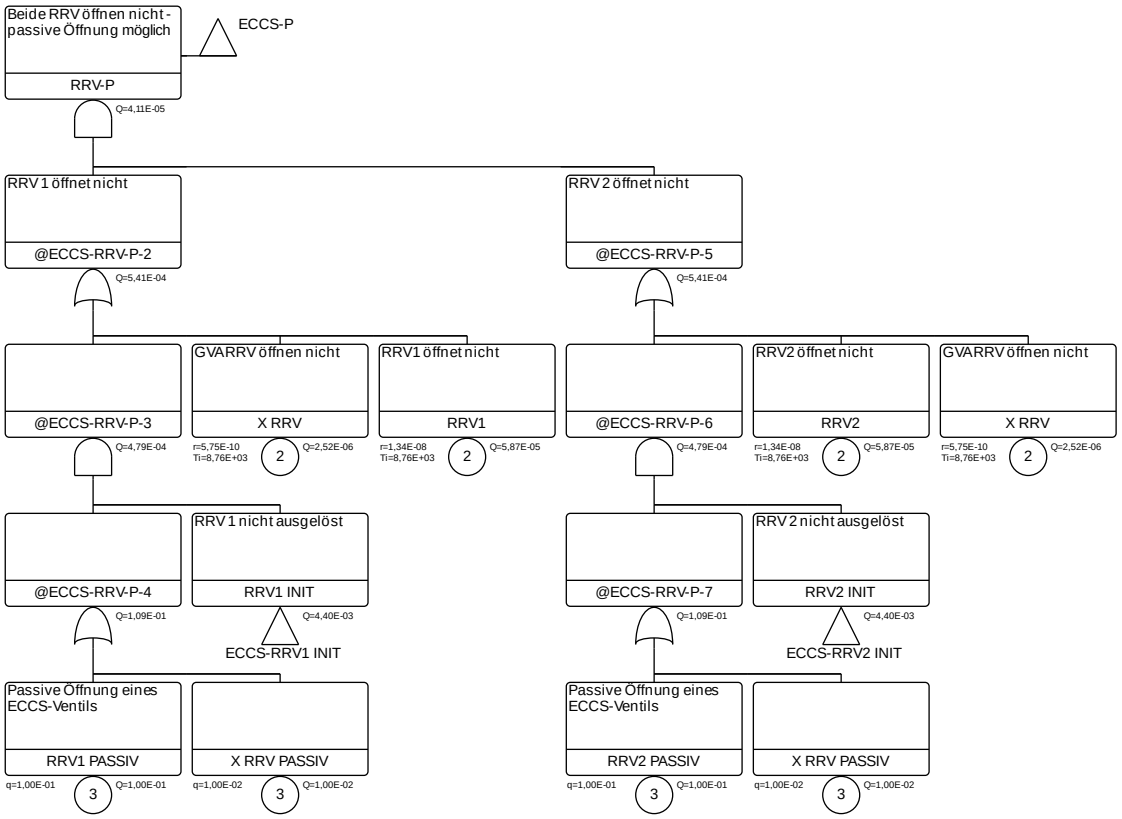


Abb. 8.13 Fehlerbaum für die Funktion der RRVs

Während RVV1 und RRV1 sowie RVV2 und RRV2 für die automatische Auslösung nur über eine Redundanz des ESFAS angesprochen werden können, kann das RVV3 über beide Redundanzen des ESFAS angesteuert werden. Die Auslöselogik für RVV1 und RVV3 ist im Fehlerbaum in Abb. 8.14 implementiert. Die entsprechende Logik für die RRVs unterscheidet sich durch das Fehlen des Hausevents LTOP, da für An- und Abfahrprozesse bei einer Detektion eines Überdrucks entsprechend Abschnitt 8.2.4 nur die RVVs automatisch angefordert werden.

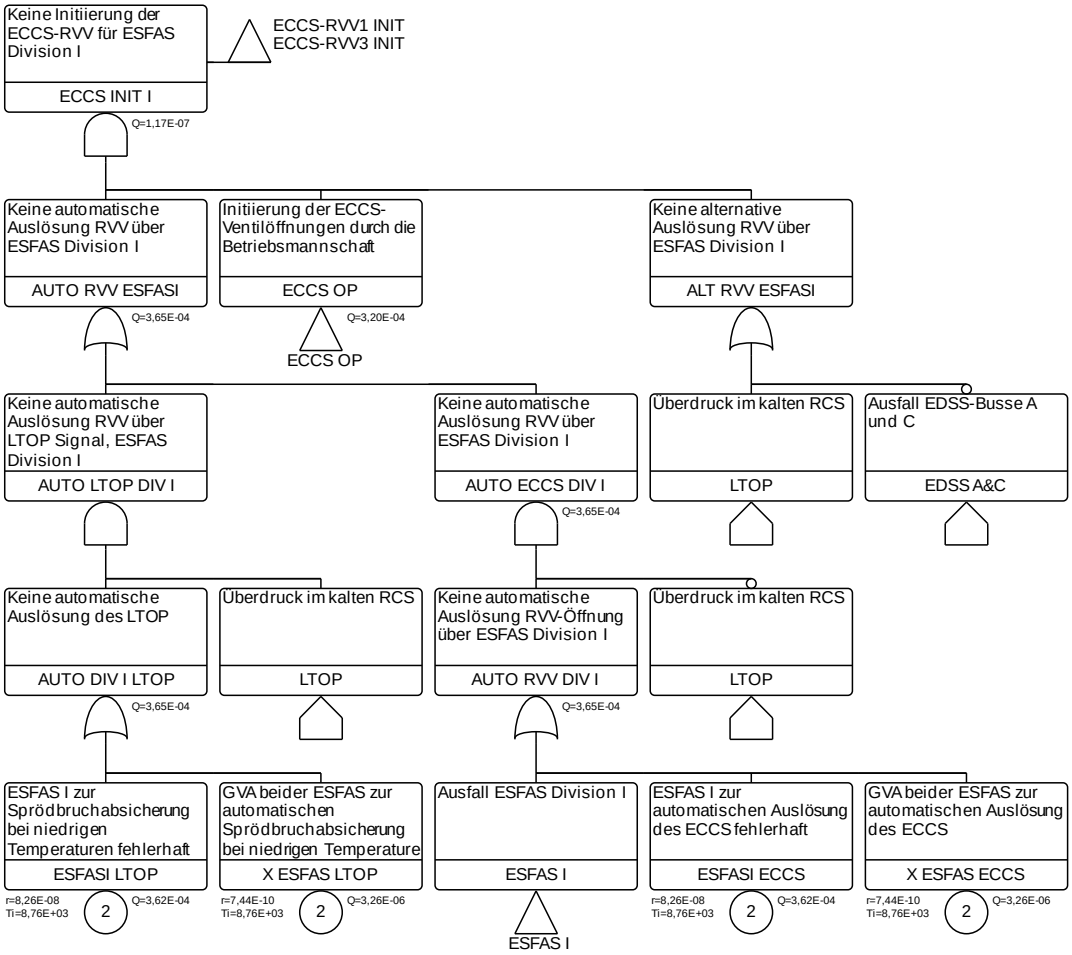


Abb. 8.14 Fehlerbaum zur Auslösung des RVV1 und RVV3 über die ESFAS-Redundanz I

8.2.4 Ausfall des LTOP

Der LTOP wird für An- und Abfahrprozeduren aktiviert, wenn die Temperatur im RCS unterhalb von 159 °C liegt. Übersteigt der Druck im RCS den maximal zulässigen Druck für die aktuell gemessene Temperatur (vgl. Abb. 8.15), so werden die drei RVVs aktiviert. Für die Grenze des maximal zulässigen Druckes ist die Öffnungszeit der RVVs berücksichtigt, so dass im Fall einer Transienten mit schnellem Druckanstieg (im Fall einer fehlerhaften Druckhalterheizung, siehe /NUS 20c/) die Versagensgrenze (Sprödbruchgrenze) der druckführenden Umschließung des RCS nicht überschritten wird.

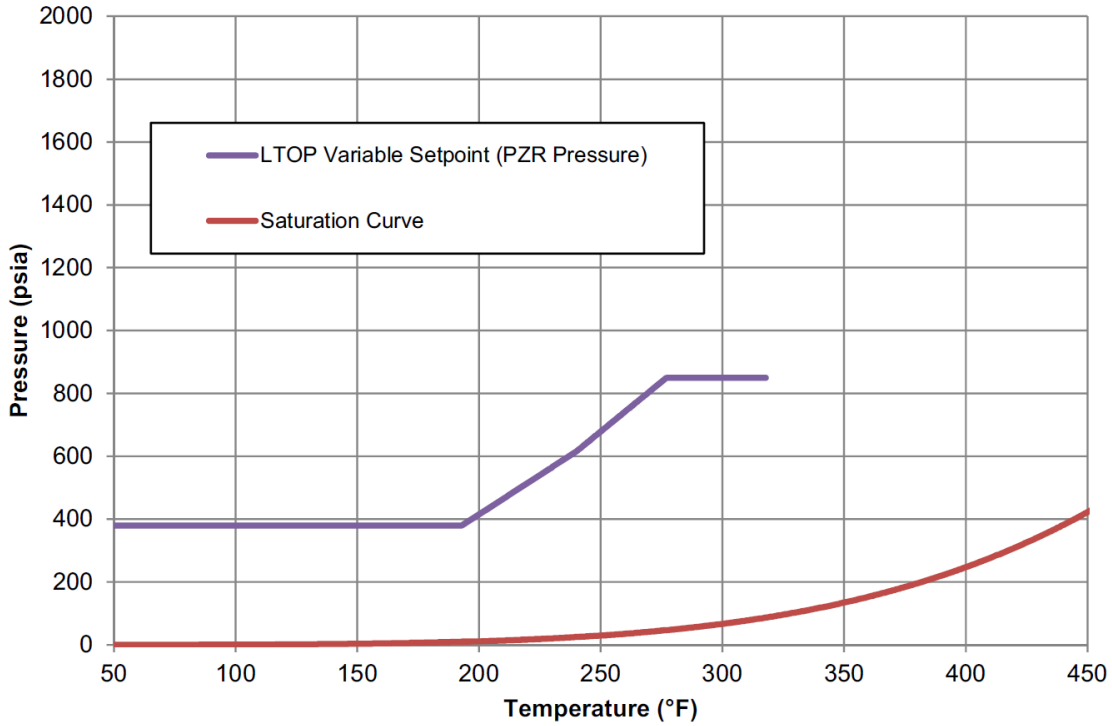


Abb. 8.15 Anregedrücke für den LTOP /NUS 20c/

8.2.5 Absperrung des Notkühlsystems nach einem Kühlmittelverlust

Nach einem KMV spricht die Leckdetektion an und veranlasst den Abschluss des CVCS. Bei einem Problem der automatischen Leckdetektion kann die Betriebsmannschaft eingreifen und eine Absperrung der defekten Leitung veranlassen. Ein erfolgreicher Abschluss der defekten Leitung setzt die Verfügbarkeit mindestens eines der entsprechenden CIV voraus. Die Fehlerbäume der Absperrungen der CVCS-Einspeiseleitung und der CVCS-Entnahmeleitung sind in Abb. 8.16 und Abb. 8.17 dargestellt.

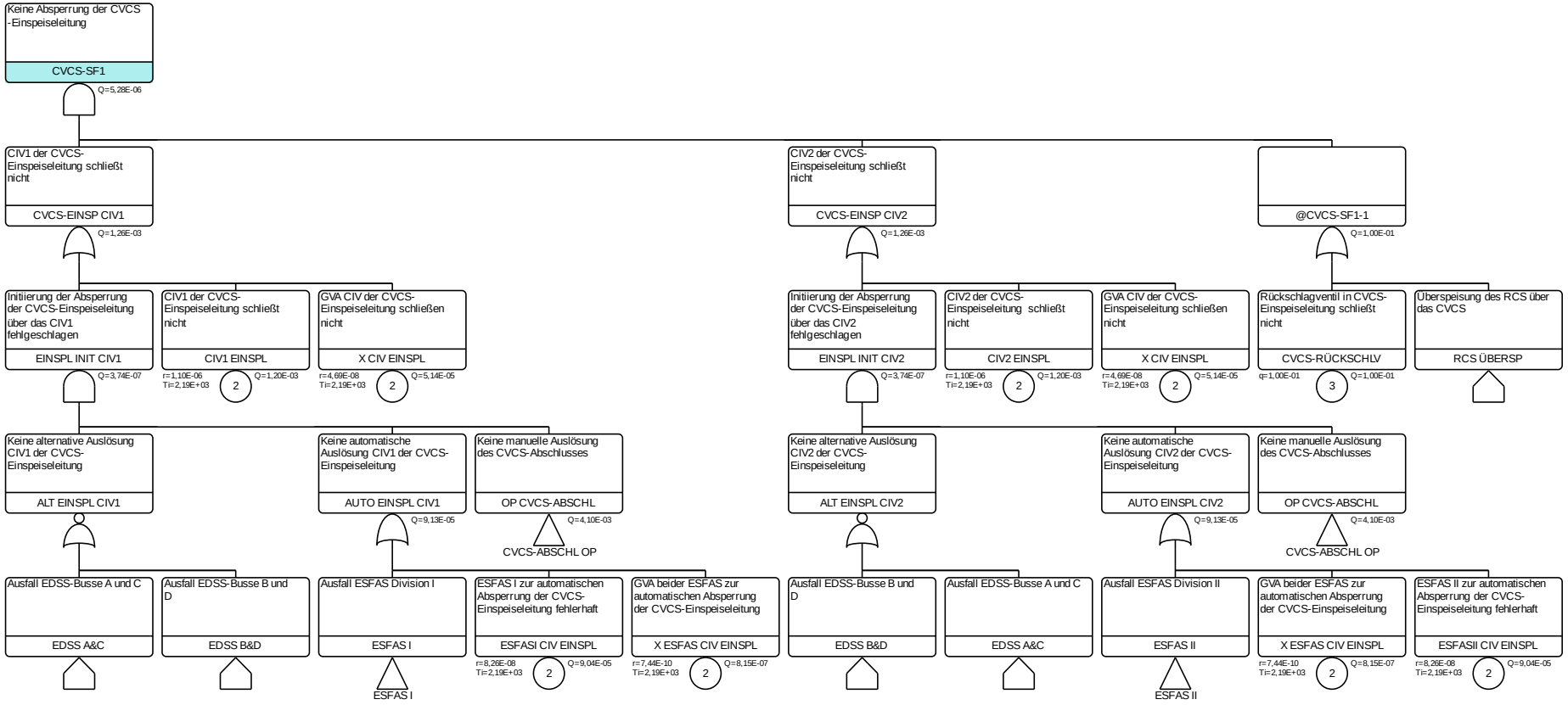


Abb. 8.16 Fehlerbaum der Absperrung der CVCS-Einspeiseleitung nach einem KMV

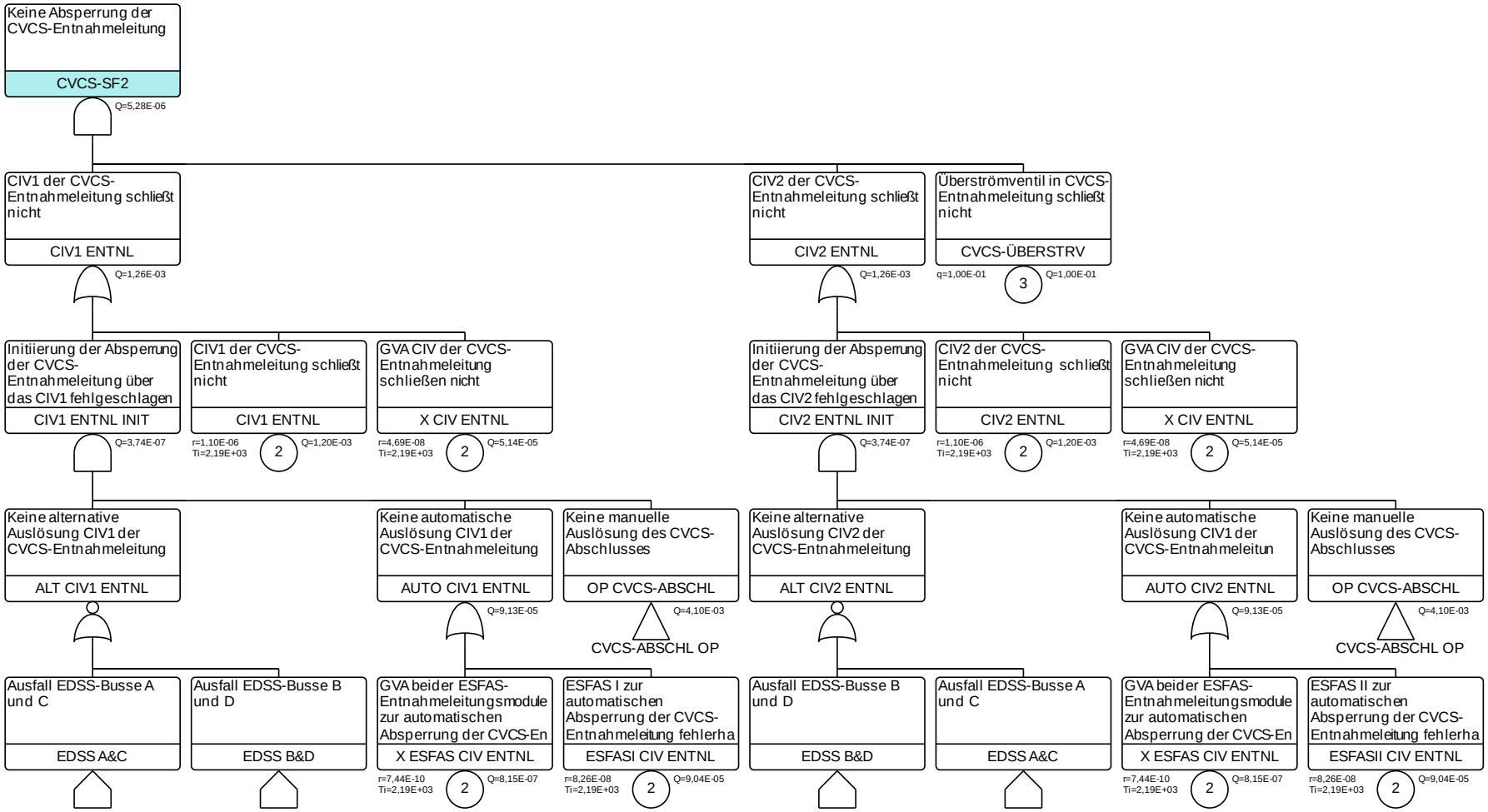


Abb. 8.17 Fehlerbaum der Absperrung der CVCS-Entnahmeleitung nach einem KMV

8.2.6 Absperrung eines Dampferzeuger-Bypasslecks

Der Dampferzeugerabschluss des betroffenen Dampferzeugers wird automatisch durch das Leckdetektionssystem ausgelöst. Der Dampferzeugerabschluss ist ausgefallen, wenn sowohl FWIVs oder MSIVs als auch deren Ersatzventile nicht schließen. Der entsprechende Fehlerbaum für den verunfallten Dampferzeuger ist in Abb. 8.18 dargestellt.

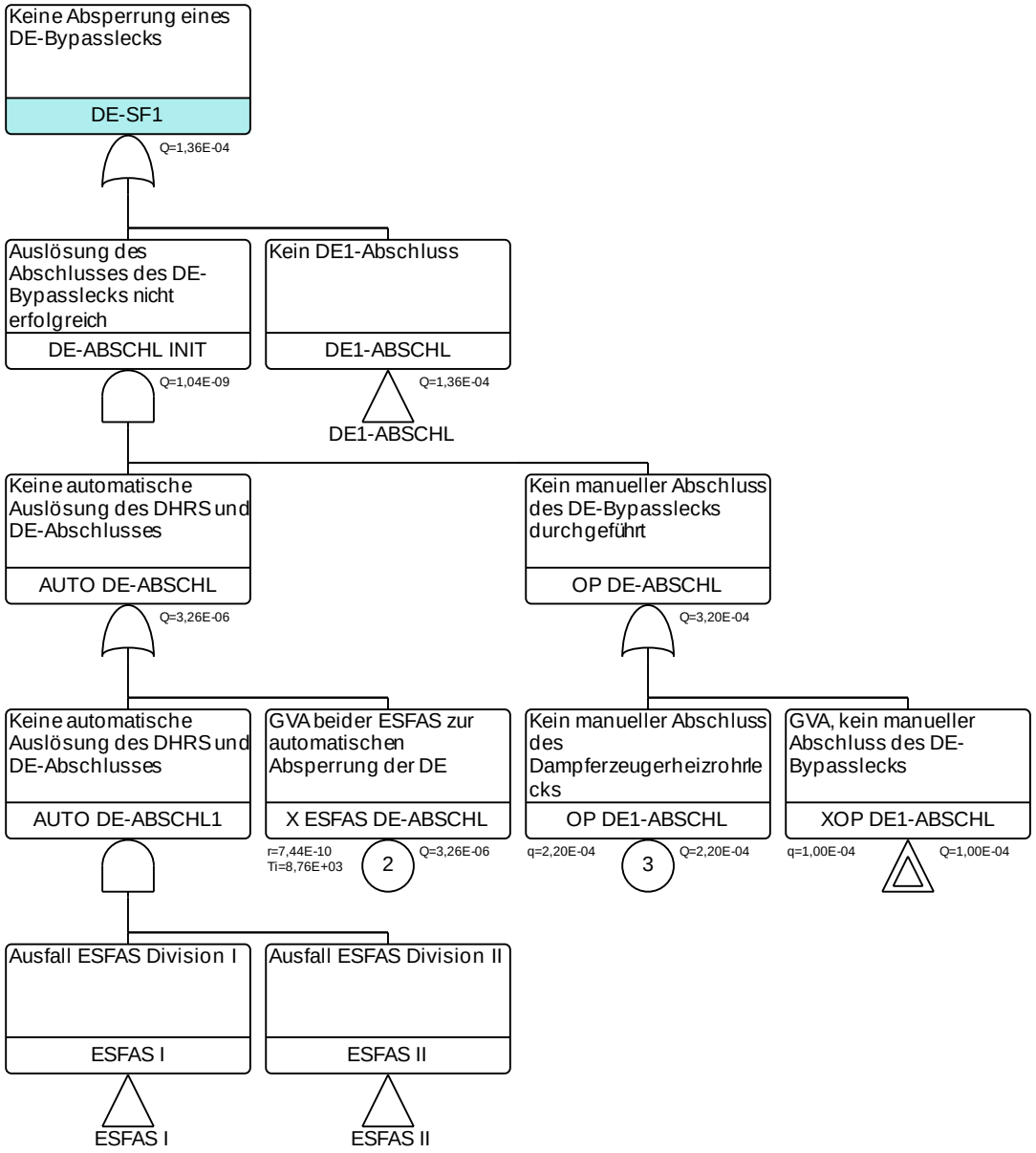


Abb. 8.18 Fehlerbaum Absperrung des verunfallten Dampferzeugers nach einem Dampferzeuger-Bypassleck

8.2.7 Umschaltung auf Inselbetrieb

Ein Ausfall im Stromnetz führt zu einem Lastabwurf auf Eigenbedarf. Ein Modul in der Anlage ist vorgesehen, um in diesem Fall alle anderen Module mit ausreichend Strom zu versorgen. Ein entsprechender Inselbetrieb ist nicht vorgesehen, wenn der Ausfall der Versorgung auf Ausfälle in der Anlage (z. B. der EHVS-Transformatoren) oder im Umspannwerk beruht, da für diese Fälle eine längere Reparaturzeit zu erwarten ist. Die Umschaltung auf Inselbetrieb ist vorgesehen, damit die Anlage möglichst schnell wieder ans Netz gehen kann, es handelt sich dementsprechend nicht primär um eine Sicherheitsfunktion (siehe Abb. 8.19).

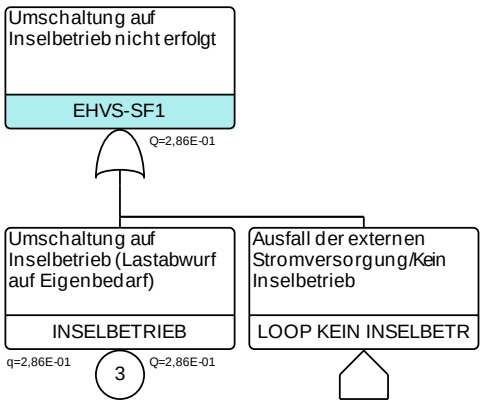


Abb. 8.19 Umschaltung auf Inselbetrieb der Anlage

8.3 Handmaßnahmen

8.3.1 Wiederbespeisung des Kühlkreislaufes

Der Fehlerbaum für das CVCS ist in Abb. 8.20 gezeigt. Neben der erfolgreichen Durchführung der Handmaßnahmen innerhalb des Zeitbudgets sind die Verfügbarkeiten des Boreinspeisesystems, des Deionatsystems, des Niederspannungssystems ELVS, mindestens einer CVCS-Einspeisepumpe und die Möglichkeit zur Wiederöffnung der abgeschlossenen CIV erforderlich.

Ein Sicherheitsbehälterbypass über das CVCS bei einer fehlerhaften Zuschaltung des CVCS (die Branch-Point Alternative CVCS-HM1#2) ergibt sich beispielsweise durch einen Ausfall der Kühlmittelversorgung des Systems oder durch einen Ausfall beider CVCS-Aufbereitungspumpen. Für einzelne Transienten ist das Sprühen in den Druckhalter notwendig, um die druckführende Umschließung des RCS vor zu hohem Druck zu schützen (insbesondere, wenn beide RSVs fehlerhaft nicht öffnen), siehe Abb. 8.21.

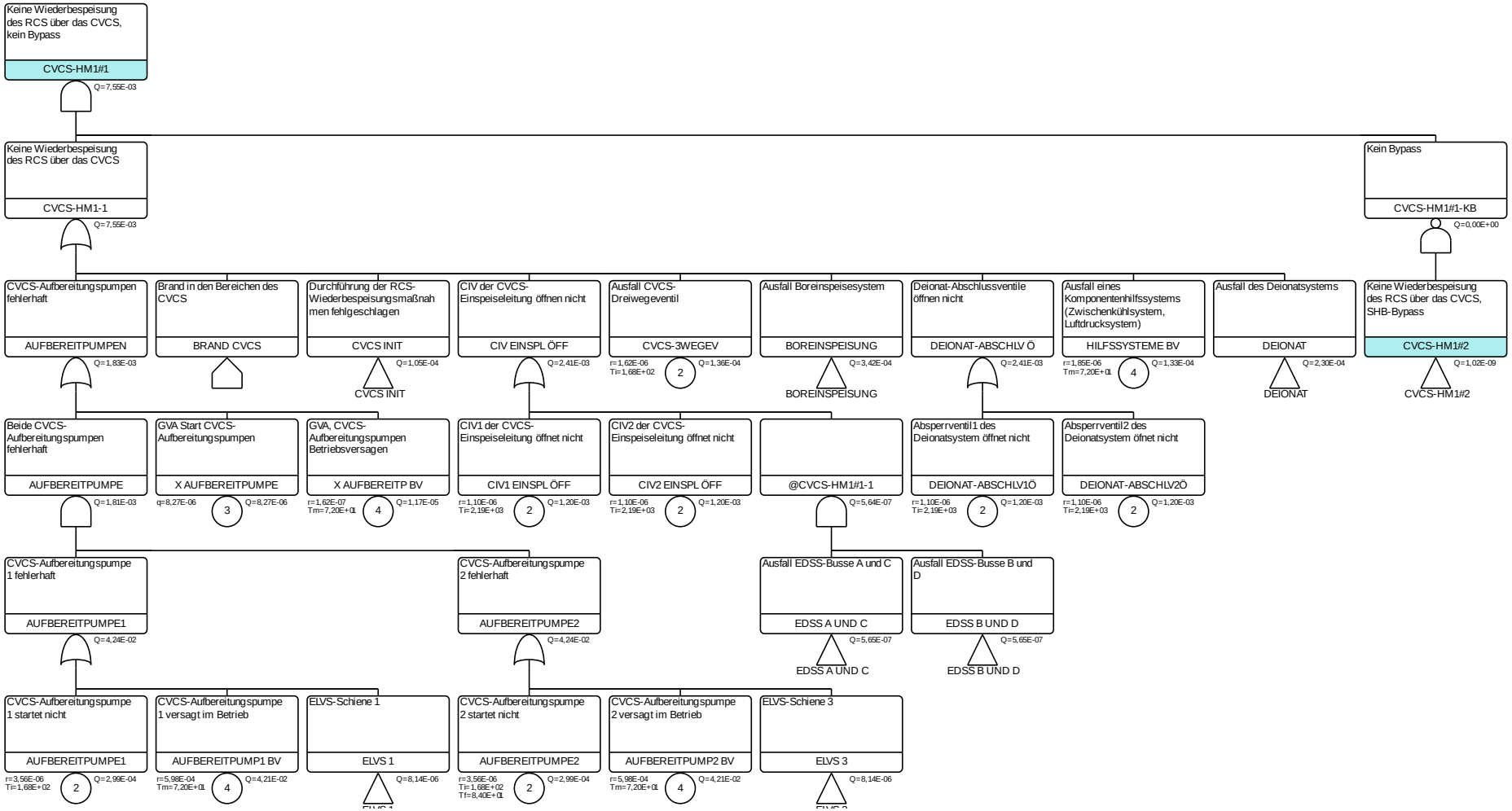


Abb. 8.20 Wiederbespeisung des RCS über das CVCS

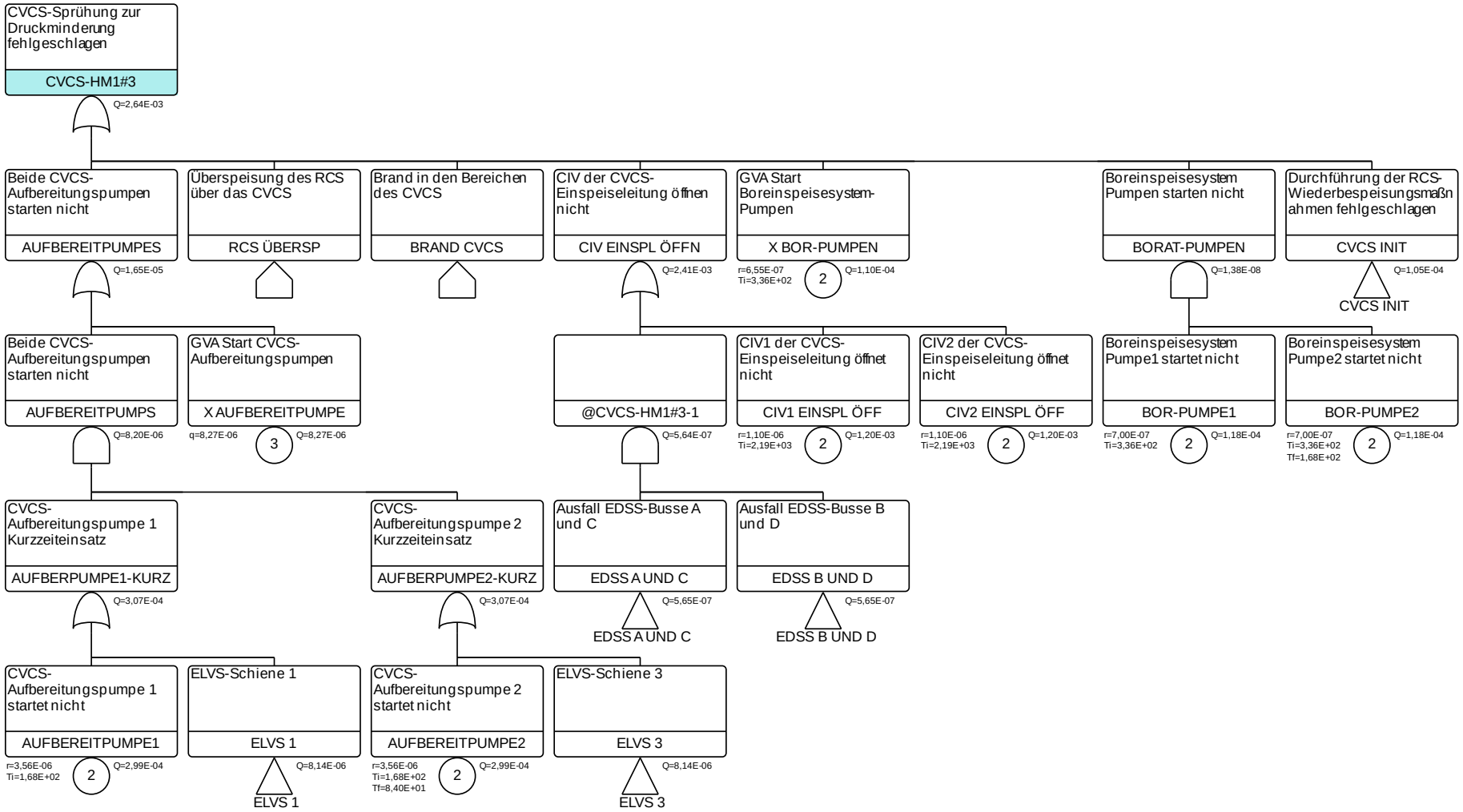


Abb. 8.21 Fehlerbaum zur Druckhalter-Sprühen

Eine dauerhafte Überspeisung des RCS über das CVCS kann mit Hilfe der Absperrung des Deionatsystems erfolgen, da ansonsten der Kühlmittelvorrat nicht für eine Gefährdung des Sicherheitsbehälters ausreicht. Der entsprechende Fehlerbaum ist in der Abb. 8.22 dargestellt.

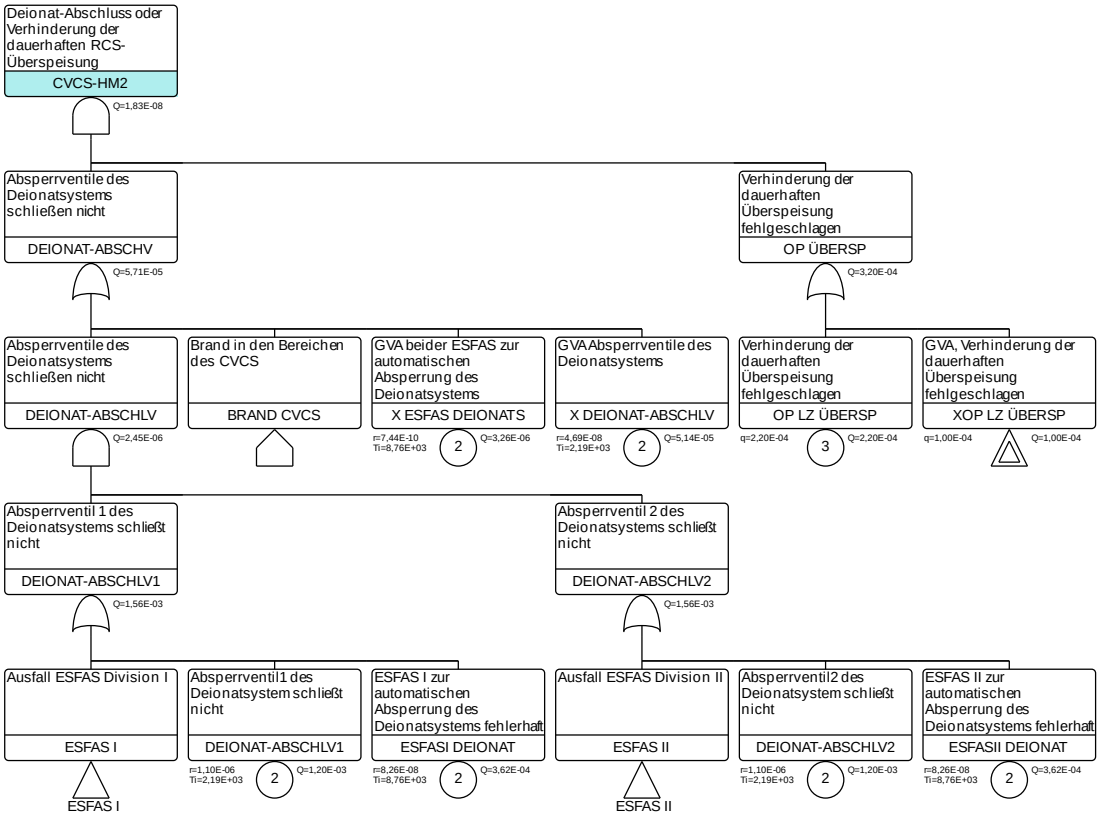


Abb. 8.22 Verhinderung der dauerhaften CVCS-Überspeisung des RCS

8.3.2 Sicherheitsbehälter-Fluten über das CFDS

Das Fluten des Sicherheitsbehälters über das CFDS setzt die korrekte Durchführung aller Maßnahmen des Betriebspersonals voraus. Dazu zählt das Öffnen des CIV, der Start mindestens einer der CFDS-Pumpen, die Durchschaltung der Rohrleitungen auf das betroffene Modul und der Start der besonderen Heizvorrichtung zur Umgehung der Sperrvorrichtung bei Temperaturen von über 177 °C im heißen Strang. Sind die genannten Pumpen und Ventile oder die Heizvorrichtung unverfügbar oder fehlt die Niederspannungsstromversorgung, so kann das Sicherheitsbehälter-Fluten nicht durch-geführt werden. Der Fehlerbaum ist in Abb. 8.23 dargestellt.

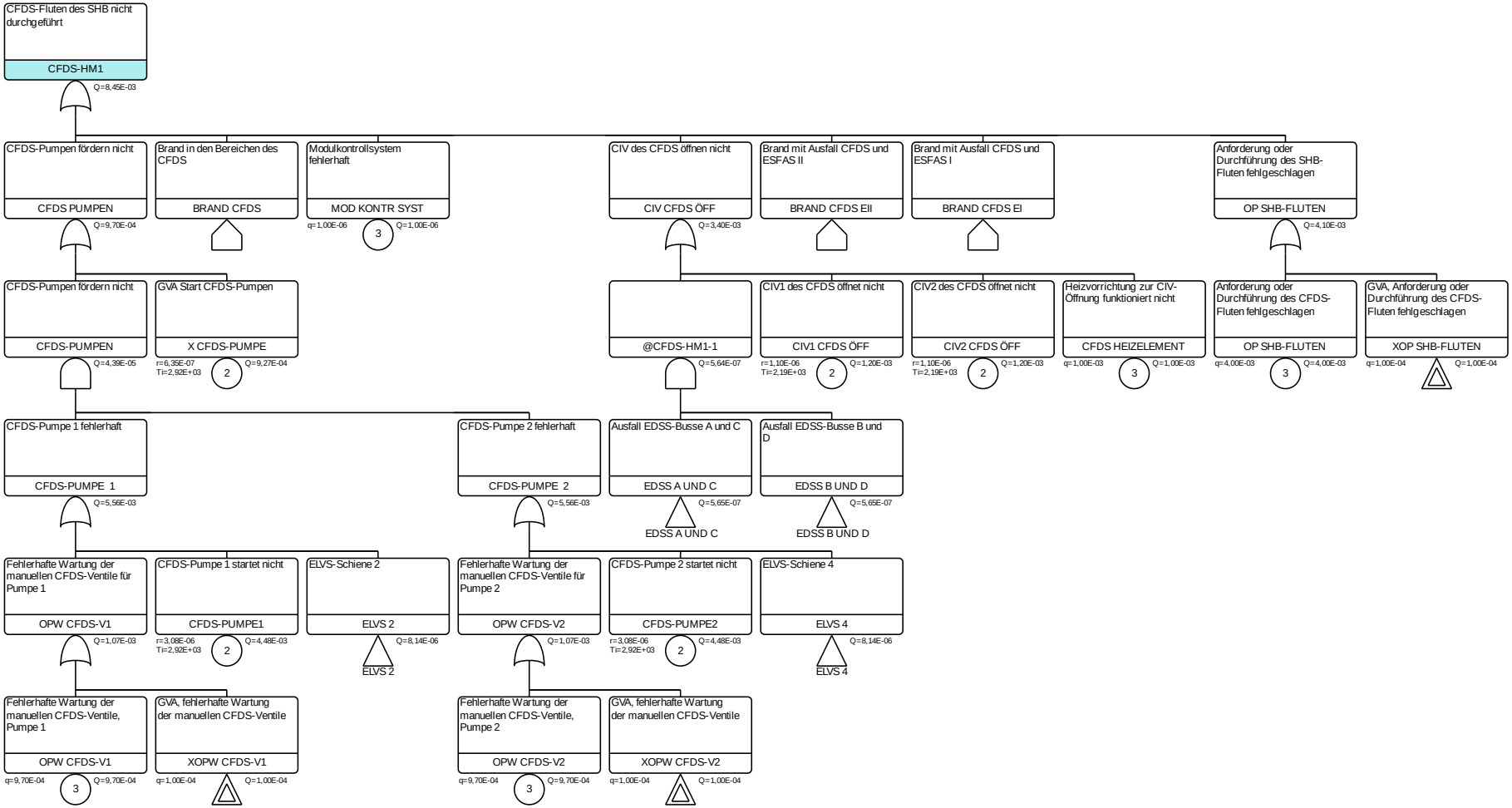


Abb. 8.23 Fehlerbaum des Sicherheitsbehälter-Flutens über das CFDS

8.3.3 CFDS-Drainagefunktion

Der Fehlerbaum der CFDS-Drainagefunktion ergibt sich analog zum Fehlerbaum des Sicherheitsbehälter-Flutens über das CFDS unter zusätzlicher Berücksichtigung möglicher Ausfälle der CFDS-Lufteinspeisefunktion, welche zur erfolgreichen Drainage benötigt wird. Der Fehlerbaum ist in Abb. 8.24 gezeigt.

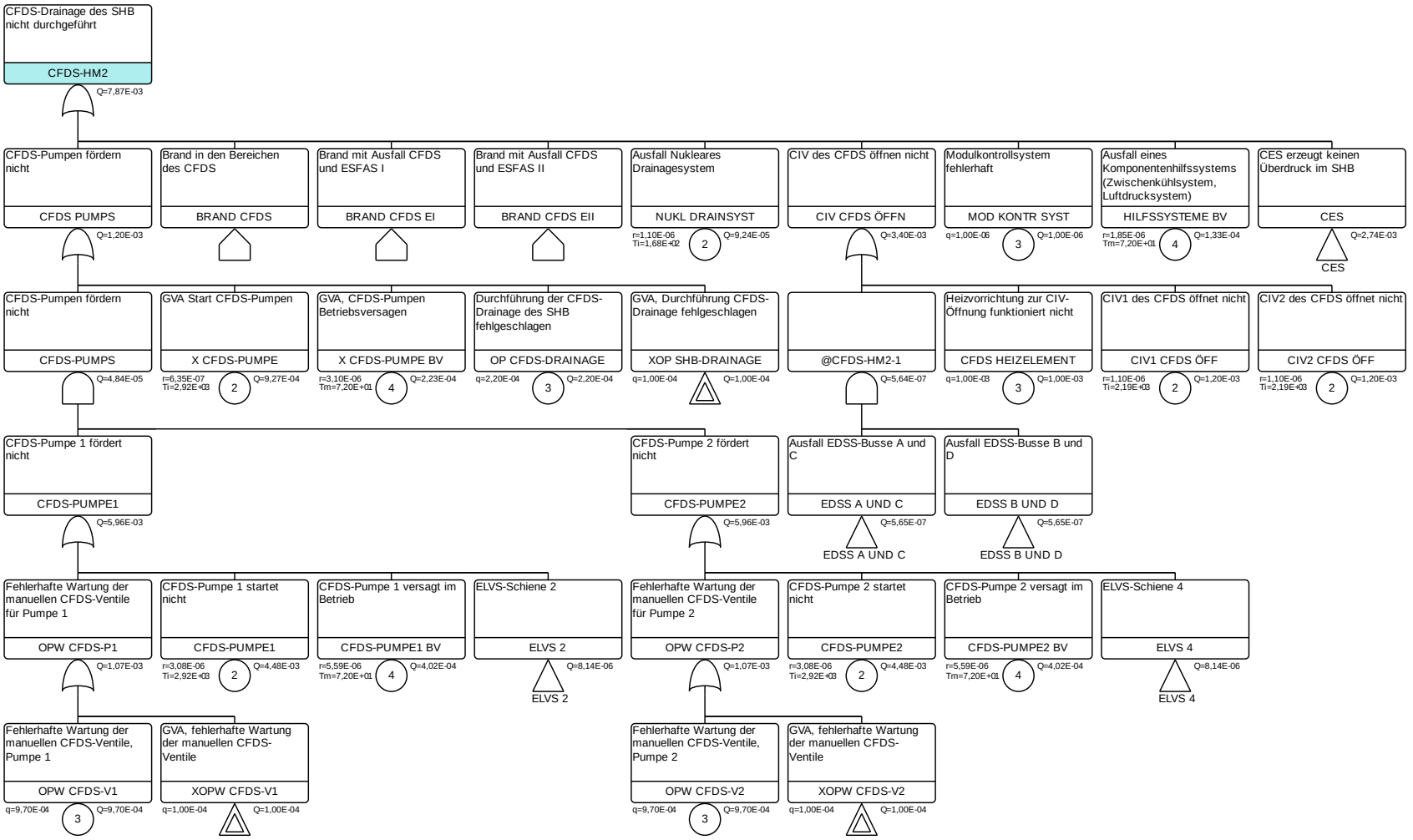


Abb. 8.24 Fehlerbaum zur CFDS-Drainagefunktion

8.3.4 Elektrische Energieversorgung

Wiederherstellung der externen Stromversorgung

Nach einem Ausfall der externen Stromversorgung, der Notstromversorgung und des Inselbetriebs werden die Haltemagnete des ECCS für 24 h mit Batteriestrom versorgt. Sofern in dieser Zeit die externe Stromversorgung wiederhergestellt wird, kann das Auslösen des ECCS verhindert werden. Prinzipiell besteht auch noch die Möglichkeit einer Reparatur der Notstromversorgung in der Zeit zwischen 3 h[30] und 24 h nach dem auslösenden Ereignis, allerdings wird diese Möglichkeit hier konservativ nicht berücksichtigt. Der zugehörige Fehlerbaum findet sich in Abb. 8.25.

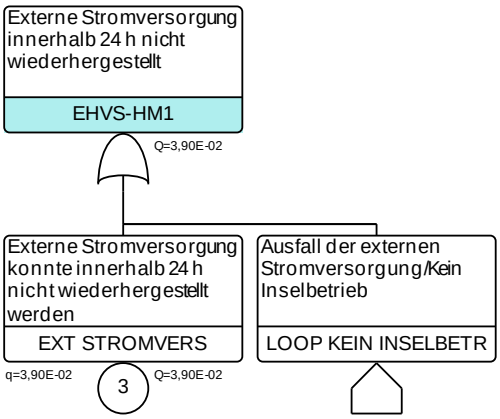


Abb. 8.25 Fehlerbaum zur Wiederherstellung der externen Stromversorgung

Notstrom über Gasturbinengenerator oder Notstromdieselgeneratoren

Zur Notstromversorgung über die Gasturbine muss die Turbine erfolgreich gestartet und nach dem Start durch die Betriebsmannschaft zugeschaltet werden. Die Betriebsmannschaft hat ca. 3 h Zeit für die erfolgreiche Inbetriebnahme. Darüber hinaus darf die Gasturbine auch im Betrieb während der Missionszeit von 72 h nicht versagen. Der Fehlerbaum des Gasturbinengenerators ist in Abb. 8.26 dargestellt.

---

[30] Für den erfolgreichen Start und die Zuschaltung der Notstromversorgung steht der Betriebsmannschaft bereits ein Zeitbudget von 3 h zur Verfügung. Es ergeben sich weitere 21 h bis zur automatischen Öffnung der ECCS-Ventile.

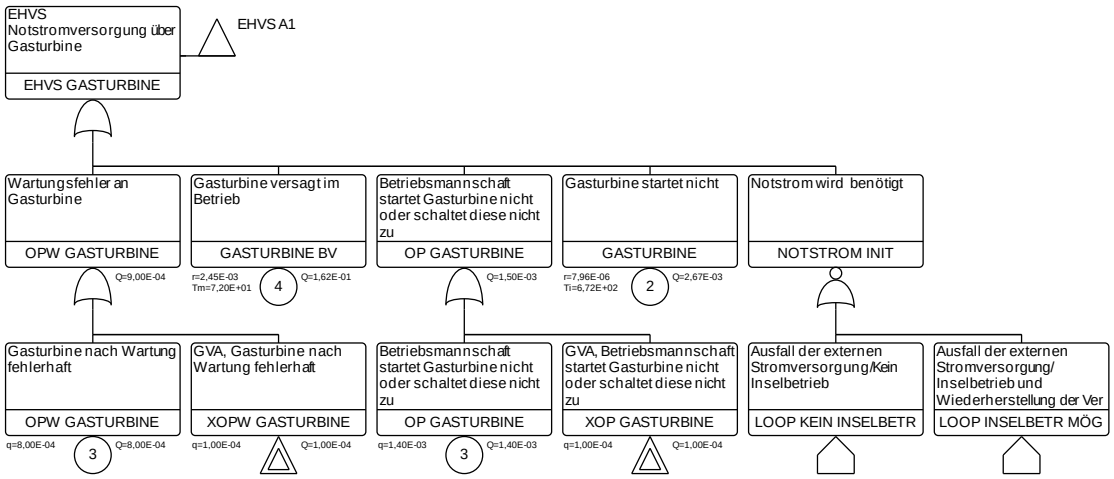


Abb. 8.26 Fehlerbaum bzgl. des Ausfalls der Gasturbine

Die Notstromversorgung über die Dieselgeneratoren erfordert den erfolgreichen Start beider Generatoren, siehe Abb. 8.27. Die Generatoren werden in das Niederspannungsnetz (ELVS) durch die Betriebsmannschaft zugeschalten. Die Betriebsmannschaft hat ca. 3 h Zeit für die erfolgreiche Inbetriebnahme und Zuschaltung. Ein Dieselgenerator darf prinzipiell[31] im Betrieb während der Missionszeit von 72 h ausfallen, da bereits der Betrieb eines Dieselgenerators für die Notstromversorgung der gesamten Anlage ausreicht.

[31] Die Versorgung aller Stromschienen hängt auch von Funktion von ELVS-Leistungsschaltern ab. Die maximale Leistung eines Dieselgenerators reicht nur für den Betrieb einzelner Pumpen aus, z. B. ist in der Liste der nominellen Verbraucher nur eine CVCS-Aufbereitungspumpe aufgeführt, d. h. der Betrieb des CVCS eines Moduls, /NUS 20j/.

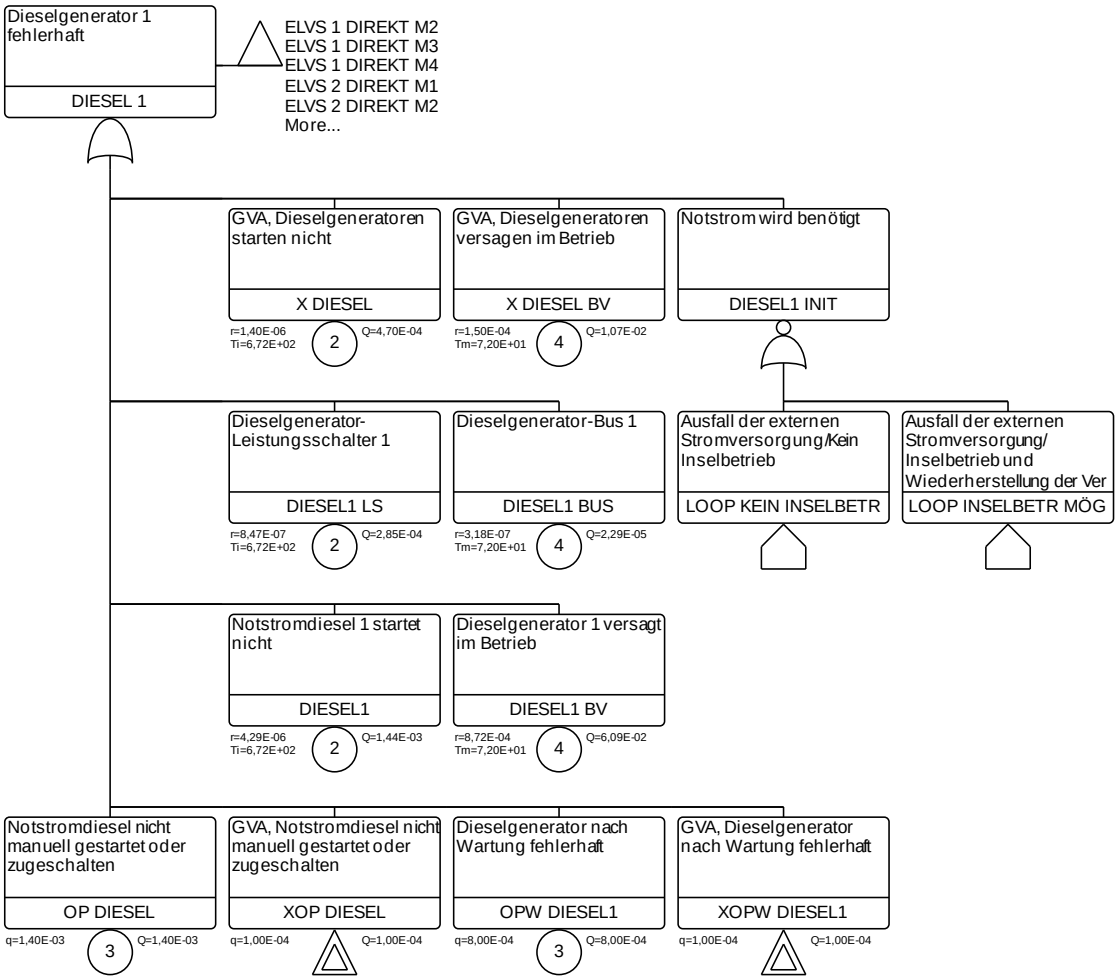


Abb. 8.27 Fehlerbaum zur Verfügbarkeit der Notstromdieselgeneratoren

8.3.5 Modulöffnung und Entladung des Kerns während eines Brennelementwechsels

Im Fall eines Ausfalls des Naturumlaufs während eines Brennelementwechsels kann durch eine Modulöffnung und eine Kernentladung die Naturumlaufkühlung wieder hergestellt werden. Die Ausfallwahrscheinlichkeiten für diese Maßnahmen ergeben sich entsprechend den Fehlerbäumen in Abb. 8.28.

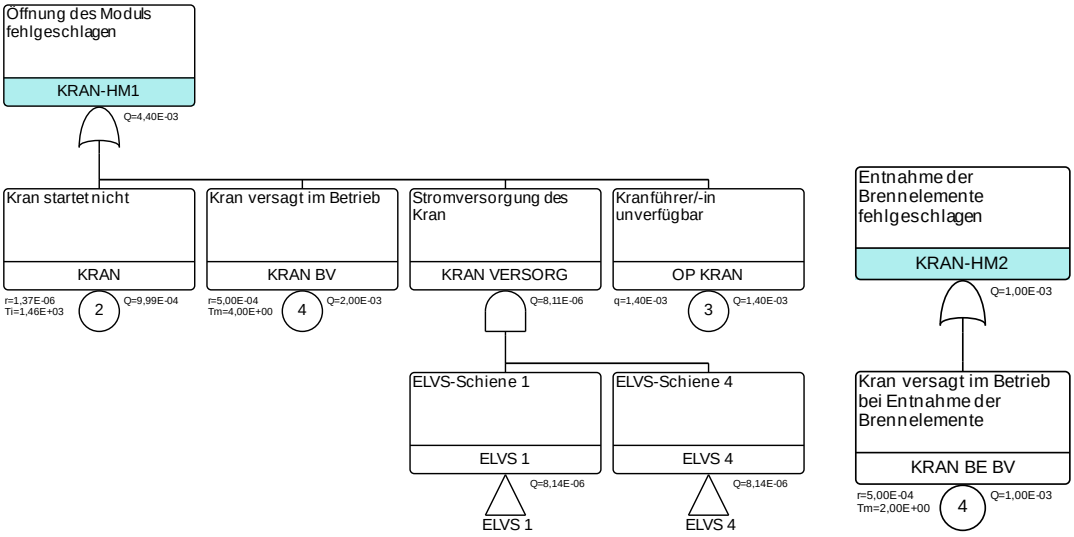


Abb. 8.28 Modulöffnung und Brennelemententnahme durch eine(n) Kranführer/-in

9 Quantifizierung des Anlagenmodells

Die Ereignisabläufe können mit Hilfe der Zuweisung von Zuverlässigkeitskenngrößen für die einzelnen Komponenten der unterliegenden Fehlerbäume quantifiziert werden. Diese Kenngrößen basieren in der Regel auf der Betriebserfahrung für unabhängige Ausfälle von Komponenten und mit zusätzlichen Modellannahmen für GVA gleichartiger Komponenten. Die Bestimmung der Zuverlässigkeitskenngrößen basiert somit auf sehr aufwändigen Verfahren bzgl. Datenerhebung und -auswertung, weshalb für PSA für in Betrieb befindliche Anlagen bestmöglich auf anlagenspezifische Datenquellen zurückgegriffen werden soll.

Im vorliegenden Fall einer PSA für einen SMR ist die Datenlage aufgrund neuartiger Komponenten und nur geringer Betriebserfahrung in Pilotanlagen besonders schlecht. Hier stellt sich die Frage nach der Vergleichbarkeit der Systeme mit konventionellen Anlagen bzgl. deren Zuverlässigkeit. Für die Schätzung der Wahrscheinlichkeit von GVA kann größtenteils der aktuelle Fachband zu PSA-Methoden und Daten /FAK 16/ verwendet werden. Ansonsten wird auf generische Daten oder auf Experteneinschätzungen zurückgegriffen. Das Testintervall für einige Ventile, die im Leistungsbetrieb nicht getestet werden können, erfolgt in unregelmäßigen Abständen bei Abfahren und Abkühlen der Anlage auf unter 93 °C (Abfahren, kalt). In diesem Zustand ist die Anlage ohne die Verwendung von Sicherheitssystemen stabil /NUS 20g/. Anhand der Unterlagen /NUS 20g/ ist davon auszugehen, dass die Tests der in diesem Zustand getesteten Ventile nacheinander erfolgen und nicht verteilt. Das Testintervall beträgt mehr als drei Monate, die Tests finden aber mindestens alle zwei Jahre zum Brennelementwechsel statt, dies wird über eine Lognormalverteilung modelliert.

In den nachfolgenden Abschnitten wird auf die Zeitbudgets für Handmaßnahmen und die Bestimmung der Zuverlässigkeitskenngrößen näher eingegangen.

9.1 Zeitbudgets für Handmaßnahmen

Für die Störfallbeherrschung und zur Verhinderung von Kernschadenszuständen und Versagen der Barrieren druckführende Umschließung und Sicherheitsbehälter gibt es mehrere Eingreifmöglichkeiten des Bedienpersonals. Diese Eingreifmöglichkeiten sind:

- Manuelle Aktivierung der Nachkühlsysteme DHRS-T01, DHRS-T02, DHRS-T03 und DHRS-T04 als Backup für die automatische Aktivierung;

- Manuelle Aktivierung oder Deaktivierung des ECCS, ECCS-T01, ECCS-T03 und ECCS-T04, als Backup für die automatische Aktivierung;
- Einspeisung durch das CVCS, CVCS-T01 und CVCS-T04, wobei diese Maßnahme das Wieder-Öffnen der CIVs, das Durchschalten des deionisierten Wassers und die Aktivierung einer CVCS-Aufbereitungspumpe erfordert. Die Durchführung der Maßnahme kann entweder von der Warte oder lokal erfolgen.
- Sicherheitsbehälter-Fluten über das CFDS, CFDS-T01;
- Einschalten der CFDS-Drainagefunktion, CFDS-T02 und CFDS-T03;
- Notstrom über Gasturbinengenerator oder Notstromdieselgeneratoren, EHVS-T01 und ELVS-T01;
- Schließen von Absperrarmaturen nach einem Leck, falls die automatische Auslösung fehlschlägt, CVCS-T02, CVCS-T03 und RCS-T04;
- Manuelle Auslösung des Überdrucksignals bei niedrigen Temperaturen im RCS (z. B. während eines An- oder Abfahrprozesses), LTOP;
- Öffnen des Moduls und Entladen der Brennelemente bei Ausfall des Naturumlaufes vor oder nach einem Brennelementwechsel, KRAN-T01 und KRAN-T02.

Das Zeitbudget der Betriebsmannschaft teilt sich in drei unterschiedliche Zeitbereiche, wenige Minuten (Inbetriebnahme des DHRS, das CFDS-Fluten des Sicherheitsbehälter, dem Schließen von Absperrarmaturen nach einem KMV oder Maßnahmen zum Schutz vor einem Überdruck im Anfahrprozess), wenige Stunden (Inbetriebnahme des ECCS oder der CVCS-Wiederbespeisung, Dampferzeuger-Abschluss nach einem Dampferzeuger-Bypassleck oder Sicherheitsbehälter-Drainage über das CFDS) und über einem Tag (Schutz der Sicherheitsbehälter-Integrität während einer RCS-Überspeisung) entsprechend Tab. 9.1.

Tab. 9.1 Zeitbudgets für Handmaßnahmen

Eingriffsmöglichkeit	Zeitbudget
Manuelle Aktivierung des ECCS	Eine manuelle Aktivierung des ECCS bzw. eine Öffnung der ECCS-Ventile ist im Fall eines Versagens der automatischen Auslösung möglich. Nach einem KMV in den Sicherheitsbehälter sinkt der Füllstand im RDB entsprechend Abb. 9.2 ab und der Füllstand im Sicherheitsbehälter steigt nach Abb. 9.1. Das Zeitbudget für die manuelle Aktivierung nach fehlerhafter automatischer Aktivierung liegt im Bereich von einer Stunde, um eine Kernabdeckung zu verhindern. Zu diesem Zeitpunkt ist anzunehmen, dass die Systemdiagnose bereits abgeschlossen ist. Das Zeitbudget der Betriebsmannschaft ist da komfortabel und beträgt insgesamt **wenige Stunden**. Schlägt die Handmaßnahme fehl, besteht noch die Möglichkeit, dass der Druck im RCS über die RDB-Außenkühlung sich an den Druck im Sicherheitsbehälter angleicht und die ECCS-Ventile passiv öffnen /NUS 20/. Es ist zu empfehlen, eine ausreichende Effizienz der RDB-Außenkühlung mit einem thermohydraulischen Modell nachzuweisen.
Manuelle Aktivierung des DHRS bzw. Abschluss der Dampferzeuger	Das Zeitbudget beträgt **wenige Minuten**, da sofern der Abschluss der Dampferzeuger nicht vollständig ist, der Kühlmittelverlust im Sekundärkühlkreis die Funktion des DHRS gefährden kann. Im gleichen Zeitraum sollten auch die Auslöseventile des DHRS öffnen, um den RCS zu kühlen. Das Ausdampfen des Druckhalters innerhalb weniger Minuten mit Dampfabgabe über die RSVs in den Sicherheitsbehälter gefährdet den Naturumlauf im RCS. Im Fall einer Dampferzeugerüberspeisung als auslösendem Ereignis steigt der Füllstand im betroffenen Dampferzeuger innerhalb von 2 min von 20 % auf 60 % an, sofern der Dampferzeugerabschluss nach 76 s automatisch ausgelöst wird, Abb. 9.3. Dieses Ereignis ist bzgl. der maximalen Aktivierungszeit des DHRS besonders herausfordernd.
Einspeisung durch das CVCS	Die Einspeisung durch das CVCS wird für den Ausfall des ECCS benötigt. Mit einer Kernabdeckung nach einem KMV in den Sicherheitsbehälter ist nach Abb. 9.2 etwa eine Stunde nach Feststellung eines Ausfalls des ECCS zu rechnen. Die Systemdiagnose sollte zu diesem Zeitpunkt bereits abgeschlossen sein und eine Wiederbespeisung des RCS so weit vorbereitet. Das Zeitbudget der Betriebsmannschaft liegt also insgesamt bei **wenigen Stunden**, analog zur manuellen Aktivierung des ECCS. Im Fall eines Ausfalls des Modulkontrollsystems oder mehrerer beteiligter EDSS-Busse, müssen die Arbeiten lokal im Bereich des Moduls ausgeführt werden.
Überspeisung durch das CVCS: Lokale Deaktivierung der CVCS-Aufbereitungspumpen	Mit einer Einspeiserate von ca. 1,3 l/s füllt sich der Druckhalter nach Alarmierung aufgrund eines hohen Füllstandes (80 %, ca. 5 m³ Restvolumen) innerhalb ca. 1 h. Das CVCS kann bis zu einem Maximaldruck von 155 bar einspeisen, was eine Öffnung der RSVs bewirkt. Ist die Überspeisung des RCS nicht aus der Warte zu stoppen, so hat die Betriebsmannschaft die Möglichkeit, über manuelle Ventile oder die CVCS-Aufbereitungspumpen aus dem Betrieb zu nehmen, die weitere Einspeisung innerhalb **weniger Stunden** zu stoppen und so die Auslösung des ECCS zu verhindern.

Eingriffsmöglichkeit	Zeitbudget
Überspeisung durch das CVCS: Schutz der Integrität des Sicherheitsbehälter durch Deionatabschluss	Nach mehreren Stunden der Überspeisung des RCS ist die Funktion des ECCS aufgrund zu hoher Kühlmittelmengen gefährdet. Die weitere Nachwärmeabfuhr kann direkt über die Außenhülle des RCS, den wassergefüllten Sicherheitsbehälter bis zum Reaktorbecken erfolgen. Das CVCS kann bei anhaltenden Einspeiseraten bis 1,3 l/s in weiteren 71 h 340 m³ Wasser einspeisen (bei Absperrung des Deionatsystems kann maximal 95 m³ boriertes Wasser eingespeist werden), der Sicherheitsbehälter fasst maximal 174 m³ (Einbauten nicht berücksichtigt). Aufgrund der guten Kühlung über die Außenhülle des Sicherheitsbehälter, ist von einem Druckabfall trotz Kühlmitteleinspeisung auszugehen, vgl. Abschnitt 7.4.7. Beschränkt sich das Inventar zur Einspeisung auf die maximal gelagerten 95 m³ im Boreinspeisesystem, so ist nicht davon auszugehen, dass der Auslegungsdruck im Sicherheitsbehälter von 90 bar überschritten wird. Stehen auch die Kühlmittelreserven aus dem Deionatsystem zur Verfügung, so ist es möglich, dass es bis zu einem Hochdruckversagen des Sicherheitsbehälter nach **mehr als einem Tag** kommen kann. Eine Sicherheitsbehälter-Drainage mit Hilfe des CFDS kann wegen zu hohem Druck im Sicherheitsbehälter /NUS 20d/ zu diesem Zeitpunkt nicht mehr durchgeführt werden.
Sicherheitsbehälter-Fluten über das CFDS	Die Wärmeabgabe über den Sicherheitsbehälter muss ähnlich schnell zur Verfügung stehen wie das DHRS, da es bei dessen Ausfall und den zusätzlichen Ausfällen des ECCS und der RSVs benötigt wird, entsprechend Abschnitt 7.4.1. Das Betriebspersonal muss innerhalb von **wenigen Minuten** reagieren, die Maßnahmen in einem ähnlichen Zeitbereich durchführen und das Auffüllen des Sicherheitsbehälter dauert weitere Minuten. Das RCS-Kühlmittelinventar beträgt ca. 60 m³. Die Nachzerfallsleistung liegt bei ungefähr 10 MW. Der RCS-Druck bei 128 bar, die mittlere Kühlmitteltemperatur beträgt 285 °C. Daraus errechnet sich eine Aufwärmzeit des RCS-Kühlmittels von ca. 10 min bis zum Erreichen der Siedetemperatur.
Einschalten der CFDS-Drainagefunktion	Für das Einschalten der CFDS-Drainagefunktion nach einem Leck zwischen Sicherheitsbehälter und Reaktorbecken hängt das Zeitbudget zur Verhinderung der Aktivierung des ECCS stark von der Leckgröße ab und liegt im Bereich von **wenigen Stunden**. Eine eventuelle Dampfabgabe über die RSVs verhindert allerdings eine mögliche Drainage.
Notstrom über Gasturbinengenerator oder Notstromdieselgeneratoren	Das Einschalten der Notstromdieselgeneratoren oder des Gasturbinengenerators erhöht die Wahrscheinlichkeit für die Beherrschung der Transiente nach einem externen Stromausfall. Wichtig ist hier die Möglichkeit der Einspeisung durch das CVCS, **wenige Stunden** nach dem auslösenden Ereignis zur Verhinderung einer möglichen Kernabdeckung, entsprechend der Zeit zur manuellen Aktivierung des ECCS. Für die Sicherheitsbehälter-Flutung über das CFDS stehen nur **wenige Minuten** zur Inbetriebnahme der Notstromversorgung zur Verfügung. Die Systemdiagnose und die Feststellung eines Ausfalls der externen Stromversorgung und der Notstromversorgung ist für die Betriebsmannschaft besonders einfach.

Eingriffsmöglichkeit	Zeitbudget
Schließen von Absperrarmaturen nach einem Leck	Das Zeitbudget beträgt **wenige Minuten** je nach Größe des Lecks. Als Puffer für die Funktion des Naturumlaufes im RCS dient das Volumen des Druckhalters, das bei 50 %-Füllstand ca. 7 m³ beträgt. Ein Kühlmittelverlust von durchschnittlich 25 l/s entleert den Druckhalter nach ca. fünf Minuten. Ein ähnliches Beispiel ist in Abb. 9.4 gezeigt. Sofern der automatische Abschluss des Lecks nach 157 s fehlschlägt, ist mit einer Entleerung des Druckhalters nach 5 min zu rechnen. Danach verliert der Primärkühlkreislauf Kühlmittel und der Naturumlauf und die Wärmeabfuhr über die Dampferzeuger sind gefährdet. Für die manuelle Absperrung des betroffenen Dampferzeugers nach einem Dampferzeuger-Bypassleck (für den Fall, dass der automatische Abschluss fehlschlägt) liegt ein größeres Zeitbudget von **ein bis zwei Stunden** vor. Eine Druckhalterfüllstandkurve nach Dampferzeuger-Bypassleck ist in Abb. 9.5 gezeigt.
Verhinderung eines Überdrucks im RCS beim An- oder Abfahren	Schlägt der LTOP fehl, so bleiben nur **wenige Minuten** für die Betriebsmannschaft, um Gegenmaßnahmen (z. B. die Durchführung einer RESA) einzuleiten. Es wird angenommen, dass die Betriebsmannschaft beim Anfahrprozess auf das betroffene Modul fokussiert ist.
Öffnen des Moduls und Entladen einzelner Brennelemente	Kommt es zu einem Versagen des Naturumlaufes vor oder nach einem Brennelementwechsel, so kann durch Öffnen des Moduls (abgeschätzt 4 h) und Entladen einzelner Brennelemente (abgeschätzt 2 h) die Naturumlaufkühlung wiederhergestellt werden. Ein(e) Kranführer(in) ist typischerweise während des Brennelementwechsels vor Ort. Das Zeitbudget für den Start der Maßnahme liegt im Bereich von **einer Stunde**, hängt jedoch von der Schwere des Ausfalls des Naturumlaufs ab.

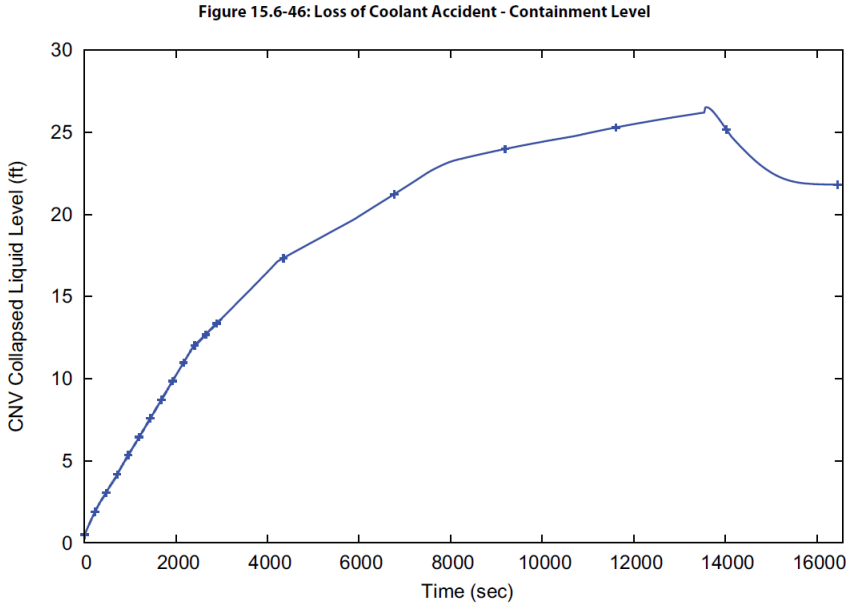


Abb. 9.1 Füllstand im Sicherheitsbehälter nach einem KMV in den Sicherheitsbehälter mit 5 % der maximal anzunehmenden Querschnittsfläche /NUS 20b/, dabei wird nach ca. 13.550 s das ECCS automatisch aktiviert

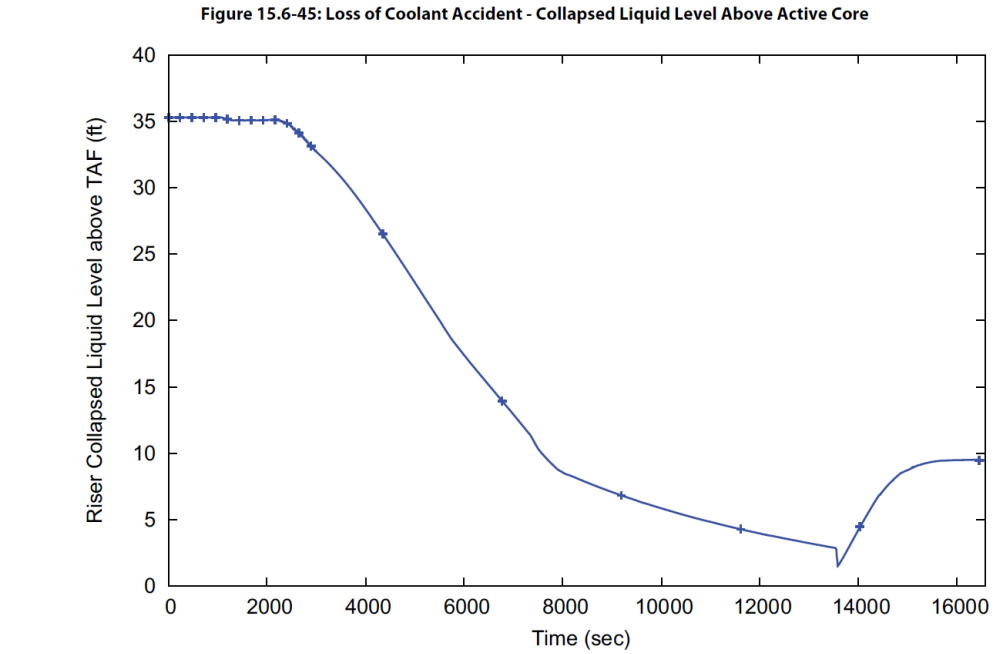


Abb. 9.2 Kernüberdeckung nach einem KMV in den Sicherheitsbehälter mit 5 % der maximal anzunehmenden Querschnittsfläche /NUS 20b/

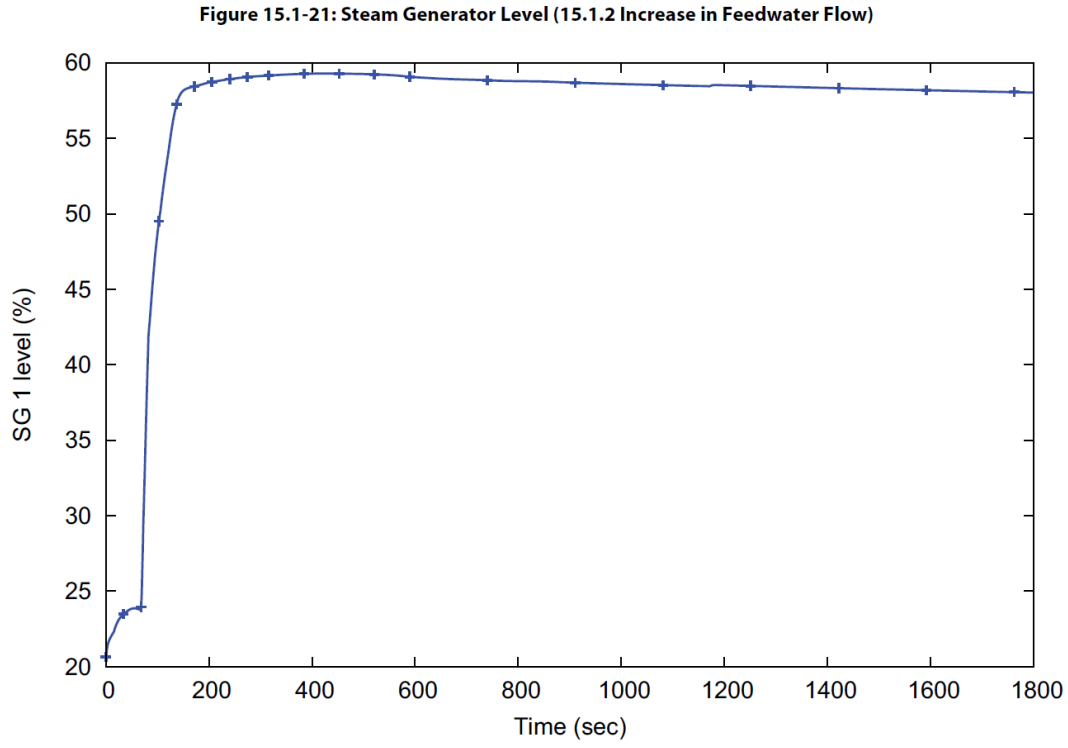


Abb. 9.3 Füllstand im Dampferzeuger nach einer Überspeisung /NUS 20b/, dabei wird nach 76 s der Dampferzeugerabschluss automatisch durchgeführt

Figure 15.6-10: Failure of Lines Carrying Primary Coolant Outside Containment - Maximum Reactor Pressure Vessel Pressure Scenario - Pressurizer Level

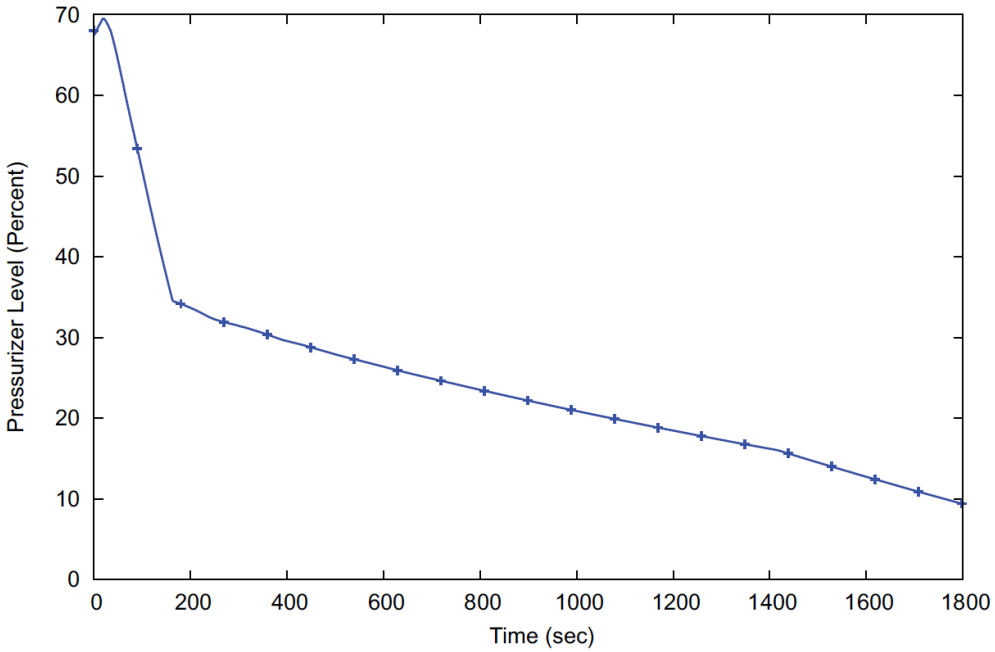


Abb. 9.4 Füllstand im Druckhalter nach KMV außerhalb des Sicherheitsbehälters /NUS 20b/ mit Absperrung des Lecks nach 157 s

Figure 15.6-33: Steam Generator Tube Failure – Limiting Reactor Pressure Vessel Pressure Scenario – Pressurizer Level

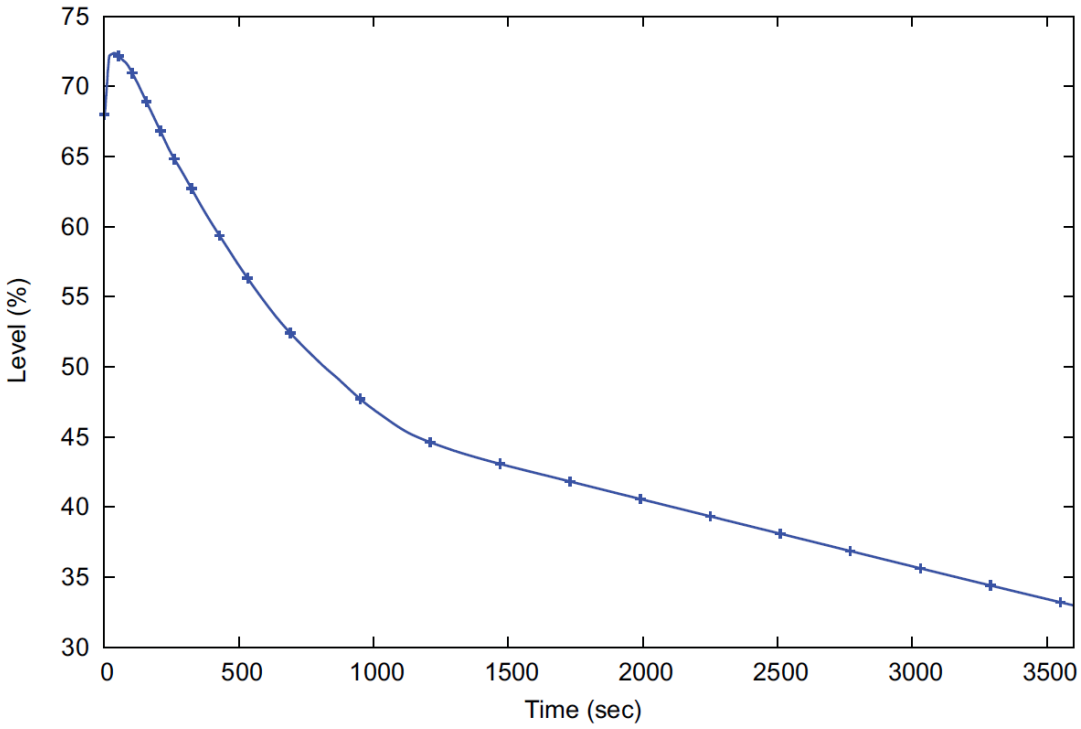


Abb. 9.5 Druckhalterfüllstandsverlauf nach einem Dampferzeuger-Bypassleck /NUS 20b/

9.2 Zuverlässigkeitskenngrößen

Für die Bestimmung der Zuverlässigkeit von Systemen und Komponenten wurden anhand der GRS vorliegenden Daten die in den Fehlerbäumen modellierten Komponentenzuverlässigkeitskenngrößen, ebenso wie die verwendeten Handmaßnahmen, Notfallmaßnahmen und Ausfälle der passiven Systeme quantifiziert. Nachfolgend finden sich in Tab. 9.2 die ermittelten Ausfallraten von Komponenten und Systemen pro Stunde bzw. Ausfallwahrscheinlichkeiten mit deren Verteilungen, basierend auf den jeweiligen Testintervallen, Missionszeiten oder Zeitbudgets zum einen für Pumpen, Komponenten der Stromversorgung, Abschaltelemente, Ventile, Leittechnik sowie weitere Komponenten und Systeme mit aktiver Funktion, zum anderen auch für die Naturumläufe, Handmaßnahmen und Wartungsfehler.

Tab. 9.2 Zuverlässigkeitskenngrößen

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
Pumpen					
CVCS	CVCS-Aufbereitungspumpe 1/2 startet nicht	3,56 E-06, lognormal, EF = 7,89	Testintervall: 7 Tage (Betrieb im Wechsel)	2,99 E-04	/VGB 12/, Borierpumpe
CVCS	CVCS-Aufbereitungspumpe 1/2 versagt im Betrieb	5,98 E-04, lognormal, EF = 10,16	Missionszeit: 72 h	4,21 E-02	/VGB 12/, Borierpumpe
CVCS	GVA der CVCS-Aufbereitungspumpen	–	–	8,27 E-06, lognormal, EF = 4	Generischer Konvoi Zusatzborierpumpen
CVCS	GVA der CVCS-Aufbereitungspumpen im Betrieb	1,62 E-07, lognormal, EF = 4	Missionszeit: 72 h	1,17 E-05	Generischer Konvoi Zusatzborierpumpen
CFDS	CFDS-Pumpe 1/2 startet nicht	3,08 E-06, lognormal, EF = 3,09	Testintervall: 4 Monate (BE-Wechsel eines Moduls)	4,48 E-03	/VGB 12/, Sammelkollektiv 4
CFDS	CFDS-Pumpe 1/2 versagt im Betrieb	5,59 E-06, lognormal, EF = 3,95	Missionszeit: 72 h	4,02 E-04	/VGB 12/, Sammelkollektiv 4
CFDS	GVA beider CFDS-Pumpen	6,35 E-07, lognormal, EF = 4,8	Testintervall: 4 Monate (BE-Wechsel eines Moduls)	9,27 E-04	/FAK 16/, Kreiselpumpe
CFDS	GVA beider CFDS-Pumpen im Betrieb	3,1 E-06, lognormal, EF = 4,9	Missionszeit: 72 h	2,23 E-04	/FAK 16/, Kreiselpumpe
Deionatsystem	Deionatpumpe 1/2/3 startet nicht	7,00 E-07, lognormal, EF = 2,59	Testintervall: 14 Tage (Betrieb im Wechsel)	1,18 E-04	/VGB 12/, Sammelkollektiv 3
Deionatsystem	Deionatpumpe 1/2/3 versagt im Betrieb	7,91 E-06, lognormal, EF = 3,33	Missionszeit: 72 h	5,69 E-04	/VGB 12/, Sammelkollektiv 3
Deionatsystem	GVA 2 von 3 Deionatpumpen	2,18 E-07, lognormal, EF = 4,5	Testintervall: 14 Tage (Betrieb im Wechsel)	3,66 E-05	/FAK 16/, Kreiselpumpe
Deionatsystem	GVA aller Deionatpumpen	4,17 E-07, lognormal, EF = 5,4	Testintervall: 14 Tage (Betrieb im Wechsel)	7,01 E-05	/FAK 16/, Kreiselpumpe

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
Deionatsystem	GVA 2 von 3 Deionatpumpen im Betrieb	1,5 E-06, lognormal, EF = 4,5	Missionszeit: 72 h	1,08 E-04	/FAK 16/, Kreiselpumpe
Deionatsystem	GVA aller Deionatpumpen im Betrieb	2,1 E-06, lognormal, EF = 5,4	Missionszeit: 72 h	1,51 E-04	/FAK 16/, Kreiselpumpe
Boreinspeisesystem	Boreinspeisepumpe 1/2 startet nicht	7,00 E-07, lognormal, EF = 2,59	Testintervall: 14 Tage (Betrieb im Wechsel)	1,18 E-04	/VGB 12/, Sammelkollektiv 3
Boreinspeisesystem	Boreinspeise-pumpe 1/2 ver-sagt im Betrieb	7,91 E-06, lognormal, EF = 3,33	Missionszeit: 72 h	5,69 E-04	/VGB 12/, Sammelkollektiv 3
Boreinspeisesystem	GVA beider Boreinspeise-pumpen	6,55 E-07, lognormal, EF = 4,8	Testintervall: 14 Tage (Betrieb im Wechsel)	1,10 E-04	/FAK 16/, Kreiselpumpe
Boreinspeisesystem	GVA beider Boreinspeise-pumpen im Betrieb	3,1 E-06, lognormal, EF = 4,9	Missionszeit: 72 h	2,23 E-04	/FAK 16/, Kreiselpumpe
CES	CES-Pumpe 1/2 startet nicht	7,00 E-07, lognormal, EF = 2,59	Testintervall: 14 Tage (Betrieb im Wechsel)	1,18 E-04	/VGB 12/, Sammelkollektiv 3
CES	CES-Pumpe 1/2 versagt im Betrieb	7,91 E-06, lognormal, EF = 3,33	Missionszeit: 72 h	5,69 E-04	/VGB 12/, Sammelkollektiv 3
CES	GVA beider CES-Pumpen	6,55 E-07 lognormal, EF = 4,8	Testintervall: 14 Tage (Betrieb im Wechsel)	1,10 E-04	/FAK 16/, Kreiselpumpe
CES	GVA beider CES-Pumpen im Betrieb	3,1 E-06, lognormal, EF = 4,9	Missionszeit: 72 h	2,23 E-04	/FAK 16/, Kreiselpumpe
Stromversorgung					
Turbinengenerator	Lastabwurf auf Eigenbedarf, Inselbetrieb	–	–	2,86 E-01, Beta, α = 8,58	/QUE 14/
Notstromdiesel	Notstromdiesel 1/2 startet nicht	4,29 E-06, lognormal, EF = 2,74	Testintervall: 4 Wochen	1,44 E-03	/VGB 12/, Notstromaggre-gat 320-1.740 kW
Notstromdiesel	Notstromdiesel 1/2 versagt im Betrieb	8,72 E-04, lognormal, EF = 4,80	Missionszeit: 72 h	6,09 E-02	/VGB 12/, Notstromaggre-gat 320-1.740 kW

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
Notstromdiesel	GVA beider Notstromdiesel	1,40 E-06, lognormal, EF = 4,9	Testintervall: 4 Wochen	4,70 E-04	/FAK 16/, Dieselaggregat
Notstromdiesel	GVA beider Notstromdiesel im Betrieb	1,50 E-04, lognormal, EF = 5,4	Missionszeit: 72 h	1,07 E-02	/FAK 16/, Dieselaggregat
Notstromdiesel	Dieselgenerator-Bus 1/2, A1/2 und B1/2	3,18 E-07, lognormal, EF = 4,12	Missionszeit: 72 h	2,29 E-05	/VGB 12/, Sammelschiene 400 – 660 V
Notstromdiesel	Dieselgenerator-Leistungs-schalter 1/2 schließt nicht	8,47 E-07, lognormal, EF = 5,56	Testintervall: 4 Wochen	2,85 E-04	/VGB 12/, Niederspan-nungsleistungsschalter
Gasturbine	Gasturbine startet nicht	7,96 E-06, lognormal, EF = 2,66	Testintervall: 4 Wochen	2,67 E-03	/VGB 12/, Notstromaggre-gat 2.682 - 7.300 kW
Gasturbine	Gasturbine versagt im Betrieb	2,45 E-03, lognormal, EF = 4,69	Missionszeit: 72 h	1,62 E-01	/VGB 12/, Notstromaggre-gat 2682 - 7300 kW
Externe Strom versorgung	Ext. Stromversorgung inner-halb 24 h wiederhergestellt	–	–	3,9 E-02, lognormal, EF = 3	/NUS 20/, diese Größe ist standortabhängig
EHVS	EHVS-Stromschiene 1/2/3/4 versagt im Betrieb	3,96 E-07, lognormal, EF = 8,44	Missionszeit: 72 h	2,85 E-05	/VGB 12/, Sammel-schiene 20 – 30 kV
EHVS	GVA aller vier EHVS-Strom-schienen	3,96 E-08, lognormal, EF = 8,44	Missionszeit: 72 h	2,85 E-06	Beta-Modell
EHVS	EHVS-Haupttransformator 345 kV-13,8 kV	2,17 E-06[32], lognormal, EF = 4,13	Missionszeit: 72 h	1,56 E-04	/VGB 12/, Maschinentransformator
EHVS	EHVS-Leistungsrelais schließt nicht	2,84 E-07, lognormal, EF = 8,44	Testintervall: 4 Wochen	9,54 E-05	/VGB 12/, Generator-schalter 20 - 30 kV
EMVS	EMVS-Stromschiene 1/2/3/4 versagt im Betrieb	4,13 E-07, lognormal, EF = 3,22	Missionszeit: 72 h	2,97 E-05	/VGB 12/, Sammel-schiene 6 - 10,5 kV

[32] Vergleichbar mit dem Wert in /DOY 21/ mit 2,85 E-06/h.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
EMVS	GVA aller vier EMVS-Strom-schienen	4,13 E-08, lognormal, EF = 3,22	Missionszeit: 72 h	2,97 E-06	Beta-Modell
EMVS	EMVS-Transformator 13,8kV-4,16kV	6,91 E-07, lognormal, EF = 3,62	Missionszeit: 72 h	4,98 E-05	/VGB 12/, Eigenbedarfs-transformator
EMVS	EMVS-Leistungsrelais schließt nicht	5,37 E-07, lognormal, EF = 5,17	Testintervall: 4 Wochen	1,80 E-04	/VGB 12/, Leistungs schalter 6 - 10,5 kV
ELVS	ELVS-Strom-schiene 1/2/3/4 versagt im Betrieb	3,18 E-07, lognormal, EF = 4,12	Missionszeit: 72 h	2,29 E-05	/VGB 12/, Sammel-schiene 400-660 V
ELVS	GVA aller vier ELVS-Strom-schienen	3,18 E-08, lognormal, EF = 4,12	Missionszeit: 72 h	2,29 E-06	Beta-Modell
ELVS	ELVS-Transformator 4,16 kV - 480 V	6,20 E-07, lognormal, EF = 4,25	Missionszeit: 72 h	4,46 E-05	/VGB 12/, Niederspan-nungstransformator
ELVS	ELVS-Leistungsschalter schließt nicht	8,47 E-07, lognormal, EF = 5,56	Testintervall: 4 Wochen	2,85 E-04	/VGB 12/, Niederspan-nungsleistungsschalter
EDSS	EDSS-Gleichrichter	3,80 E-06, lognormal, EF = 3,25	Missionszeit: 72 h	2,74 E-05	/VGB 12/, Gleichrichter 220 V
EDSS	EDSS-Bus A/B/C/D versagt im Betrieb	7,84 E-08, Gamma, α = 0,5	Missionszeit: 72 h	5,64 E-06	/NUS 20/
EDSS	GVA aller vier EDSS-Busse	–	–	5,64 E-07	Beta-Modell
EDSS	Batterie 1/2 eines EDSS-Busses A/B/C/D[33]	3,42 E-08, lognormal, EF = 8,44	Testintervall: Monate	3,74 E-05	/VGB 12/, Batterie 220 V
EDSS	GVA zweier Batterien EDSS-Busse einer Redundanz	1,16 E-08, lognormal, EF = 10,8	Testintervall: 3 Monate	1,27 E-05	/FAK 16/, Batterie, keine Spannung

[33] Einzel- und GVA-Ausfälle des gemeinsam genutzten Teils des EDSS werden analog berücksichtigt. Das gemeinsam genutzte EDSS verwendet insgesamt vier Batterien in den zwei Redundanzen, alle vier Batterien werden in einer GVA-Betrachtung entsprechend der GVA-Betrachtung einer Redundanz der modulspezifischen EDSS berück-sichtigt.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
EDSS	GVA dreier Batterien EDSS-Busse einer Redundanz	1,02 E-08, lognormal, EF = 21,3	Testintervall: 3 Monate	1,12 E-05	/FAK 16/, Batterie, keine Spannung
EDSS	GVA aller Batterien EDSS-Busse einer Redundanz	1,59 E-08, lognormal, EF = 71,2	Testintervall: 3 Monate	1,74 E-05	/FAK 16/, Batterie, keine Spannung
Abschalteelemente					
RTS	GVA, 3 oder mehr Abschalt-elemente	1,52 E-09, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	6,66 E-06	/NUS 20/
Aktive Ventile					
DHRS	Auslöseventil 1/2 DE1/2 öff-net nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	4,80 E-03	/NUS 20/
DHRS	GVA der Auslöseventile DE1/2	4,69 E-08, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	2,05 E-04	/NUS 20/
DHRS	GVA aller 4 Auslöseventile	3,15 E-09, Beta, α = 0,5	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)	1,38 E-05[34]	/NUS 20/
Dampferzeuger-Abschluss	MSIV DE1/2 schließt nicht (rechtzeitig)	1,10 E-06[35], Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	4,80 E-03	/NUS 20/

[34] Die Wahrscheinlichkeit für das GVA aller vier Ventile ist vergleichbar und in der gleichen Größenordnung wie für die Absperrventile eines wasserführenden Systems in /FAK 16/.

[35] Werte sind in der gleichen Größenordnung wie in /VGB 12/ für die hydraulisch betriebene Schnellschlussklappe Zwischenkühlsystem mit einer nahezu doppelt so großen Nennweite von 600 mm aber deutlich niedrigeren Arbeitsdrücken. Es gibt nicht viel deutsche Betriebserfahrung zu hydraulisch betriebenen Ventilen. Das eigenmediumbetätigte Frischdampf-Abblaseventil ist von den Betriebsparametern ähnlich und ist mit einer niedrigeren Ausfallrate von 7,73 E-08/h bestimmt, /VGB 12/. In diesem Falle muss aber noch der mögliche GVA der beiden magnetbetätigten Vorsteuerventile mit einer Ausfallrate von 5,04 E-07 berücksichtigt werden /FAK 16/, dadurch ergibt sich die gleiche Größenordnung wie in /NUS 20/.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
Dampferzeuger-Abschluss	GVA der beiden MSIV	4,69 E-08, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	2,05 E-04	/NUS 20/
Dampferzeuger-Abschluss	Backup-MSIV DE1/2 schließt nicht (rechtzeitig)	1,10 E-06, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	4,80 E-03	/NUS 20/
Dampferzeuger-Abschluss	GVA der beiden Backup-MSIV	4,69 E-08[36], Beta, α = 0,5	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)	2,05 E-04	/NUS 20/
Dampferzeuger-Abschluss	GVA aller MSIV und Backup-MSIV	3,15 E-09, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	1,38 E-05	/NUS 20/
Dampferzeuger-Abschluss	FWIV DE1/2 schließt nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	4,80 E-03	/NUS 20/
Dampferzeuger-Abschluss	GVA beider FWIV	4,69 E-08, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	2,05 E-04	/NUS 20/
Dampferzeuger-Abschluss	Speisewasser-Regelventil DE1/2 schließt nicht[37]	4,24 E-06, lognormal, EF = 4,04	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)	1,83 E-02	/VGB 12/, Volllastregelventil
Dampferzeuger-Abschluss	GVA beider Speisewasser-Regelventile	2,52 E-07, lognormal, EF = 8,7	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	1,10 E-03	/FAK 16/, Regelventil

[36] Ein GVA der vier beteiligten magnetbetätigten Vorsteuerventilen liegt nach /FAK 16/ bei 2,29E-07/h und damit deutlicher höher als die Werte von /NUS 20/, allerdings arbeiten diese Ventile auch unter anderen Betriebsbedingungen.

[37] Das vollständige Schließen der Speisewasser-Regelventile kann im Betrieb nicht getestet werden, aber die Ventile sind grundsätzlich dauerhaft im Einsatz.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
CVCS-Abschluss	CIV1/2 der CVCS-Einspeise-leitung schließt nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
CVCS-Abschluss	GVA beider CIV der CVCS-Einspeiseleitung	4,69 E-08, Beta, α = 0,5	Testintervall: 3 Monate	5,14 E-05[38]	/NUS 20/
CVCS-Abschluss	CIV1/2 der CVCS-Einspeise-leitung öffnet nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
CVCS-Abschluss	CIV1/2 der CVCS-Entnahme-leitung schließt nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
CVCS-Abschluss	GVA beider CIV der CVCS-Entnahmeleitung	4,69 E-08, Beta, α = 0,5	Testintervall: 3 Monate	5,14 E-05	/NUS 20/
CVCS-Abschluss	CIV1/2 der CVCS-Entnahme-leitung öffnet nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
CFDS-Abschluss	CIV1/2 des CFDS öffnet nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
Deionat-Abschluss	Deionatabsperrventil 1/2 öffnet nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
Deionat-Abschluss	Deionatabsperrventil 1/2 schließt nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 3 Monate	1,20 E-03	/NUS 20/
Deionat-Abschluss	GVA beider Deionat absperrventile	4,69 E-08, Beta, α = 0,5	Testintervall: 3 Monate	5,14 E-05	/NUS 20/
ECCS	ECCS-Ventil öffnet nicht	1,34 E-08, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)[39]	5,87 E-05	/NUS 20/

[38] Die Ausfallwahrscheinlichkeit von NuScale (Ventile + Auslösehydraulik) für den GVA ist vergleichbar mit den Werten für den Ausfall (Schließversagen) zweier Absperrventile (motorgesteuerte Ventile) nach /FAK 16/.

[39] Die Tests finden unter kälteren Bedingungen und niedrigeren Differenzdrücken als im Anforderungsfall statt.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
ECCS	GVA der RVV 3v3	2,83 E-10, Beta, α = 0,5	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)[39]	1,24 E-06	/NUS 20/
ECCS	GVA der RVVs 2v3	1,24 E-10, lognormal, EF = 6,6	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	5,43 E-07	/FAK 16/, Absperrventil (dampf-führend), reskaliert[40]
ECCS	GVA der RRV	5,75 E-10, Beta, α = 0,5	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	2,52 E-06	/NUS 20/
ECCS	Magnetventil eines ECCS-Ventils öffnet nicht	8,68 E-08, Beta, α = 11,5	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	3,80 E-04	/NUS 20/
ECCS	GVA 2 von 2 Magnetventile der RRV	3,72 E-09, Beta, α = 0,5	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	1,63 E-05	/NUS 20/
ECCS	GVA 2 von 6 Magnetventile	4,18 E-10, lognormal, EF = 4,4	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	6,48 E-07	/FAK 16/, Vorsteuerventil (magnet-betätigt), reskaliert[41]
ECCS	GVA 3 von 6 Magnetventile	1,48 E-10, lognormal, EF = 4,7	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	4,95 E-07	/FAK 16/, Vorsteuerventil (magnet-betätigt), reskaliert

[40] Die Absperrventile sind motorgesteuert, die RVVs werden hydraulisch betätigt. Die Ausfallraten wurden über die Werte von NuScale /NUS 20/ reskaliert (3 Größenordnungen niedrigere GVA-Wahrscheinlichkeit), die Vorsteuerventile scheinen aber, der Größenordnung nach zu urteilen, nicht in den NuScale Ausfallwahrscheinlichkeiten für die RVVs und RRVs enthalten sein.

[41] Die Vorsteuerventile der deutschen Betriebserfahrung sind den Bedingungen im Primär- oder Sekundärkühlkreislauf ausgesetzt, was von den Bedingungen im NuScale-SMR abweicht. Aus diesem Grund werden die GVA-Werte im Vergleich mit /NUS 20/ um einen Faktor 270 reskaliert.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
ECCS	GVA 4 von 6 Magnetventile	1,13 E-10, lognormal, EF = 5,4	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	9,29 E-07	/FAK 16/, Vorsteuerventil (magnet-betätigt), reskaliert
ECCS	GVA 5 von 6 Magnetventile	2,12 E-10, lognormal, EF = 6,3	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	3,63 E-07	/FAK 16/, Vorsteuerventil (magnet-betätigt), reskaliert
ECCS	GVA 6 von 6 Magnetventile	1,19 E-09, lognormal, EF = 10,7	Testintervall: 12 Monate, lognormal EF = 1,3 (Abfahren, kalt)[39]	5,21 E-06	/FAK 16/, Vorsteuerventil (magnet-betätigt), reskaliert
CVCS	Drei-Wege-Mischventil schaltet nicht um	1,62 E-06, lognormal EF = 3,27	Testintervall: 7 Tage	1,36 E-04	/VGB 12/, Dreiwegeventil
Nukleares Drainagesystem	Systemventil öffnet nicht	1,10 E-06, Beta, α = 0,5	Testintervall: 7 Tage	9,24 E-05	/NUS 20/
Passive Ventile					
Reaktorschutz	RSV 1/2 öffnet nicht	2,50 E-07, lognormal, EF = 3,38	Testintervall: 40 Monate (alle 5 Jahre und 20% alle 2 Jahre), lognormal, EF = 1,55	3,64 E-03	/VGB 12/, DH-Sicherheitsventil
Reaktorschutz	RSV 1/2 schließt nach Druckabfall nicht wieder	5,01 E-08, Beta, α = 0,5	Testintervall: 40 Monate, lognormal, EF = 1,55	7,31 E-04	/NUS 20/
Reaktorschutz	GVA der RSVs	3,21 E-09, Beta, α = 0,5	Testintervall: 40 Monate, lognormal, EF = 1,55	4,69 E-05	/NUS 20/
CVCS	Überströmventil der CVCS-Entnahmeleitung schließt nicht	–	–	0,1, lognormal, EF = 10	/NUS 20/
CVCS	Rückschlagventil der CVCS-Einspeiseleitung schließt nicht	–	–	0,1, lognormal, EF = 10	/NUS 20/
ECCS	Passive Öffnung der ECCS-Ventile (RVVs und RRVs)	–	–	0,1, lognormal, EF = 10	/NUS 20/

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
ECCS	GVA Passive Öffnung der RVVs/RRVs	–	–	0,01[42]. lognormal, EF = 10	Eigene Abschätzung
Dampferzeuger-Abschluss	Speisewasser-Rückschlag-ventil DE1/2 schließt nicht	1,66 E-07, lognormal, EF = 5,66	Testintervall: 2 Jahre (Brennelementwechsel)	1,45 E-03	/VGB 12/, Rückschlagventil
Dampferzeuger-Abschluss	GVA beider Speisewasser-Rückschlagventile	1,56 E-08, lognormal, EF = 12,0	Testintervall: 2 Jahre (Brennelementwechsel)	1,36 E-04	/FAK 16/, Rückschlagventil
Dampferzeuger-Abschluss	Backup-Speisewasser-Rück-schlagventil DE1/2 schließt nicht	1,66 E-07, lognormal, EF = 5,66	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	7,27 E-04	/VGB 12/, Rückschlagventil
Dampferzeuger-Abschluss	GVA beider Backup-Speise-wasser-Rückschlagventile	1,56 E-08, lognormal, EF = 12,0	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	6,83 E-05	/FAK 16/, Rückschlagventil
Dampferzeuger-Abschluss	GVA aller Speisewasser-Rückschlagventile	4,81 E-09, lognormal, EF = 23,9	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	2,11 E-05	/FAK 16/, Rückschlagventil
ECCS	IAB eines ECCS-Ventils schließt nicht	1,58 E-07, lognormal, EF = 8,44	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)[39]	6,92 E-04	/VGB 12/, Federvorsteuerventil der Druckhalterarmatur
ECCS	Fehlerhafte Blockierung, IAB eines ECCS-Ventils öffnet nicht	4,78 E-07, lognormal, EF = 4,33	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)[39]	2,09 E-03	/VGB 12/, Federvorsteuerventil der Druckhalterarmatur

[42] Die passive Öffnung für die RVVs und RRVs ist für alle Unfallabläufe außer dem Überdruck im kalten RCS modelliert. Allerdings ist die Öffnung an die Druckangleichung zwischen RCS und SB gekoppelt. Im Falle eines ausreichend großen KMV in den SB ist dieser Druckangleich trivial gegeben, Abb. 7.8. Ist das DHRS verfügbar, so baut sich der Druck im Primärkreis ab. Nach einem Ausfall der Primärkreiskühlung kann zunächst nur über die RSVs und später nur noch über die RDB-Außenkühlung Druck im RCS abgebaut werden. Kommt es zu keiner Druckangleichung, so ist mit einem vollständigen Ausfall der passiven Öffnung der ECCS-Ventile zu rechnen.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
ECCS	GVA, fehlerhafte Blockierung, IAB der RRV öffnen nicht	4,35 E-07, lognormal, EF = 6,3	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	1,90 E-03	/FAK 16/, Vorsteuerventil (federbelastet)
ECCS	GVA 2 von 3, fehlerhafte Blockierung, IAB zweier RVVs öffnen nicht	2,14 E-07, lognormal, EF = 5,4	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	9,37 E-04	/FAK 16/, Vorsteuerventil (federbelastet)
ECCS	GVA, fehlerhafte Blockierung, IAB aller RVVs öffnen nicht	2,27 E-07, lognormal, EF = 8,0	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	9,94 E-04	/FAK 16/, Vorsteuerventil (federbelastet)
Leittechnik					
RTS	GVA zweier Redundanzen – Ausfall automatische RESA	1,69 E-10: lognormal, EF = 10	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	7,40 E-07	/NUS 20/, „Reactor trip breakers“
ESFAS	ESFAS I/II zur automatischen Auslösung einer Sicherheitsfunktion fehlerhaft[43]	8,26 E-08, lognormal, EF = 10	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	3,62 E-04	/NUS 20/
ESFAS	GVA zweier Redundanzen – Ausfall einer Sicherheitsfunktion[43]	7,44 E-10, lognormal, EF = 10	Testintervall: 12 Monate, lognormal, EF = 1,3 (Abfahren, kalt)	3,26 E-06	/NUS 20/
Modulkontrollsystem	Steuerung zum Start des CVCS- und des CFDS-Systems fehlerhaft	–	–	1 E-06 Lognormal, EF = 10	Eigene Abschätzung

[43] Als Sicherheitsfunktionen sind hier die Auslösungen des ECCS und des DHRS, das LTOP, die Abschlüsse des CVCS, der Dampferzeuger und des Deionatsystems unabhängig berücksichtigt.

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
Weitere Komponenten und Systeme					
Komponenten-hilfssysteme	Ausfall Zwischenkühlsystem oder System für komprimierte Luft	1,85 E-06, lognormal, EF = 10	Missionszeit: 72 h	1,33 E-04	/NUS 20/, Wert für das entsprechende auslösende Ereignis
Kran	Kran startet nicht	1,37 E-06, Beta, α = 0,5	Testintervall: 2 Monate	1,0 E-03	Eigene Abschätzung
Kran	Kran versagt im Betrieb	5 E-04 Gamma, α = 0,5	Missionszeiten: 4h: Modulöffnung 2h: Entnahme von Brennelementen	Modulöffnung: 2,0 E-03, Entnahme von Brennele-menten: 1,0 E-03	Eigene Abschätzung
DHRS	Fehlende Entlüftung der DHRS-Redundanz 1/2 und Ausfall der Überwachung	–	–	1,00 E-06, lognormal, EF = 10	Eigene Abschätzung
CFDS	Heizvorrichtung zur Ventilöffnung startet nicht	–	–	1,00 E-03, lognormal, EF = 10	Eigene Abschätzung
Naturumläufe					
DHRS	Ausfall Naturumlaufes unter Auslegungsbedingungen	5,56 E-08, lognormal, EF = 3	Missionszeit: 72 h	4 E-06	/NUS 20/
DHRS	GVA des DHRS-Naturumlaufes, Dampferzeuger-Verstopfung	3,57 E-08, lognormal, EF = 3	Missionszeit: 72 h	2,57 E-06	/NUS 20/
DHRS	GVA des Naturumlaufes bei-der Redundanzen des DHRS nach KMV	1 E-07, lognormal, EF = 3	Missionszeit: 72 h	7,2 E-06	Eigene Abschätzung
ECCS	Ausfall des Naturumlaufes unter Auslegungsbedingun-gen	1,39 E-09, lognormal, EF = 2	Missionszeit: 72 h	1,0 E-07	/NUS 20/
ECCS	Ausfall des Naturumlaufes für nur eine Redundanz der RVVs	1 E-06, lognormal, EF = 3	Missionszeit: 72 h	7,2 E-05	Eigene Abschätzung

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
ECCS	Ausfall des Naturumlaufes im Fall nur eines geöffneten RRV	1 E-07, lognormal, EF = 3	Missionszeit: 72 h	7,2 E-06	Eigene Abschätzung
Handmaßnahmen					
CVCS	Leckabsperrung	–	Zeitbudget: wenige Minuten	4,0 E-03	Eigene Abschätzung
CVCS	Lokale Verhinderung einer dauerhaften Überspeisung	–	Zeitbudget: wenige Stunden	1,4 E-03	Eigene Abschätzung
CVCS	Deionat-Abschluss	–	Zeitbudget: wenige Stunden	2,2 E-04	Eigene Abschätzung
CVCS	Lokale Handmaßnahmen zur Wiederbespeisung	–	Zeitbudget: wenige Stunden	1,4 E-03	/NUS 20/
CVCS	Handmaßnahmen (aus Kontrollraum) zur Wiederbespeisung	–	Zeitbudget: wenige Stunden	2,2 E-04	Eigene Abschätzung
ECCS	Manuelle Aktivierung des ECCS	–	Zeitbudget: wenige Stunden	2,2 E-04	/NUS 20/
RCS	Verhinderung eines Über-drucks im RCS beim An- oder Abfahren	–	Zeitbudget: wenige Stunden	4,0 E-03	Eigene Abschätzung
RCS	Absperrung des betroffenen Dampferzeugers nach einem Dampferzeuger-Bypasslecks	–	Zeitbudget: wenige Stunden	2,2 E-04	Eigene Abschätzung
CFDS	SB-Drainage nach Leck im SB	–	Zeitbudget: wenige Stunden	2,2 E-04	Eigene Abschätzung
CFDS	SB-Fluten	–	Zeitbudget: wenige Stunden	4,0 E-03	/NUS 20/
Dampferzeuger-Abschluss und DHRS	Manuelle Aktivierung des DHRS bzw. Abschluss der Dampferzeuger	–	Zeitbudget: wenige Stunden	4,0 E-03	Eigene Abschätzung
Dieselgeneratoren	Notstrom über Dieselgeneratoren	–	Zeitbudget: wenige Stunden	1,4 E-03	/NUS 20/

System	Ereignis	Ausfallrate [1/h]	Testintervall, Missionszeit oder Zeitbudget	Ausfallwahr-scheinlichkeit	Quelle
Gasturbine	Notstrom über Gasturbine	–	Zeitbudget: wenige Stunden	1,4 E-03	/NUS 20/
Kran	Modulöffnung und Entladen einzelner Brennelemente	–	Zeitbudget: wenige Stunden	1,4 E-03	Eigene Abschätzung
Wartungsfehler					
CFDS	Teil A/B der manuellen Ventile falsch eingestellt	–	–	9,7 E-04, lognormal, EF = 5	/NUS 20/
CVCS	Teil A/B der manuellen Ventile falsch eingestellt	–	–	9,7 E-04, lognormal, EF = 5	/NUS 20/
Dampferzeuger-Abschluss	MSIV-Bypass Dampferzeuger 1/2 fehlerhaft offen und schließt nicht	–	–	4,66 E-06, lognormal, EF = 5	„Schließt nicht“: 4,8 E-03 und „fehlerhaft nach Wartung“: 9,7 E-04
Dampferzeuger-Abschluss	Backup-MSIV-Bypass DE1/2 fehlerhaft offen und schließt nicht	–	–	4,66 E-06, lognormal, EF = 5	
Gasturbine	Gasturbine nach Wartung fehlerhaft	–	–	8,0 E-04, lognormal, EF = 10	/NUS 20/
Dieselgeneratoren	Dieselgenerator 1/2 nach Wartung nicht funktionsfähig	–	–	8,0 E-04, lognormal, EF = 10	/NUS 20/

9.3 Modellierung der Fehlerwahrscheinlichkeit von Handmaßnahmen innerhalb einer Sequenz

Sind im Laufe einer Sequenz mehrere Handmaßnahmen notwendig, bzw. schlägt die erste Handmaßnahme fehl und weitere Handmaßnahmen sind daraufhin erforderlich, so hängen die Fehlerwahrscheinlichkeiten der Handmaßnahmen teilweise voneinander ab. Abhängigkeiten ergeben sich insbesondere bei der Unterlassung von Handmaßnahmen. Die Betriebsmannschaft, die einen Fehler macht, kann als (temporär) fehleranfällig betrachtet werden. Dieser Zustand der Fehleranfälligkeit erhärtet sich mit jedem weiteren Fehler einer folgenden Aufgabe /SWA 83/. Im Ergebnis ist die Fehlerwahrscheinlichkeit für mehrere Handmaßnahmen in abhängiger Betrachtung signifikant höher als das Produkt der Fehlerwahrscheinlichkeit für alle Handmaßnahmen in unabhängiger Betrachtung.

Die Modellierung der Fehler bei der Diagnose des Modulzustandes und der Durchführung von Handmaßnahmen wurde die Alpha-Faktor Methode angewendet. Hierfür teilt sich die Gesamtfehlerwahrscheinlichkeit zunächst in einen unabhängigen Teil, der u. a. die Unterschiede der durchzuführenden Handmaßnahmen berücksichtigt, und einen abhängigen Teil, der Gemeinsamkeiten modelliert. Zu den Unterschieden zählen beispielsweise die unterschiedlichen Bedingungen bei der Durchführung der Maßnahmen, z. B. lokal oder aus der Warte durchgeführt, Start eines Dieselgenerators oder Öffnung eines Ventils, auch sind teilweise andere Personen mit den Aufgaben betraut, z. B. Elektriker oder andere Techniker. Gemeinsamkeiten der Handmaßnahmen werden über die Alpha-Faktor Methode modelliert, hierzu zählen z. B. eine korrekte Analyse des Modulzustandes, der Qualifizierungsstand einzelner Mitarbeiter oder deren Umgang mit Stress. Gleichartige Fehler bei der Moduldiagnose und Durchführung von Handmaßnahmen werden entsprechend der Anzahl der möglichen Handmaßnahmen innerhalb einer Ereignisablaufanalyse wie folgt quantifiziert /SWA 83/:

- Einzelfehler:
  $W_1 = N = 1{,}0 \cdot 10^{-4}$,
- zwei gleichartige Fehler, niedrige Abhängigkeit:
  $W_2 = W_1 \cdot W_{\mathrm{nA}} = N \cdot \frac{1 + 19 \cdot N}{20} = 5{,}01 \cdot 10^{-6}$,
- dritter gleichartiger Fehler, mittlere Abhängigkeit:
  $W_3 = W_2 \cdot W_{\mathrm{mA}} = N \cdot \frac{1 + 19 \cdot N}{20} \cdot \frac{1 + 6 \cdot N}{7} = 7{,}16 \cdot 10^{-7}$,

– vierter gleichartiger Fehler: hohe Abhängigkeit:
$W_4 = N \cdot \frac{1+19 \cdot N}{20} \cdot \frac{1+6 \cdot N}{7} \cdot \frac{1+N}{2} = 3{,}58 \cdot 10^{-7}$,

– mehr als vier gleichartige Fehler, komplette Abhängigkeit:
$W_{>4} = W_4 = 3{,}58 \cdot 10^{-7}$.

Da eine Handmaßnahme nicht nur durch einen Einzelfehler, sondern auch durch weitere gleichartige Fehler keinen Erfolg hat, sollen die gleichartigen Fehlerwahrscheinlichkeiten rekursiv von den Fehlerwahrscheinlichkeiten für eine geringere Anzahl gleichartiger Fehler abgezogen werden. Für n Handmaßnahmen innerhalb einer Ereignisablaufanalyse gilt:

– n gleichartige Fehler: $W'_n = W_n$,

– n-1 gleichartige Fehler: $W'_{n-1} = W_{n-1} - W'_n$,

– n-2 gleichartige Fehler: $W'_{n-2} = W_{n-2} - \sum_{i=0}^{1} \binom{1}{i} \cdot W'_{n-i}$,

– x gleichartige Fehler: $W'_x = W_x - \sum_{i=x+1}^{n} \binom{n-x}{n-i} \cdot W'_i$,,

– Einzelfehler: $W'_1 = W_1 - \sum_{i=2}^{n} \binom{n-1}{n-i} \cdot W'_i$

Da bei den Ereignisabläufen nur entweder 3, 4 bzw. 8 Maßnahmen durchzuführen sind, werden für das PSA-Modell diese drei Fälle verwendet, n = 3, 4 und 8. Die passenden Modellparameter sind in Tab. 9.3 angegeben.

Tab. 9.3 Wahrscheinlichkeiten für gleichartige Fehler der Betriebsmannschaft während eines Ereignisablaufes

Zahl der Handmaßnahmen	n = 3	n = 4	n = 8
1	W'_1 = 9,07 E-05	W'_1 = 8,68 E-05	W'_1 = 7,46 E-05
2	W'_2 = 4,29 E-06; α_2 = 4,50 E-2	W'_2 = 3,94 E-06; α_2 = 6,34 E0-2	W'_2 = 2,50 E-06; α_2 = 1,02 E-1
3	W'_3 = 7,16 E-07; α_3 = 2,51 E-03	W'_3 = 3,58 E-07; α_3 = 3,84 E-03	W'_3 = 3,58 E-07; α_3 = 2,92 E-02
4 bis 7	–	W'_4 = 3,58 E-07; α_4 = 9,61 E-04	W'_{4-7} = 0,0; $\alpha_{4\text{-}7}$ = 0,0
8	–	–	W'_8 = 3,58 E-07; α_8 = 5,21 E-04

Der Fehlerbaum zur Beschreibung einer Fehlerabhängigkeit n = 3 für den gleichartigen Ausfall von Gasturbine und Dieselgeneratoren nach einer Wartung ist in Abb. 9.6 dargestellt. Die Fälle GVA OPW USV-2AA und GVA OPW USV-2AB beschreiben den gleichartigen Ausfall der Gasturbine und eines Dieselgenerators. Das Ereignis GVA OPW USV-ALL beschreibt den Ausfall aller drei Quellen für Notstrom. Der Fehlerbaum bezieht sich auf den Ereignisablauf eines Notstromfalls.

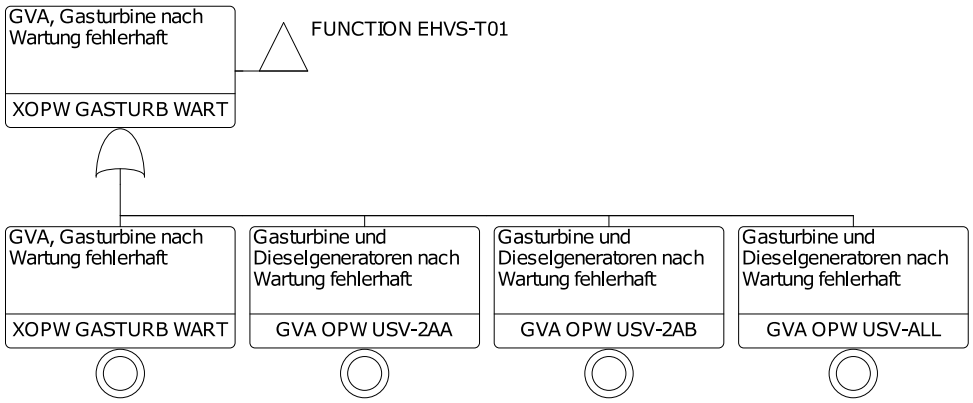


Abb. 9.6 Fehlerbaum zur Beschreibung eines gleichartigen Ausfalls der Gasturbine und/oder der Dieselgeneratoren nach fehlerhafter Wartung

9.4 Modulübergreifende Betrachtungen

Modulübergreifende auslösende Ereignisse sind beispielsweise der Verlust der externen Stromversorgung, Verlust der Hilfssysteme oder Feuer- und Überflutungsereignisse. Für diese Ereignisse ergeben sich zusätzliche Randbedingungen bzgl. der Verfügbarkeiten folgender Systeme bzw. Maßnahmen:

- Boreinspeisesystem (ein System für bis zu zwölf Module),
- Deionatsystem (ein System für bis zu zwölf Module),
- Verfügbarkeit von Handmaßnahmen (die Betriebsmannschaft ist möglicherweise mit mehreren Modulen gleichzeitig beschäftigt),
- Fehlerhafte Ausführung von Reparaturen, Wartungsarbeiten oder Testläufen (gemeinsamer Ausfall gleicher Systeme unterschiedlicher Module möglich),
- Reaktorbecken als Not- und Nachwärmesenke (ein System für alle zwölf Module),
- CFDS (ein System für bis zu sechs Module),

- Notstromdieselgeneratoren (zwei Diesel, mindestens einer ist für die Versorgung der zwölf Module notwendig, allerdings ist die Leistung begrenzt und es können nicht alle Pumpen gleichzeitig betrieben werden),
- Gasturbine (ein System für zwölf Module).

Die Auswirkungen modulübergreifender Faktoren auf die Kernschadenshäufigkeiten soll anhand zweier wichtiger auslösender Ereignisse, die modulübergreifend wirken, untersucht werden. Eine entsprechende Analyse, die Multi-Unit PSA (auch als Multi-Module PSA bezeichnet), wird in Abschnitt 11 beschrieben.

10 Ergebnisse der PSA der Stufe 1

Das oben beschriebene PSA-Modell behandelt ein einzelnes SMR-Reaktormodul bzw. eine Transiente, die unabhängig von den anderen Modulen in nur einem Reaktor abläuft. Dieses Modell wird nachfolgend ausgewertet, insbesondere werden die Kernschadenshäufigkeiten[44] quantifiziert.

In Abschnitt 10.1 sind die Kernschadenshäufigkeiten nach auslösendem Ereignis aufgeschlüsselt und die für das Ergebnis einflussreichsten Systemausfälle angegeben. In Abschnitt 10.2 werden die Ausfallwahrscheinlichkeiten der einzelnen Systeme miteinander verglichen. Als Startpunkt für eine mögliche Fortsetzung der Arbeiten in einer PSA der Stufe 2 sind die Häufigkeiten der unterschiedlichen Kernschadenszustände in Abschnitt 10.3 angegeben und die wichtigsten Minimalschnitte. Darüber hinaus findet sich ein Vergleich mit den wichtigsten Minimalschnitten der NuScale-PSA /NUS 20/. Die für das Ergebnis besonders relevanten Parameterwerte sind in Abschnitt 10.4 präsentiert.

10.1 Kernschadenshäufigkeiten nach auslösenden Ereignissen

Die Kernschadenshäufigkeiten aufgeschlüsselt nach auslösendem Ereignis sind in der vierten Spalte in Tab. 10.1 dargestellt. Das funktionale Versagen des RCS und der interne Brand machen jeweils ca. ein Viertel der Kernschadenhäufigkeit aus. Die andere Hälfte der Kernschadenshäufigkeit ist durch den Absturz eines Moduls im Reaktor- oder Brennelementwechselbecken gegeben. Die Ergebnisse finden sich grafisch in der Abb. 10.1.

[44] Der Endzustand eines Überdruckversagens des RCS wird auch als Kernschadensendzustand bewertet.

Tab. 10.1 Ergebnisse der PSA der Stufe 1 für alle Kernschadensendzustände

Kürzel	Kernschaden nach/im …	Häufigkeiten (pro Jahr)					Hauptbeiträge der Systeme
		Auslösendes Ereignis	CDF, Mittelwert	Anteil [%]	CDF, 5% Perzentil	CDF, 95% Perzentil	
LB	Leistungsbetrieb	2,5 E+00	1,2 E-07	61,3	9,2 E-09	3,6 E-07	1. RCS 2. Notstrom
T	Transienten	1,3 E+00	5,8 E-08	29,2	3,5 E-09	2,1 E-07	1. RCS 2. Notstrom
TA	Allgemeine Transiente	1,3E+00	9,5 E-10	0,48	1,2 E-12	2,4 E-09	1. DHRS 2. RSVs
TN	Ausfall der externen Stromversorgung	2,2 E-02	6,9 E-09	3,45	2,0 E-11	2,1 E-08	1. ELVS 2. Notstrom
TD	EDSS-Ausfall	4,7 E-05	2,7 E-10	0,14	3,9 E-12	9,4 E-10	1. CIS 2. ECCS
TS	Leitungsleck im Sekundärkühlkreis	4,4 E-05	1,9 E-12	0,0009	5,1 E-15	6,4 E-12	1. RSV 2. DHRS
TÜ	Dampferzeuger-Überspeisung	1,0 E-05	4,1 E-13	0,0002	1,1 E-15	1,4 E-12	1. RSV 2. DHRS
TH	Überspeisung durch das CVCS	1,0 E-05	1,6 E-13	0,00008	3,6 E-16	5,6 E-13	1. CIS/CVCS 2. ECCS
TV	Ausfall von Komponentenhilfssystemen	1,6 E-02	9,9 E-10	0,50	3,7 E-12	3,5 E-09	1. DHRS 2. RSVs
TL	Leck zwischen Reaktorbecken und Sicherheits-behälter	1,0 E-07	2,9 E-11	0,014	2,9 E-13	1,1 E-10	1. Hilfssysteme 2. CIS
TF	Funktionales Versagen des Naturumlaufes	1,0 E-07	5,0 E-08	25,2	1,9 E-09	1,9 E-07	1. RCS 2. RTS
R	Reaktivitätsstörfälle	2,0 E-04	2,7 E-09	1,38	3,0 E-11	1,1 E-08	1. RTS 2. ESFAS
RS	Fehlausfahren der Steuerstäbe	2,0 E-04	2,7 E-09	1,38	3,0 E-11	1,1 E-08	1. RTS 2. ESFAS
L	Kühlmittelverluststörfälle	2,6 E-03	4,1 E-09	2,04	1,7 E-11	1,1 E-08	1. CIS 2. CVCS
LC	Leck der CVCS-Einspeiseleitung in den Sicher-heitsbehälter	1,4 E-04	2,6 E-10	0,132	6,0 E-13	6,8 E-10	1. CIS/CVCS 2. ECCS
LR	Leck der CVCS-Entnahmeleitung in das Reak-torgebäude	1,4 E-04	5,9 E-13	0,0003	2,7 E-15	2,1 E-12	1. RSVs 2. DHRS

Kürzel	Kernschaden nach/im …	Häufigkeiten (pro Jahr)					Hauptbeiträge der Systeme
		Auslösendes Ereignis	CDF, Mittelwert	Anteil [%]	CDF, 5% Perzentil	CDF, 95% Perzentil	
LE	Leck der CVCS-Einspeiseleitung in das Reaktorgebäude	2,8 E-04	1,4 E-11	0,007	6,0 E-14	5,0 E-11	1. CIS/CVCS 2. CFDS
LP	KMV in den Sicherheitsbehälter	2,0 E-03	3,3 E-09	1,65	8,4 E-12	9,6 E-09	1. CIS/CVCS 2. ECCS
LH	Dampferzeuger-Bypassleck	4,5 E-05	2,3 E-12	0,001	7,5 E-15	7,4 E-12	1. DHRS 2. RSVs
LV	Fehlerhafte Aktivierung des ECCS	1,1 E-05	1,8 E-11	0,009	4,7 E-14	5,5 E-11	1. CIS/CVCS/CES 2. ECCS
IB	Interner Brand	1,1E+00	4,9 E-08	24,4	7,0 E-10	1,6 E-07	1. ELVS/Notstrom 2. CIS
IB-TA	IB - Allgemeine Transiente	1,0E+00	9,1 E-10	0,46	1,1 E-11	2,7 E-09	1. DHRS 2. RSVs
IB-TN	IB - Ausfall der Versorgung	6,5 E-02	2,9 E-08	14,5	8,1 E-11	8,8 E-08	1. ELVS/Notstrom 2. ECCS
IB-TH	IB - Überspeisung durch das CVCS	6,0 E-02	4,8 E-09	2,39	1,5 E-11	1,5 E-08	1. DHRS 2. RSVs
IB-LV	IB - Fehlerhafte Aktivierung des ECCS	3,9 E-03	1,6 E-08	8,24	8,6 E-11	4,0 E-08	1. CIS/CVCS/CES 2. ECCS
IÜ	Interne Überflutung	5,1 E-02	1,3 E-09	0,63	5,2 E-12	4,1 E-09	1. DHRS 2. RSVs
IÜ-TA	IÜ - Allgemeine Transiente	3,2 E-02	2,3 E-11	0,012	3,0 E-14	5,8 E-11	1. RSVs 2. CFDS
IÜ-TV	IÜ - Ausfall von Komponentenhilfssystemen	1,9 E-02	1,2 E-09	0,59	4,4 E-12	4,1 E-09	1. RSVs 2. DHRS
NLB	Nichtleistungsbetrieb	2,3 E-07	8,3 E-08	41,9	1,5 E-08	2,4 E-07	1. Kran 2. Betriebsmannschaft
NF	Fall eines Moduls, POS3&5	1,1 E-07	8,5 E-08	42,5	1,5 E-08	2,4 E-07	-
NÜ	Überdruck im kalten RCS, POS2&6	1,2 E-07	1,2 E-10	0,062	9,0 E-13	4,4 E-10	1. ECCS 2. IAB
NLB-TF	Funktionales Versagen des Naturumlaufes	1,2 E-09	5,7 E-12	0,003	1,5 E-13	2,2 E-11	1. Kran 2. Betriebsmannschaft
	Gesamt	2,5E+00	2,0 E-07	100	4,2 E-08	5,3 E-07	1. RCS 2. Notstrom

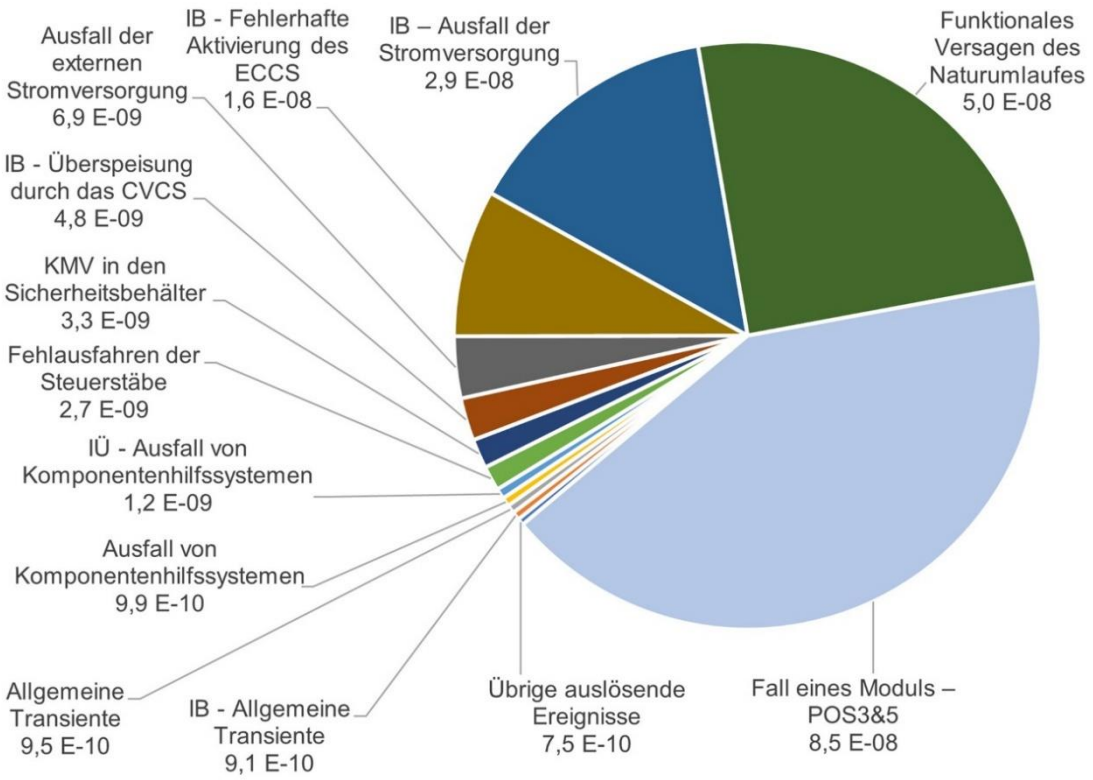


Abb. 10.1 Beiträge der einzelnen auslösenden Ereignisse zur Kernschadenshäufigkeit

Das Reaktorsicherheitskonzept erscheint aufgrund der Ergebnisse nicht sehr ausgewogen, allerdings können die wesentlichen Beiträge zur Kernschadenshäufigkeit noch weiter ausgearbeitet werden. Insbesondere die Eintrittshäufigkeit für das funktionale Versagen des Naturumlaufs im RCS, mögliche Maßnahmen nach einem Modulabsturz und die Kreditierung von Brandbekämpfungsmaßnahmen können das Ergebnis wesentlich modifizieren. Dadurch wäre optimal eine Verbesserung der Gesamtkernschadenshäufigkeit um maximal zwei Größenordnungen denkbar.

10.2 Ausfälle der Systemfunktionen

Die Wahrscheinlichkeiten für die Ausfälle der Systemfunktionen sind in Tab. 10.2 angegeben. Es ist zu beachten, dass sich Modifikation aufgrund von Hausevents ergeben können, z. B. liegt im Fall eines SBO keine Stromversorgung vor und diese Information kann beispielsweise die Ausfallwahrscheinlichkeit für eine RESA senken.

Tab. 10.2 Wahrscheinlichkeiten für die Ausfälle der Systemfunktionen

Systemfunktion	Ausfall, Mittelwert	Ausfall, 5%-Perzentil	Ausfall 95 -Perzentil	Wichtigste beitragende Komponenten
CFDS-HM1	8,4 E-03	4,8 E-03	1,6 E-02	1. Betriebsmannschaft 2. CFDS-CIV
CFDS-HM2	7,8 E-03	1,8 E-03	2,2 E-02	1. CFDS-CIV 2. CES-CIV
CVCS-HM1#1	1,2 E-02	9,7 E-04	3,5 E-02	1. CVCS-CIV 2. Deionat-Abschlussventile
CVCS-HM1#2	3,3 E-09	3,8 E-13	8,8 E-09	1. CVCS-CIV 2. CVCS-Aufbereitungspumpe
CVCS-HM1#3	2,6 E-03	2,0 E-04	9,5 E-03	1. CVCS-CIV 2. Boratpumpe
CVCS-HM2	2,0 E-08	7,8 E-10	6,9 E-08	1. Betriebsmannschaft 2. Deionat-Abschlussventile
CVCS-SF1	4,7 E-06	1,4 E-08	2,1 E-05	1. CVCS-CIV 2. ESFAS
CVCS-SF2	4,7 E-06	1,4 E-08	2,1 E-05	1. CVCS-CIV 2. ESFAS
DE-SF1	2,1 E-04	3,4 E-06	8,5 E-04	1. FWIV 2. MSIV
DHRS-SF1#1[45]	5,0 E-01	5,0 E-01	5,0 E-01	1. RSVs (sprechen an) 2. DHRS-Auslöseventile
DHRS-SF1#2	3,2 E-05	2,2 E-06	1,2 E-04	1. DHRS-Auslöseventile 2. MSIV
DHRS-SF1#3	5,2 E-04	2,9 E-05	1,8 E-03	1. DHRS-Auslöseventile 2. FWIV
ECCS-SF1#1	1,5 E-04	1,0 E-05	4,3 E-04	1. CES-CIV 2. RRV
ECCS-SF1#2	1,5 E-04	1,1 E-05	4,4 E-04	1. CES-CIV 2. RRV
ECCS-SF1#3	7,6 E-06	3,6 E-07	2,7 E-05	1. Magnetventile 2. RVVs
ELVS-HM1	3,1 E-03	2,6 E-04	1,1 E-02	1. Notstromdieselgeneratoren 2. Gasturbine
IAB-SF1	3,4 E-03	1,5 E-04	1,3 E-02	1. IAB 2. RVVs/RRVs

[45] Mit einer Wahrscheinlichkeit von 5,0 E-01 sprechen die RSVs im Unfallverlauf an, obwohl beide Redundanzen des DHRS auslegungsgemäß kühlen. Die nominelle Ausfallwahrscheinlichkeit ist daher nicht auf die Ausfallwahrscheinlichkeit des DHRS bezogen.

Systemfunktion	Ausfall, Mittelwert	Ausfall, 5%-Perzentil	Ausfall 95 -Perzentil	Wichtigste beitragende Komponenten
KRAN-HM1	4,4 E-03	1,6 E-03	1,1 E-02	1. Kran 2. Betriebsmannschaft
LTOP-SF1	1,0 E-03	5,9 E-05	3,7 E-03	1. RVVs 2. Magnetventile
RESA-SF1	1,4 E-05	1,1 E-06	4,5 E-05	1. ESFAS 2. Abschaltstäbe
RSV-SF1#1	7,3 E-04	2,5 E-06	2,9 E-03	1. RSV
RSV-SF1#2	7,1 E-05	3,3 E-06	2,4 E-04	1. RSV

Die Systemfunktionen KRAN-HM2, RCS-ER1, EHVS-HM1 und EHVS-HM1 werden durch ein einziges Basisereignis repräsentiert und sind deshalb nicht in Tab. 10.2 aufgeführt.

10.2.1 Systemausfälle

Für die Betrachtung der Systemausfälle werden die Ausfälle der wichtigsten Systemfunktionen bzgl. der einzelnen Systeme betrachtet. Die Systemausfallwahrscheinlichkeiten sind über den Mittelwert der Unsicherheitsanalyse in Tab. 10.3 dargestellt und in Abb. 10.2 grafisch aufbereitet.

Tab. 10.3 Systemausfälle

System	Ausfall Mittelwert
CVCS	1,19 E-02
CFDS	8,44 E-03
Kran	4,39 E-03
Notstrom	3,09 E-03
RSV	7,29 E-04
LTOP	1,01 E-03
DHRS (1v1 Redundanz)	5,16 E-04
CIS	2,06 E-04
ECCS	1,49 E-04
DHRS (beide Redundanzen)	3,24 E-05
RESA	1,38 E-05

Erwartungsgemäß ist die RESA sehr zuverlässig. Darüber hinaus zeigen sich auch die passiven Systeme DHRS und ECCS als besonders zuverlässig. Die betrieblichen Sys-

teme CVCS und das CFDS, die über Handmaßnahmen zugeschaltet werden können und auf den Betrieb von Pumpen angewiesen sind, sind deutlich weniger zuverlässig. Die Notstromversorgung geht hier als ein Schwachpunkt der Anlage hervor.

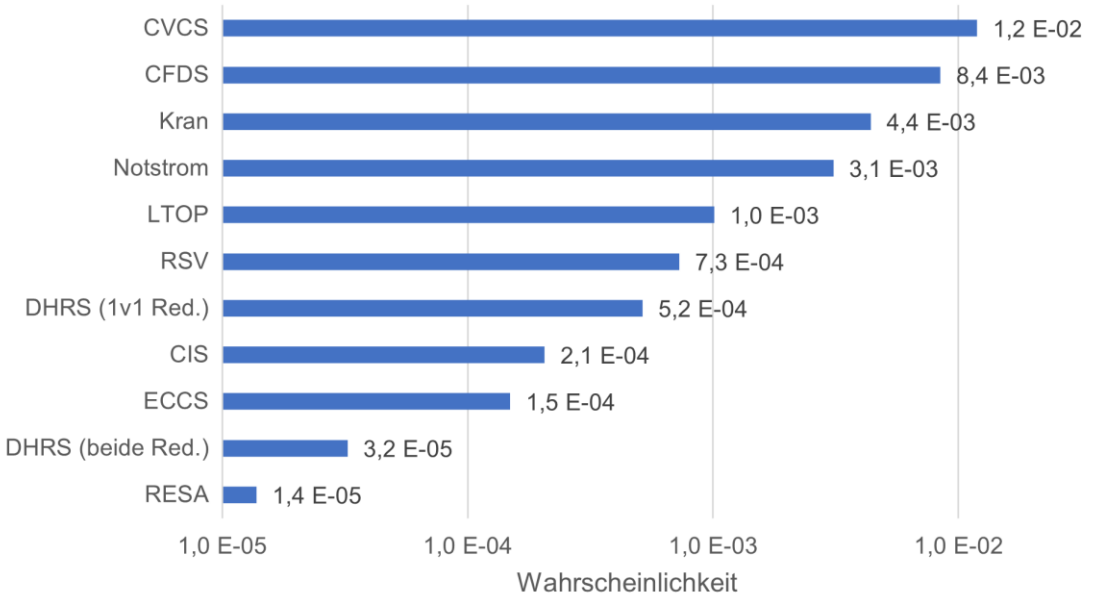


Abb. 10.2 Systemausfallwahrscheinlichkeiten

10.3 Häufigkeiten der einzelnen Kernschadenszustände

Entsprechend den Ausführungen in Kapitel 5 wurden insgesamt sieben Kernschadenszustände unterschieden. Die Ergebnisse sind in Abb. 10.3 dargestellt. Ein Kernschaden mit Schmelzerückhaltung ist der wahrscheinlichste Fall vor einem Kernschaden mit Leck am Sicherheitsbehälter, der im Wesentlichen durch den Modulabsturz gegeben ist. Die weiteren Kernschadensendzustände sind deutlich unwahrscheinlicher und liefern nur einen geringen Beitrag zum Gesamtergebnis.

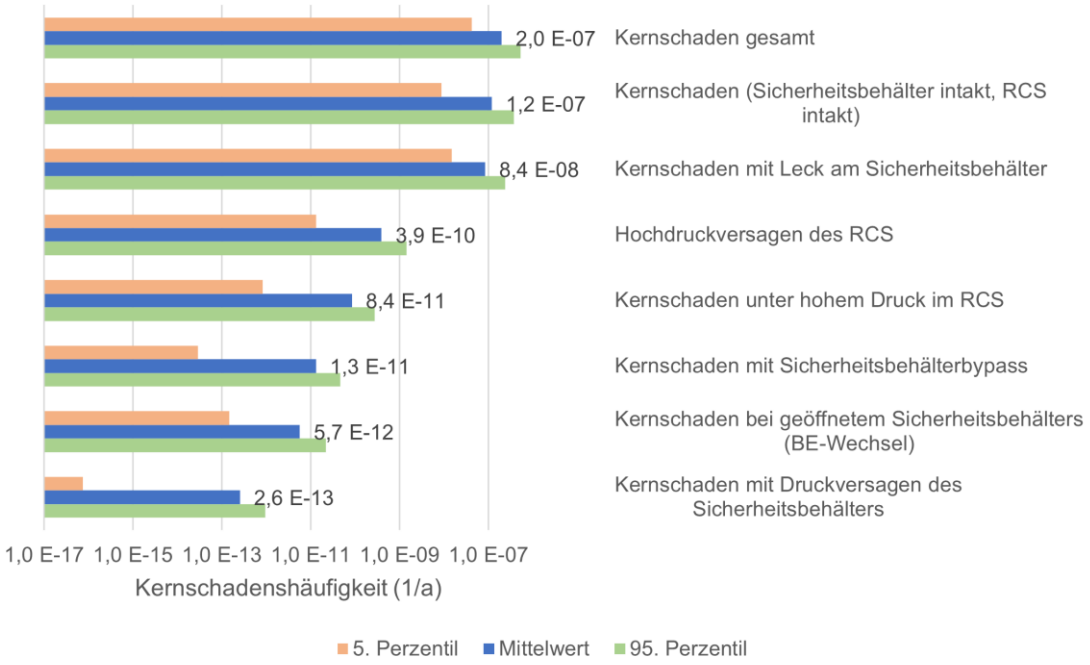


Abb. 10.3 Häufigkeiten mit Mittelwert, 5%- und 95%-Perzentilen der möglichen unterschiedlichen Kernschadenszustände

10.3.1 Wichtigste Minimalschnitte

Die wichtigsten Minimalschnitte können Tab. 10.4 entnommen werden. Sie sind einzeln nach den unterschiedlichen Kernschadensendzuständen unterteilt. Der größte Beitrag zur Gesamtkernschadenshäufigkeit liefert das funktionale Versagen des Naturumlaufs, dessen Ausfallhäufigkeit aufgrund bisher fehlender thermohydraulischer Analysen nur auf der Grundlage einer Experteneinschätzung festgelegt wurde und sollten zukünftig genauer quantifiziert werden soll.

Anhand der Umstände des Versagens lässt sich auch eine mögliche Stabilisierung des Naturumlaufs nach einer RESA besser quantifizieren. Ein weiterer wichtiger Beitrag zur Gesamtkernschadenshäufigkeit kommt aus einem möglichen Modulabsturz. Für diesen Fall sind keine Notfallmaßnahmen vorgesehen. Auch hier könnten Simulationen helfen, um die Konservativität zu reduzieren, z. B. durch eine Bestimmung der Zeitspanne bis zum Kernschaden oder der Wahrscheinlichkeit, dass der Sicherheitsbehälter beim Absturz Schaden nimmt. Ein zweiter Kran könnte möglicherweise das Modul wieder rechtzeitig aufstellen.

Tab. 10.4 Wesentliche Minimalschnitte für die einzelnen Kernschadenszustände

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	5. Ausfall/ Ereignis	Häufigkeit [1/a]
Kernschaden (Sicherheitsbehälter intakt, RCS intakt)					**9,1 E-08**
Funktionales Versagen des Naturumlaufs	Naturumlauf stabilisiert sich nach RESA nicht				5,0 E-08 (55 %)
Interner Brand: Ausfall der Stromversorgung	Gasturbine BV	GVA Dieselgeneratoren BV	GVA CES CIV		5,8 E-09 (6 %)
			GVA RRV IAB blockiert	RRV1/2 passive Öffnungsfunktion versagt	2,1 E-09 (2 %)
				GVA RRV passive Öffnungsfunktion	2,1 E-09 (2 %)
Fehlausfahren der Steuerstäbe	GVA Abschaltstäbe fallen nicht ein				1,3 E-09 (1 %)
Interner Brand: Überspeisung durch das CVCS	GVA CIV des CES	RSV sprechen im Unfallverlauf an	RSV1 schließt nicht wieder		1,1 E-09 (1 %)
Kernschaden mit Leck am Sicherheitsbehälter					**8,4 E-07**
Absturz eines Moduls in den Belade-bereich, POS5					3,1 E-08 (37 %)
Absturz eines Moduls in den Belade-bereich, POS3					2,5 E-08 (30 %)
Absturz eines Moduls in den Operations-bereich, POS5					1,6 E-08 (18 %)
Absturz eines Moduls in den Operations-bereich, POS3					1,3 E-08 (15 %)
Hochdruckversagen des RCS					**3,4 E-10**
Überdruck im kalten RCS	GVA RVVs IAB blockiert				1,2 E-10 (35 %)

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	5. Ausfall/ Ereignis	Häufigkeit [1/a]
Interner Brand: Überspeisung durch das CVCS	GVA RSV	GVA Abschaltstäbe fallen nicht ein			1,9 E-11 (5 %)
Interne Überflutung: Ausfall von Komponentenhilfssystemen	GVA RSV	GVA DHRS-Auslöseventile			1,2 E-11 (4 %)
		GVA MSIV und Backup-Ventile			1,2 E-11 (4 %)
Ausfall von Komponentenhilfssystemen	GVA RSV	GVA DHRS-Auslöseventile			1,0 E-11 (3 %)
		GVA MSIV und Backup-Ventile			1,0 E-11 (3 %)
Kernschaden unter hohem Druck im RCS					**5,7 E-11**
Interner Brand: Überspeisung durch das CVCS	GVA CIV CVCS-Einspeiseleitung	GVA ECCS-Magnetventile			1,6 E-11 (28 %)
		GVA RVVs IAB blockiert	GVA RRV IAB blockiert		5,8 E-12 (10 %)
	GVA ECCS-Magnetventile	GVA MSIV und Backup-Ventile			4,3 E-12 (8 %)
		GVA DHRS-Auslöseventile			4,3 E-12 (8 %)
		GVA Abschaltstäbe			2,1 E-12 (4 %)
	GVA RVVs IAB blockiert	GVA RRV IAB blockiert	GVA MSIV und Backup-Ventile		1,6 E-12 (3 %)
			GVA DHRS-Auslöseventile		1,6 E-12 (3 %)
Kernschaden mit Sicherheitsbehälter-Bypass					**1,3 E-11**
Leck CVCS-Einspeise-leitung in das Reaktorgebäude	CVCS-Rückschlagventil	GVA CVCS-Einspeiseleitung CIV	Betriebsmannschaft Sicherheitsbehälter-Fluten		5,8 E-12 (43 %)
			CFDS CIV1 öffnet nicht wieder		1,7 E-12 (13 %)
			CFDS CIV2 öffnet nicht wieder		1,7 E-12 (13 %)

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	5. Ausfall/ Ereignis	Häufigkeit [1/a]
			CFDS CIV Heizelement		1,4 E-12 (11 %)
			GVA CFDS-Pumpen		1,3 E-12 (10 %)
Kernschaden bei geöffnetem Sicherheitsbehälter (Brennelementwechsel)					**5,9 E-12**
Ausfall des Naturumlaufs im Laufe eines Brennelement-wechsels	Kran BV				2,4 E-12 (41 %)
	Betriebsmann-schaft Kran				1,7 E-12 (29 %)
	Kran Startver-sagen				1,2 E-12 (20 %)
	Kran Brenn-elemententla-dung BV	Naturumlauf stabilisiert sich nicht			6,0 E-13 (10 %)
Kernschaden mit Druckversagen des Sicherheitsbehälters					**1,2 E-13**
Interner Brand: Überspeisung durch das CVCS	GVA CVCS-Einspeise-leitung CIV	GVA CIV des CES	Betriebs-mannschaft verhindert Überspeisung nicht		3,5 E-14 (30 %)
			GVA Betriebs-mannschaft		1,4 E-14 (12 %)
		GVA RRV blockiert	Betriebs-mannschaft verhindert Überspeisung nicht	RRV1/2 passive Öff-nungs-funk-tion versagt	1,3 E-14 (11 %)
				GVA RRV passive Öff-nungs-funk-tion	1,3 E-14 (11 %)

10.3.2 Vergleich mit Minimalschnitten von NuScale

Viele der oben genannten Minimalschnitte, die in einen Kernschaden führen, sind in den Ergebnissen der PSA von NuScale in /NUS 20/ nicht aufgeführt. Dafür konnten mehrere Gründe genauer untersucht werden. So fehlen in der NuScale-PSA beispielsweise Minimalschnitte, in denen ECCS-Ventile aufgrund einer fehlerhaften Blockade durch den IAB nicht öffnen. Die von NuScale veröffentlichten Minimalschnitte /NUS 20/ können weitestgehend reproduziert werden (siehe dazu Tab. 10.5). Teilweise sind die Kernschadenhäufigkeiten bei NuScale sogar etwas höher.

Im Zusammenhang mit Ausfällen von Handmaßnahmen, ergeben sich in der NuScale-PSA teilweise deutlich höhere Kernschadenhäufigkeiten. Die Modellierung der Fehler der Betriebsmannschaft sind zukünftig noch weiter zu überarbeiten. Insbesondere gab es hier Schwierigkeiten, die Zeitbudgets der Handmaßnahmen zu schätzen, welche mit Hilfe von Unfallanalysen genauer bestimmt werden können.

Tab. 10.5 Vergleich der Minimalschnitte im Leistungsbetrieb aus der NuScale-PSA

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	Analyse	Häufigkeit [1/a}
Leistungsbetrieb				**NuScale**	**3,0 E-10**
				GRS	**6,05 E-08**
EDSS-Ausfall aller Busse	GVA RRV			NuScale	2,56 E-11 (9,4 %)
				GRS	3,20 E-12 (0,01 %)
KMV in den Sicherheits-behälter	GVA RRV	Ausfall Hand-maßnahmen		NuScale	2,02 E-11 (7,4 %)
				GRS	5,04 E-13
Ausfall von Komponen-tenhilfssyste-men	GVA RRV	RSV schließt nicht wieder	RSV spricht an	NuScale	1,48 E-11 (5,4 %)
				GRS	1,47 E-11 (0,02 %)
EDSS-Ausfall aller Busse	GVA RVVs			NuScale	1,26 E-11 (4,6 %)
				GRS	1,57 E-12
Ausfall von Komponen-tenhilfssyste-men	GVA DHRS-Auslöse-ventile	GVA RSV		NuScale	1,03 E-11 (3,8 %)
				GRS	1,03 E-11 (0,02 %)
KMV in den Sicherheits-behälter	GVA RVVs	Ausfall Hand-maßnahme		NuScale	9,94 E-12 (3,7 %)
				GRS	2,48 E-13
Ausfall von Komponen-tenhilfssyste-men	GVA RVVs	RSV spricht an	RSV schließt nicht wieder	NuScale	7,28 E-12 (2,7 %)
				GRS	7,25 E-12
Leck der CVCS-Ein-speiseleitung in das Reak-torgebäude	GVA CIV der CVCS-Ein-speiseleitung	Ausfall CVCS-Rückschlag-ventil	Ausfall Hand-maßnahme	NuScale	5,76 E-12 (2,1 %)
				GRS	5,75 E-12

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	Analyse	Häufigkeit [1/a}
Ausfall von Komponen-tenhilfssyste-men	GVA RSV	Ausfall RESA		NuScale	4,90 E-12 (1,8 %)
				GRS	4,99 E-12
Allgemeine Transiente	GVA RRV	Ausfall Hand-maßnahme	RSV spricht an RSV & schließt nicht wieder	NuScale	4,83 E-12 (1,8 %)
				GRS	1,20 E-13
KMV in den Sicherheits-behälter	GVA RRV	Ausfall CVCS-Drei-wegeventil		NuScale	4,79 E-12 (1,8 %)
				GRS	6,85 E-13
KMV in den Sicherheits-behälter	GVA RRV	Ausfall Deionatab-schlussventil		NuScale	4,79 E-12 (1,8 %)
				GRS	1,21 E-11 (0,02 %)
Interner Brand				**NuScale**	**9,7 E-10**
				GRS	**2,99 E-08**
Überspeisung durch das CVCS	GVA RRV	RSV spricht an	RSV schließt nicht wieder	NuScale	5,53 E-11 (6,7 %)
				GRS	5,52 E-11 (0,2 %)
Fehlerhafte Aktivierung des ECCS	GVA RRV	Ausfall Hand-maßnahme CVCS		NuScale	7,60 E-11 (9,2 %)
				GRS	1,93 E-12
Allgemeine Transiente	GVA RSV			NuScale	2,81 E-11 (3,4 %)
				GRS	Betriebsmann-schaft kann Kernschaden verhindern
Überspeisung durch das CVCS	GVA RVVs	RSV spricht an	RSV schließt nicht wieder	NuScale	2,73 E-11 (3,3 %)
				GRS	2,72 E-11 (0,1 %)
Fehlerhafte Aktivierung des ECCS	GVA RRV			NuScale	2,52 E-11 (3,1 %)
				GRS	Möglichkeit zur CVCS-Einspeisung modelliert
Fehlerhafte Aktivierung	GVA RVVs	Ausfall Hand-maßnahme		NuScale	3,76 E-11 (4,6 %)

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	Analyse	Häufigkeit [1/a}
des ECCS		CVCS		GRS	9,51 E-13
Überspeisung durch das CVCS	GVA RSV	Ausfall RESA		NuScale	1,84 E-11 (2,2 %)
				GRS	1,87 E-11 (0,1 %)
Allgemeine Transiente	GVA RSV	Ausfall ESFAS I		NuScale	1,77 E-11 (2,2 %)
				GRS	Nicht berücksichtigt
Allgemeine Transiente	GVA RSV	GVA MSIV in einem Dampf-- erzeuger		NuScale	1,44 E-11 (1,8 %)
				GRS	Zusätzlich Ausfall Handmaßnahme Sicherheitsbehälter-Fluten berücksichtigt
Allgemeine Transiente	GVA RSV	GVA FWIV in einem Dampf-erzeuger		NuScale	1,44 E-11 (1,8 %)
				GRS	Zusätzlich Ausfall Handmaßnahme Sicherheitsbehälter-Fluten berücksichtigt
Fehlerhafte Aktivierung des ECCS	GVA RVVs			NuScale	1,24 E-11 (1,5 %)
				GRS	Möglichkeit zur CVCS-Einspeisung modelliert
Interne Überflutung				**NuScale**	**6,1 E-11**
				GRS	**9,05 E-10**
Ausfall von Komponen-tenhilfssyste-men	GVA RRV	RSV spricht an	RSV schließt nicht wieder	NuScale	1,78 E-11 (29,8 %)
				GRS	1,75 E-11 (2 %)
Ausfall von Komponen-tenhilfssyste-men	GVA RSVs	GVA DHRS-Auslöse-ven-tile		NuScale	1,24 E-11 (20,8 %)
				GRS	1,23 E-11 (1 %)
Ausfall von Komponen-tenhilfssyste-men	GVA RVVs	RSV spricht an	RSV schließt nicht wieder	NuScale	8,78 E-12 (14,7 %)
				GRS	8,61 E-12 (1 %)

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	Analyse	Häufigkeit [1/a}
Ausfall von Komponen-tenhilfssyste-men	GVA RSVs	Ausfall RESA		NuScale	5,91 E-12 (9,9 %)
				GRS	5,93 E-12 (1 %)
Ausfall von Komponen-tenhilfssyste-men	GVA RSVs	Ausfall RESA		NuScale	2,94 E-12 (4,9 %)
				GRS	2,90 E-12 (0,3 %)
Ausfall von Komponen-tenhilfssyste-men	GVA RSVs	Ausfall RESA		NuScale	2,94 E-12 (4,9 %)
				GRS	2,90 E-12 (0,3 %)
Ausfall von Komponen-tenhilfssyste-men	GVA RSV	GVA DHRS Natur-kon-vektion		NuScale	2,32 E-12 (3,9 %)
				GRS	2,29 E-12 (0,3 %)
Ausfall von Komponen-tenhilfssyste-men	Passive Öff-nungsfunktion RRV1 und RRV2 versagt	GVA RRV Magnetventile	RSV spricht an RSV & schließt nicht wieder	NuScale	1,15 E-12 (1,9 %)
				GRS	3,62 E-13 (0,04 %)
Nichtleistungsbetrieb				**NuScale**	**8,80 E-08**
				GRS	**1,12 E-07**
Fall eines Moduls in den Bereich BE-Wechsel: POS3				NuScale	3,13 E-08 (35,8 %)
				GRS	3,10 E-08 (28 %)
Fall eines Moduls in den Bereich BE-Wechsel: POS5				NuScale	3,13 E-08 (35,8 %)
				GRS	3,10 E-08 (28 %)
Fall eines Moduls im Reaktorbe-cken: POS3				NuScale	1,25 E-08 (14,2 %)
				GRS	2,5 E-08 (22 %)
Fall eines Moduls im Reaktorbe-cken: POS5				NuScale	1,25 E-08 (14,2 %)
				GRS	2,5 E-08 (22 %)

Die entsprechenden Minimalschnitte liefern nur einen geringen Beitrag zum Ergebnis der PSA der GRS. Dies liegt hauptsächlich daran, dass verschiedene andere Versagensmechanismen des ECCS in der PSA der GRS als deutlich wahrscheinlicher ange-

nommen werden. Die Wahrscheinlichkeiten für GVA der RRV sind weniger relevant für das Ergebnis der PSA der GRS.

10.4 Besonders relevante Parameterwerte

Die 25 wichtigsten Parameter für die Kernschadenshäufigkeit sind in Tab. 10.6 nach dem anteiligen Beitrag (fractional contribution) sortiert, beginnend mit dem relevantesten Parameter. Darunter fallen einige Eintrittshäufigkeiten für die auslösenden Ereignisse, die Missionszeit und Test- und Wartungsintervalle. Darüber hinaus fällt die passive Öffnungsfunktion der ECCS-Ventile auf, diese Ausfallwahrscheinlichkeit beruht auf einer Experteneinschätzung. Die Parameter zum Ausfall der Notstromversorgung sind auch für das Ergebnis von gewisser Relevanz. Die Wahrscheinlichkeit, dass ein RSV im Betrieb des DHRS anspricht, ist mit 0,5 abgeschätzt, dieser Wert könnte mit Hilfe von Unsicherheitsanalysen optimiert werden.

Tab. 10.6 Parameter mit hoher Relevanz für die Kernschadenshäufigkeit

Parameter	Parametermittelwert
Häufigkeit eines Funktionalen Versagens des RCS	1,00 E-07 1/a
Naturumlauf stabilisiert sich nach Kernabschaltung nicht	0,5
Häufigkeit für den Fall eines Moduls im Beladebereich, POS5	3,10 E-08 1/a
Missionszeit	72 h
Häufigkeit für den Fall eines Moduls im Beladebereich, POS3	2,50 E-08 1/a
Gasturbine BV	2,45 E-03 1/h
Test- und Wartungsintervall: Abfahren der Anlage	8,76 E+03 h
Test- und Wartungsintervall: 3 Monate	2,19 E+03 h
Interner Brand mit Ausfall der Stromversorgung	6,5 E-02 1/a
GVA zweier aktiver Ventile	4,69 E-08 1/h
Häufigkeit für den Fall eines Moduls im Operationsbereich, POS5	1,55 E-08 1/a
GVA Dieselgeneratoren BV	1,50 E-04 1/h
GVA 2 IAB-Blockierventile	4,35 E-07 1/h
Häufigkeit für den Fall eines Moduls im Operationsbereich, POS3	1,25 E-08 1/a
GVA passives Öffnen aller ECCS-Ventile	1,00 E-02

Parameter	Parametermittelwert
Passives Öffnen eines ECCS-Ventils	1,00 E-01
Interner Brand mit fehlerhafter Aktivierung des ECCS	7,70 E-03 1/a
Dieselgenerator BV	8,72 E-04 1/h
Wiederöffnen eines geschlossenen Ventils	1,10 E-06 1/h
Test- und Wartungsintervall: 40 Monate	2,92 E+04 h
Interner Auslöser eines nicht-wiederherstellbaren Ausfall der Versorgung	1,51 E-02 1/a
RSV Wiederverschluss nach Öffnung	5,01 E-08 1/h
RSV spricht im Betrieb des DHRS an	0,5
GVA 3 IAB-Blockierventile	2,17 E-07 1/h
Interner Brand mit Ausfall der Komponentenhilfssysteme	6,00 E-02 1/a

10.5 Diskussion der PSA-Ergebnisse

Die ersten Ergebnisse der eigenen SMR-PSA sind vielversprechend und die Unterschiede zu den Ergebnissen von NuScale konnten überwiegend identifiziert werden. Das Reaktorsicherheitskonzept erscheint nach bisherigen Ergebnissen noch nicht genügend ausgewogen. Dies könnte sich ändern, wenn das Modell bzgl. der wesentlichen Beiträge zur Kernschadenshäufigkeit weiter ausgearbeitet wird.

Die drei wesentlichen Beiträge zur Kernschadenhäufigkeit sind in der PSA der Stufe 1 der GRS aktuell gegeben durch die Eintrittshäufigkeit für das funktionale Versagen des Naturumlaufs im RCS, für den Modulabsturz ohne Durchführung weiterer Notfallmaßnahmen und einen anlageninternen Brand als auslösendes Ereignis. Die genauere Bestimmung der Eintrittshäufigkeiten für das funktionale Versagen, die Evaluierung möglicher Notfallmaßnahmen nach einem Modulabsturz und die Kreditierung von Brandbekämpfungsmaßnahmen könnten die Kernschadenhäufigkeiten wesentlich verändern. Im günstigsten Fall wäre durch diese Maßnahme eine Verbesserung der Gesamtkernschadenshäufigkeit um maximal zwei Größenordnungen denkbar, dies ist dennoch eine Größenordnung höher als das Ergebnis von NuScale.

11 PSA für mehrere SMR-Module

Das Anlagenkonzept von NuScale sieht Anlagen mit mehreren Reaktoren vor, und zwar mit vier, sechs oder sogar zwölf Modulen. Auch für SMR-Anlagen gibt es Kosten-Nutzen-Abschätzungen, die aufzeigen, dass der Einsatz mehrerer Reaktorblöcke bzw. -module an einem Standort vorteilhaft ist, siehe u. a. /BOA 14/. Potenziale für Kosteneinsparungen liegen dabei u. a. bei der gemeinsamen Nutzung von Systemen und Infrastruktur (z. B. Umspannwerke). Das Konzept von NuScale setzt dabei auf baugleiche Reaktoren (mit einer erhöhten Gefahr für Ausfälle aus gemeinsamer Ursache) und eine Betriebsmannschaft, die für alle Reaktoren gleichzeitig zuständig ist (mit einer erhöhten Gefahr einer Überforderung des Personals bei Betriebsstörungen, Stör- oder Unfällen in mehreren Modulen).

Das veränderte Risikopotenzial der Gesamtanlage im Vergleich zu einer (hypothetischen) Anlage mit nur einem Reaktorblock kann mit Hilfe einer Mehrblock-PSA (MUPSA) quantifiziert werden. Die Durchführung einer Mehrblock-PSA orientiert sich an den Vorgaben der IAEA, /IAE 21//, mit den Entwicklungsschritten in Abb. 11.1.

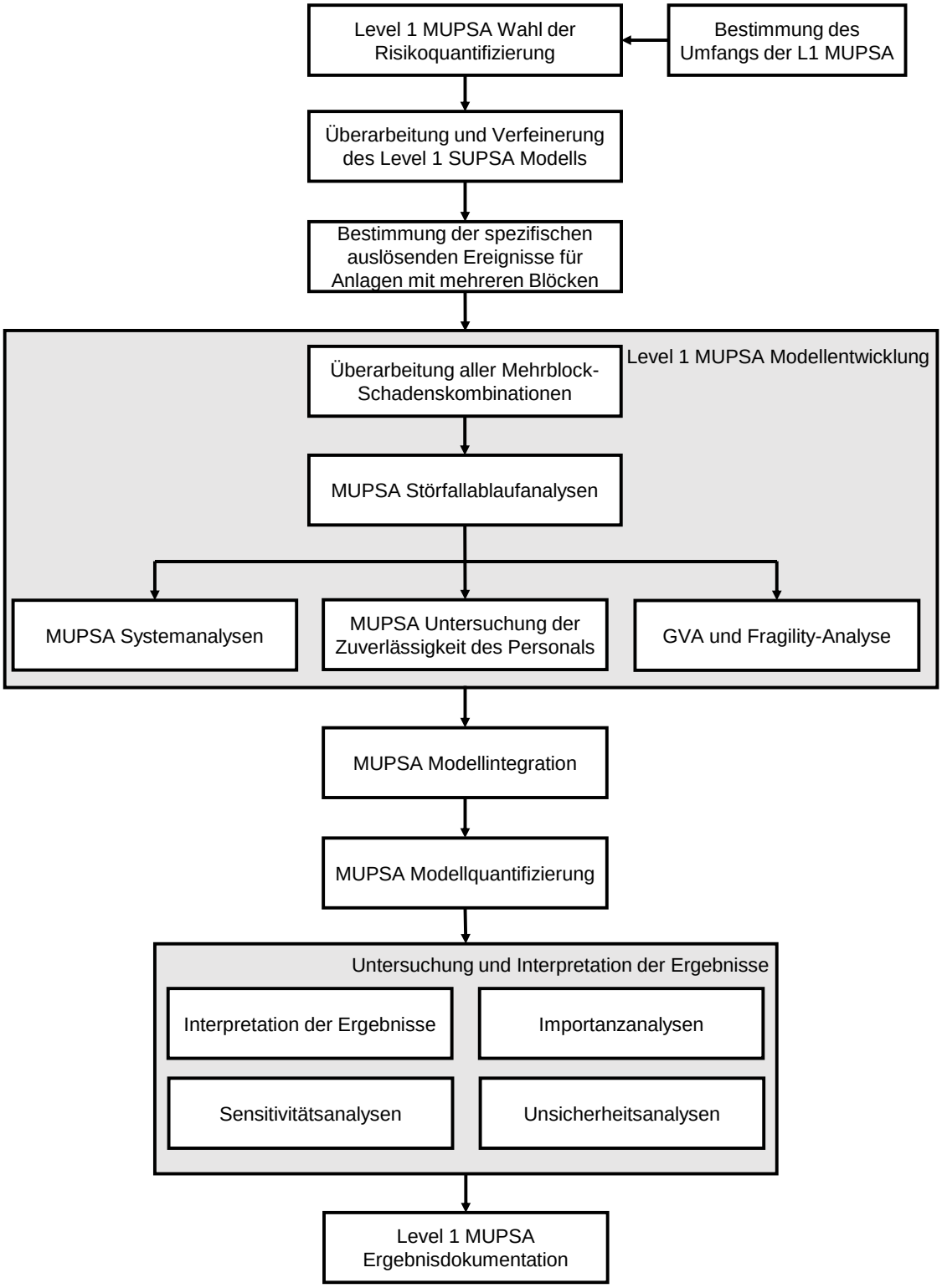


Abb. 11.1 Entwicklungsschritte bei der Erstellung der MUPSA, nach /IAE 21/

Im Folgenden wird eine entsprechend dem Leitfaden der IAEA durchgeführte Mehrblock-PSA für einen SMR vorgestellt.

11.1 Vereinfachung des Single-Unit PSA-Datensatzes als Grundlage für eine Multi-Unit PSA

Die Nutzung der vollständigen PSA der Stufe 1 für einen einzelnen Reaktor (SUPSA) als Grundlage für die Mehrblock-PSA (MUPSA) kann vergleichsweise aufwändig sein und zu einem komplizierten und unübersichtlichen Anlagenmodell führen. Dies liegt daran, dass eine extrem hohe Anzahl an möglichen Schadenskombinationen in den Modulen auftreten kann. Eine durchgeführte Maßnahme kann in einem Modul erfolgreich sein oder fehlschlagen. In zwei Modulen gibt es vier Möglichkeiten (erfolgreich in beiden, erfolgreich in Modul 1, erfolgreich in Modul 2, in keinem Modul erfolgreich), in zwölf Modulen wären es schon $12^2 = 144$ Möglichkeiten. Daher ist der erste Schritt zur Durchführung einer MUPSA eine deutliche, sinnvolle Vereinfachung der SUPSA.

11.1.1 Bestimmung des Umfangs der Mehrblock-PSA

In die MUPSA sollen alle anlageninternen Ereignisse sowie die übergreifenden Einwirkungen von innen ‘Brand‘ und ‘Überflutung‘, die mehrere Reaktormodule gleichermaßen betreffen können, eingeschlossen werden. Ereignisse, die während der Vorbereitungen oder der Durchführung eines Brennelementwechsels eines Moduls auftreten, sollen nicht betrachtet werden, da sich maximal ein einzelnes Modul in einem entsprechenden Wechselprozess befindet. Insbesondere das Szenario eines Stromausfalls stellt für das Modul im Zuge eines Brennelementwechsels keine besondere Herausforderung dar (anders als z. B. bei einem typischen DWR, wo dies ein erhöhtes Risiko darstellen kann).

11.1.2 Wahl der Risikoquantifizierung für eine Multi-Unit PSA der Stufe 1

In der Wahl der Risikoquantifizierung ist zwischen der alleinigen Untersuchung der Kernschadenshäufigkeiten mehrerer Module und der Untersuchung aller radioaktiven Quellen am Standort zu unterscheiden. Radioaktive Quellen in und außerhalb der NuScale-Anlagen sind neben den zwölf Modulen u. a. die abgebrannten Brennelemente im Brennelementlagerbecken, welches an das Reaktorbecken angeschlossen ist. Ein Leerlaufen des gesamten Beckens wird als auslösendes Ereignis nicht unterstellt[13].

Neben den abgebrannten Brennelementen im Brennelementlagerbecken ergeben sich mit dem nuklearen Abfalllager für schwach- und mittelradioaktive Abfälle sowie einem möglichen Standortzwischenlager für hochradioaktive Abfälle weitere potenzielle Radionuklidquellen. Das radioaktive Inventar und die daraus möglichen Freisetzungen aus

dem Abfalllager sind eher gering und bei einer Risikoquantifizierung vernachlässigbar. Das wesentlich höhere radioaktive Inventar in einem Standortzwischenlager, insbesondere für bestrahlte Brennelemente, wird typischerweise in besonders gesicherten Behältern aufbewahrt. Die betrachteten auslösenden Ereignisse bergen kein Risiko für das Standortzwischenlager /OBE 24a/. Die Einbeziehung von Abfalllager und Standortzwischenlager in die Risikoquantifizierung ist zudem für die Anfangsphase des Betriebs der Anlage irrelevant, da diese Einrichtungen erst im Laufe des Betriebs nach und nach gefüllt werden.

Die Risikoquantifizierung im Rahmen der Multi-Unit PSA bezieht sich somit ausschließlich auf die Kernschadenshäufigkeiten der zwölf Reaktormodule. Mögliche Endzustände der PSA der Stufe 1 sind einerseits entweder die Single-Unit CDF (SUCDF), die Multi-Unit CDF (MUCDF) oder die Standort-Kernschadenshäufigkeit (Englisch Site-Level CDF, SCDF), die sowohl die SUCDF als auch die MUCDF miteinschließt. Die SCDF quantifiziert allerdings die Anzahl der von einem Kernschaden betroffenen Module nicht näher.

Zunächst soll die Bestimmung der SCDF für die Anlagenrisikoquantifizierung ausreichen und in der MUPSA quantifiziert werden. Eine explizite Bestimmung der SUCDF und MUCDF wäre allerdings, u. a. als Grundlage für eine PSA der Stufe 2 von Interesse, da falls die MUCDF (oder das Verhältnis MUCDF/SUCDF) besonders hoch sein sollte, eine spezifische PSA der Stufe2 für mehrere Module relevant sein könnte. Außerdem ist für eine vollständige Standort-PSA noch die Häufigkeit von Schäden an den gelagerten Brennelementen (fuel damage frequency, FDF) zu bestimmen, die für das Risikomaß des Standortes berücksichtigt werden muss /HAG 21/.

11.1.3 Überarbeitung und Verfeinerung des Single-Unit PSA-Modells der Stufe 1

Die Überarbeitung und Verfeinerung des Single-Unit PSA Modells der Stufe 1 untergliedert sich wie folgt:

1. Modellvereinfachungen in der Single-Unit PSA,
2. Überarbeitungen der Systemverfügbarkeiten im Hinblick auf Ereignisse in mehreren Modulen,

3. Modellverfeinerungen und Erstellung der Single-Unit PSA separat für jeden Reaktorblock bzw. jedes Modul.

Modellvereinfachungen in der Single-Unit PSA

Für die Integration der SUPSA mehrerer Module müssen Komplexität und Umfang der PSA für die einzelnen Reaktoren wesentlich reduziert werden, ohne dabei die für das Ergebnis relevanten Teile zu entfernen. Die Arbeiten werden dadurch erschwert, dass die modulübergreifenden Abhängigkeiten mitberücksichtigt werden müssen. In der Multi-Unit PSA können eingeschränkte Systemverfügbarkeiten oder GVA das Ergebnis beeinflussen, die im Einzelmodul keinen größeren Einfluss auf das Ergebnis zeigten.

Die Betriebsmannschaft ist für alle Module gleichzeitig zuständig. Für mehrere gleichzeitig betroffene Module sind höhere Ausfallraten für die Durchführung zeitkritischer Handmaßnahmen zu erwarten. Darüber hinaus besteht je nach Ergonomie und Anordnung der Schalttafeln ein erhöhtes Risiko für Verwechslungen bzgl. der Steuerung der einzelnen Module untereinander. Systeme, die neben der regulären automatischen Auslösung auch eine manuelle Auslösung erlauben, sind die Sicherheitsbehälterabsperrung, der Dampferzeugerabschluss, das DHRS und das ECCS. Die zugehörigen Basisereignisse, zeigen in den Ergebnissen der SUPSA nur geringe Importanzen (Fussel-Vesely-Importanzen kleiner als 2,0 E-07) mit Ausnahme der manuellen Auslösung des DHRS (FV = 2,1 E-04). Alle Handmaßnahmen (Einzel- und Mehrfachmaßahmen) sollen in dem vereinfachten SUPSA-Modell nicht berücksichtigt werden bzw. können in einem späteren Entwicklungsschritt durch ein modulübergreifendes Modell ersetzt werden, Details dazu siehe Abschnitt 9.3.

Eine Neuberechnung der SUPSA zeigt keinen wesentlichen Beitrag der Anpassungen auf die Ergebnisse und die Komplexität des Modells konnte in diesem Schritt wesentlich reduziert werden.

Weitere Abhängigkeiten zwischen den Fehlerbäumen ergeben sich für die GVA aufgrund von fehlerhaften Wartungsarbeiten. Eine geringe Importanz für das SUPSA-Ergebnis haben die fehlerhaften Wartungsarbeiten am CFDS und CVCS (FV ≤ 2,0 E-07).

Das Modell wird deaktiviert und das SUPSA-Ergebnisse konnte mit hoher Genauigkeit reproduziert werden.

Überarbeitungen der Systemverfügbarkeiten im Hinblick auf Ereignisse in mehreren Modulen

Folgende Systeme sind für mehrere Module nicht gleichzeitig vollständig verfügbar und müssen in der MUPSA entsprechend modelliert werden:

- Systeme mit eingeschränkter Verfügbarkeit:
  - CFDS (ein System für sechs Module),
- Systeme, die für mehrere Module gemeinsam ausfallen:
  - Notstromdieselaggregate (zwei Dieselgeneratoren für alle Module),
  - Gasturbine (ein System für alle Module),
  - Not- und Nachwärmesenke (Reaktorbecken, ein System für alle Module),
  - EMVS (vier Stränge für sechs Module),
  - EHVS (vier Stränge für sechs Module),
  - CFDS (ein System für sechs Module),
  - Deionatsystem (ein System für alle Module),
  - Boreinspeisesystem (ein System für alle Module),
  - System zur Versorgung mit komprimierter Luft (ein System für alle Module),
  - Zwischenkühlsysteme (ein System für sechs Module),
- Modulspezifische Systeme, die von gemeinsam genutzten Systemen wesentlich abhängig sind:
  - ELVS (abhängig von EMVS und Notstromdieselaggregaten),
  - CVCS (abhängig von ELVS, Deionatsystem, Boreinspeisesystem, komprimierter Luft und Zwischenkühlsystemen),
  - EDSS (abhängig von ELVS, allerdings abgesichert durch zugehörige Batterien).

Die aufgeführten Systeme (mit Ausnahme des EDSS) sollen in einer vereinfachten konservativen Version des SUPSA-Modells nicht berücksichtigt werden. Dieses konservative Modell dient im Folgenden als Grundlage für die Auswahl der auslösenden Ereignisse der MUPSA. Wenn selbst unter dieser konservativen Annahme die Kernschadenshäufigkeiten für ein auslösendes Ereignis unter einem festzulegenden Schwellenwert

liegen, dann sind die auslösenden Ereignisse für die MUPSA nicht relevant. Diese Überlegungen führen zu einer wesentlichen Vereinfachung der MUPSA, siehe Abschnitt 11.1.4.

Modellverfeinerungen und Erstellung der Single-Unit PSA separat für jeden Reaktorblock bzw. jedes Modul

Einige der auslösenden Ereignisse in der Single-Unit PSA sind spezifisch an ein Modul gekoppelt und treten nicht in mehreren Modulen gleichzeitig auf oder nur mit einer sehr geringen bzw. vernachlässigbaren Eintrittshäufigkeit. (Eine Bestimmung dieser auslösenden Ereignisse erfolgt in Abschnitt 11.1.4). Dabei handelt es sich insbesondere um die meisten Unfälle nach einem Kühlmittelverlust sowie Unfälle im Nichtleistungsbetrieb (da der Brennelementwechsel in den Modulen nicht gleichzeitig erfolgt). Die Wahl der Risikoquantifizierung (SCDF, Standortkernschadenshäufigkeit) bedingt, dass die Ereignisablaufanalysen nach einem auslösenden Ereignis, das ausschließlich ein Modul betrifft, in der Multi-Unit PSA mit ausgewertet werden müssen. Eine Vereinfachung dieses Teils der PSA ist nicht notwendig, weil die Komplexität sich in der MUPSA nicht weiter erhöht. Der methodische Ansatz ist, in der MUPSA nicht zwölf 2 gleiche SUPSA zu integrieren, sondern die Ereignisabläufe, die nur ein einzelnes Modul betreffen, mit einer 12-fach höheren Eintrittshäufigkeit zu belegen – die Kernschadenshäufigkeiten sind aufgrund der angenommenen (theoretischen) Äquivalenz der Module in allen Modulen gleich.

Sind durch das auslösende Ereignis mehrere Module betroffen, z. B. bei einem Ausfall der externen Stromversorgung, so wird auch hier die Äquivalenz der Module für die Analysen berücksichtigt. Das heißt, im Modell sollen die Module nicht nach ihrer Position in der Anlage unterschieden werden, sondern nach den Systemausfällen, von denen die einzelnen Module im Unfallablauf betroffen sind.

Es wurden zunächst die Fehlerbäume des SUPSA-Modells für vier der zwölf Module vervielfältigt. Die Wahrscheinlichkeiten der Systemausfälle in einem oder mehreren Modulen muss in der MUPSA immer entsprechend den möglichen Realisierungen in der Anlage multipliziert werden. Fällt zum Beispiel die externe Versorgung in allen Modulen aus und tritt der Fall ein, dass die RESA daraufhin in zwei Modulen ausfällt, muss mit einem Faktor $\binom{12}{2} = 66$ multipliziert werden, da entsprechend viele mögliche Realisierungen für zwei betroffene Module in der Anlage vorliegen.

Die Idee sich auf vier von Systemausfällen betroffene Module zu beschränken hat mehrere Gründe. Einerseits erreicht die Betriebsmannschaft bei mehrfachen Systemausfällen in mehreren Modulen irgendwann ihre Leistungsgrenze und könnte durch zusätzliche Fehler einen Kernschaden wahrscheinlicher machen. andererseits wird die Erstellung und die Überarbeitung der MUPSA mit der Anzahl der implementierten Module zu aufwändig – die Information, ob die Durchführung einer MUPSA für die Anlage einen signifikanten Mehrwert bringt oder nicht, sollte mit der Beschränkung auf die vier am stärksten von Systemausfällen betroffenen Module bereits möglich sein. Die MUPSA kann bzgl. der Notwendigkeit zur Implementierung von weiteren Modulen analysiert werden.

11.1.4 Bestimmung der spezifischen auslösenden Ereignisse für die Mehrblock-PSA

Es gibt unterschiedliche Gründe, dass mehrere Reaktormodule gleichzeitig von auslösenden Ereignissen betroffen, d. h. ihre Sicherheit beeinträchtigt sein kann. Nachfolgend werden einige dieser Gründe näher untersucht:

- Unkorreliert auftretende auslösende Ereignisse: Dabei handelt es sich um auslösende Ereignisse, die in unterschiedlichen Modulen aus unterschiedlichen Gründen eintreten. Für diese Ereignisse ist die Verwendung eines Abschneidekriteriums besonders wichtig, um die Vielzahl der Kombinationen auf die wichtigsten Szenarien zu beschränken. Die Gleichzeitigkeit der Ereignisse soll hier möglichst konservativ betrachtet werden (gemeinsam verwendete Systeme werden gleichzeitig benötigt). Für die Bestimmung der Eintrittshäufigkeit der unkorreliert auftretenden auslösenden Ereignisse wird eine zeitliche Überlappung im Bereich der Missionszeit von 72 h angesetzt.
- Auslösende Ereignisse, die mehrere Reaktormodule betreffen
  - auslösende Ereignisse, die in Bereichen mit gemeinsam genutzten SSC eintreten und daher mehrere Module gleichzeitig betreffen, sowie
  - auslösende Ereignisse aufgrund von Ausfällen aus gemeinsamer Ursache, die sich beispielsweise durch leichte Netzspannungsschwankungen, einen Lastwechsel oder Vibrationen einer Bautätigkeit gleichzeitig oder kurz nacheinander in mehreren Modulen bemerkbar machen.

Die unterschiedlichen Arten auslösender Ereignisse in mehreren betroffenen Modulen werden im Folgenden näher untersucht, bzw. die Eintrittshäufigkeiten abgeschätzt und

die Notwendigkeit detaillierter Analysen in der MUPSA anhand eines Auswahlkriteriums bewertet.

Unkorreliert auftretende auslösende Ereignisse

Die Auswahl relevanter auslösender Ereignisse der Single-Unit PSA für eine weitere Berücksichtigung in der Multi-Unit PSA erfolgt über ein qualitatives und ein quantitatives Auswahlverfahren entsprechend Abschnitt 2.4.1. Bei der Betrachtung nur eines Moduls in der SUPSA werden alle Systeme mit uneingeschränkter Verfügbarkeit modelliert. Sind mehrere Module betroffen, so kommt es zu eingeschränkten Verfügbarkeiten von Systemen, insbesondere des CFDS, und der Betriebsmannschaft. Für die unkorreliert auftretenden auslösenden Ereignisse sollen zunächst die möglichen Eintrittshäufigkeiten mit einem Abschneidekriterium verglichen werden.

Die Wahrscheinlichkeit, dass sich während des Unfallablaufs in einem Modul innerhalb von 72 Stunden, ein weiterer Vorfall in einem anderen Modul ereignet, liegt für eine Eintrittshäufigkeit von X/Jahr bei

$$p = X \cdot 72h \cdot 11\ Module = X \cdot 9{,}03 \cdot 10^{-2} \cdot Jahr. \quad (11.1)$$

Die Eintrittshäufigkeit eines identischen auslösenden Ereignisses in zwei Modulen liegt bei

$$k = X \cdot 12\ Module \cdot X \cdot 0{,}5 \cdot 72h \cdot 11\ Module = 0{,}542 \cdot X^2 \cdot Jahr. \quad (11.2)$$

Der Faktor 0,5 berücksichtigt die Unbestimmtheit der ausgefallenen Module – der gemeinsame Ausfall zweier beliebiger Module errechnet sich über $\binom{12}{2} = 12 \cdot 11 \cdot 0{,}5$, mit einer Korrektur bzgl. der Doppelzählung.

Für stochastisch unabhängig, also unkorreliert, auftretende Unfälle in mehreren Modulen soll das quantitative Auswahlkriterium $\alpha = 0{,}1\ \%$ verwendet werden, d. h. Kernschadenshäufigkeiten unterhalb 0,1 % der SUPSA Gesamtkernschadenshäufigkeit werden direkt vernachlässigt. Die Schwelle bzw. das Auswahl- oder Abschneidekriterium liegt demnach bei 2,0 E-10/a.

Auslösende Ereignisse mit X < 1,9 E-05/a (aus der obigen Formel und dem Abschneidekriterium bestimmt) für mehrere Module sind somit aufgrund des Auswahlkriteriums in der MUPSA nicht zu unterstellen. Diese auslösenden Ereignisse könnten dennoch

gleichzeitig zu auslösenden Ereignissen mit X > 1,9 E-05/Jahr, insbesondere im Laufe einer allgemeinen Transiente (hohe Eintrittshäufigkeit), auftreten.

Das Abschneidekriterium bezieht sich allerdings auf die zu erwartenden Kernschadenshäufigkeiten, weshalb eine Abschätzung der Kernschadenshäufigkeit in einem der beiden betroffenen Modulen herangezogen werden muss. Das Kriterium lautet damit:

$$X \cdot KS > 2{,}0 \cdot \frac{10^{-10}}{0{,}542 \cdot Jahr^2} = 3{,}69 \cdot \frac{10^{-10}}{Jahr^2}. \quad (11.3)$$

Falls eine Kombination aus zwei betroffenen Modulen mit einem erwarteten Kernschaden eine höhere Eintrittshäufigkeit im Vergleich zum Abschneidekriterium liefert, so wird diese Kombination weiter betrachtet. Für eine Abschätzung der Kernschadenshäufigkeit sollen Ergebnisse aus der SUPSA herangezogen werden, insbesondere die in Tab. 10.1 dargestellten.

In der obigen Abschätzung wird nur der Kernschaden in einem Modul berücksichtigt, weshalb die GVA in der Abschätzung nicht auf mehrere Module übertragen werden müssen. Allerdings wird ein Erschwernisfaktor von 10 für die Handmaßnahmen auf die Kernschadenshäufigkeiten multipliziert (sofern Handmaßnahmen relevant sind). Die Ergebnisse sind in Tab. 11.1 (letzte Spalte) aufgeführt.

Damit ist die Betrachtung einer gegenseitigen Beeinflussung der Unfallabläufe in der Multi-Unit PSA für unkorrelierte auslösende Ereignisse nur in Kombination mit einer allgemeinen Transiente notwendig. Die Fälle ergeben sich dabei für eine allgemeine Transiente in einem Modul und dem Kernschaden in dem anderen Modul. Es kann damit weiter konkretisiert werden, dass eine Erschwernis bei der Unfallbeherrschung vorliegt, wenn die allgemeine Transiente die Betriebsmannschaft fordert, also insbesondere, wenn der reguläre Ablauf der Transiente gestört ist. Dies ist für einen ATWS mit 3 E-05/a, den Ausfall des DHRS mit 7 E-05/a und ein RSV, das nicht wieder schließt mit 7 E-04/a der Fall. Kombiniert mit der Wahrscheinlichkeit von 8 E-04/a für eine ungewöhnlich ablaufende allgemeine Transiente erfüllt keines der betrachteten auslösende Ereignisse das Abschneidekriterium.

Tab. 11.1 Auslösende Ereignisse, die nicht automatisch zu einer RESA in mehreren Modulen führen

Kürzel	Kernschaden bei	Häufigkeiten (pro Jahr)		
		Auslösendes Ereignis	**Kernschadens-zustand**	**Kernschadens-zustand mit Erschwernisfaktor zur Durchführung von Handmaßnahmen**
TA	Allgemeine Transiente	1,3E+00	9,5 E-10	9,5 E-09
TD	EDSS-Ausfall	4,7 E-05	2,7 E-10	2,7 E-09
TS	Leitungsleck im Sekundärkühlkreis	4,4 E-05	1,9 E-12	1,9 E-11
TÜ	Dampferzeugerüberspeisung	1,0 E-05	4,1 E-13	4,1 E-12
TH	Überspeisung durch das CVCS	1,0 E-05	1,6 E-13	1,6 E-12
TL	Leck zwischen Reaktorbecken und Sicherheitsbehälter	1,0 E-07	2,9 E-11	2,9 E-10
TF	Funktionales Versagen des Naturumlaufes	1,0 E-07	5,0 E-08	5,0 E-08
RS	Fehlausfahren der Steuerstäbe	2,0 E-04	2,7 E-09	2,7 E-08
LC	Leck der CVCS-Einspeiseleitung in den Sicherheitsbehälter	1,4 E-04	2,6 E-10	2,6 E-09
LR	Leck der CVCS-Entnahmeleitung in das Reaktorgebäude	1,4 E-04	5,9 E-13	5,9 E-12
LE	Leck der CVCS-Einspeiseleitung in das Reaktorgebäude	2,8 E-04	1,4 E-11	1,4 E-10
LP	KMV in den Sicherheitsbehälter	2,0 E-03	3,3 E-09	3,3 E-08
LH	Dampferzeuger-Bypassleck	4,5 E-05	2,3 E-12	2,3 E-11
LV	Fehlerhafte Aktivierung des ECCS	1,1 E-05	1,8 E-11	1,8 E-10
NF	Fall eines Moduls, POS3&5	1,1 E-07	8,5 E-08	8,5 E-08
NÜ	Überdruck im kalten RCS, POS2&6	1,2 E-07	1,2 E-10	1,2 E-09

Dennoch sollen im Folgenden unkorreliert auftretende allgemeine Transienten (für deren Auftreten kein kausaler Zusammenhang besteht) in zwei und drei Reaktormodulen gleichzeitig analysiert werden, um die anzuwendende Methodik auszuprobieren. Die

zugehörigen Eintrittshäufigkeiten liegen bei 9,17 E-01/a für zwei Module und 3,26 E-02/Jahr für drei Module.

Auslösende Ereignisse, die mehrere Reaktormodule betreffen

Es lassen sich zwei unterschiedliche Arten von auslösenden Ereignissen für mehrere Reaktormodule unterscheiden. Zum einen gibt es gekoppelte auslösende Ereignisse, die beispielsweise auf ein GVA-Ereignis zurückzuführen sind. Mögliche Ursachen können nach /NUS 20/ folgende Mechanismen sein:

- Alterungseffekte (z. B. Abnutzung, chemische Effekte),
- Fertigungsfehler,
- ähnliche Phasenübergänge,
- ungünstige Umgebungsbedingungen,
- ein gemeinsamer Auslöser (z. B. über ein gemeinsam verwendetes angeschlossenes System).

In diese Kategorie fallen prinzipiell alle auslösenden Ereignisse, die in Tab. 11.1 betrachtet wurden, mit Ausnahme der Ereignisse im Nichtleistungsbetrieb bzw. im Zuge eines Brennelementwechsels (nur ein Modul befindet sich in diesem Betriebszustand). Weitere mehrere Module betreffende auslösende Ereignisse sind solche, die generell alle Module betreffen bzw. übergreifend sind, hierzu zählen neben den internen Einwirkungen ‘anlageninterner Brand‘ und ‘anlageninterne Überflutung‘ auch:

- Ausfall der externen Stromversorgung (in allen Modulen gleichzeitig) /DOY 20/ für Ausfälle, die durch extreme Wetterereignisse und technische Ausfälle im Stromnetz bedingt sein können, erfolgt eine Umschaltung auf Inselbetrieb der Anlage. In diesen Fällen bleiben alle Module kritisch.
- Ausfall von Komponentenhilfssystemen (in sechs oder zwölf Modulen gleichzeitig).

Auslösende Ereignisse in Folge einzelner Einwirkungen von innen (Brand, Überflutung) oder Einwirkungskombinationen gleichzeitig in mehreren Modulen:

- Allgemeine Transiente (teilweise in sechs Modulen gleichzeitig mit Zusatzausfällen eines EDSS-Busses oder einer ESFAS-Redundanz),

- Ausfall der Stromversorgung/Notstromfall (in allen Modulen gleichzeitig),
- Überspeisung durch das CVCS (in sechs Modulen gleichzeitig),
- Fehlerhafte Aktivierung des ECCS (teilweise in allen Modulen gleichzeitig)
- Ausfall von Komponentenhilfssystemen (in sechs Modulen gleichzeitig bei Ausfall der Komponentenkühlwasser und Teilen der Wechselstromversorgung /DOY 20/, in zwölf Modulen gleichzeitig für einen Ausfall der Luftdruckversorgung).

Auslösende Ereignisse, die korreliert auf einen GVA zurückzuführen sind, können über das quantitative Auswahlkriterium α = 0,1 %, und damit 2,0 E-10/a bewertet werden. Zur Bewertung lassen sich konservativ betrachtet nur die Systeme DHRS, ECCS, RESA und RSV ohne die Möglichkeit der Auslösung durch die Betriebsmannschaft berücksichtigen. Zusätzlich wird zunächst davon ausgegangen, dass die Wahrscheinlichkeit für das auslösende GVA-Ereignis maximal 10 % des auslösenden Ereignisses ausmacht (Annahme des β-Modells). Folgende auslösende Ereignisse fallen nach diesem Kriterium aus der Betrachtung heraus:

- Leitungsleck im Sekundärkühlkreis,
- Funktionales Versagen des Naturumlaufs,
- Leck der CVCS-Entnahmeleitung in das Reaktorgebäude,
- Leck der CVCS-Einspeiseleitung in das Reaktorgebäude,
- Dampferzeuger-Bypassleck,
- EDSS-Ausfall,
- Fehlausfahren der Steuerstäbe,
- Dampferzeugerüberspeisung,
- Überspeisung durch das CVCS.

Für die übrigen auslösenden Ereignisse werden mögliche Ursachen für ein gleichzeitiges Auftreten einer GVA im Folgenden diskutiert.

Das auslösende Ereignis ‘Leck zwischen Reaktorbecken und Sicherheitsbehälter‘ könnte durch Fehler in der Verschraubung zwischen Deckel und Unterteil des Sicherheitsbehälter verursacht werden. Die Verschraubung wird in allen Modulen nach dem

Brennelementwechsel und damit zeitlich versetzt zueinander ausgeführt. Ein entsprechendes Leck ist mit einer erhöhten Wahrscheinlichkeit während oder in der Folge der Sicherheitsbehälterentwässerung oder eines Lastwechsels denkbar. Eine Temperaturänderung im Reaktorbecken und ein gemeinsamer Lastwechsel in mehreren Modulen könnte das gleichzeitige Auftreten eines entsprechenden Schadens an mehreren Modulen auslösen.

In einem einfachen Modell fällt die Eintrittshäufigkeit im Unsicherheitsband vom 95%-Perzentil, 3,75 E-07/a, nach dem Brennelementwechsel auf das 5%-Perzentil, 3,75 E-09/a, vor dem nachfolgenden Brennelementwechsel ab. Der Abfall erfolgt logarithmisch. Mit einem β-Faktor von 10 % wird die Schwelle von 2,4 E-09/a 14 Monate nach Brennelementwechsel erreicht. In einer ungünstigen Annahme könnten demnach bis zu sieben Module gleichzeitig von einem Leck zwischen Reaktorbecken und Sicherheitsbehälter betroffen sein.

Ein weiteres auslösendes Ereignis ist das Leck der CVCS-Einspeiseleitung in den Sicherheitsbehälter, hierzu zählen Lecks an Rohrleitungen, die durch den Sicherheitsbehälter verlaufen. Eine gemeinsame Ursache für ein gleichzeitiges Auftreten dieses auslösenden Ereignisses in mehreren Modulen konnte nicht gefunden werden. Einzig ein möglicher gemeinsamer Lastwechsel mit einer gleichzeitig einsetzenden Sicherheitsbehälter-Sprühen und eine gemeinsame Alterungserscheinung in allen Modulen (es wird davon ausgegangen, dass alle Module ungefähr gleich viele Betriebsstunden durchlaufen haben) könnte ein gewisses Risiko darstellen. Ein β-Faktor von 10 % wird hierfür aber als zu hoch eingeschätzt und damit wird dieses auslösende Ereignis im Rahmen der Multi-Unit PSA nicht weiter untersucht.

Das auslösende Ereignis ‘KMV in den Sicherheitsbehälter‘ setzt sich aus mehreren möglichen Auslösern zusammen. Ein direkter Schaden an der druckführenden Umschließung hat nur ein geringes Potenzial in mehreren Modulen gleichzeitig zu entstehen (mögliche kleine alterungsbedingte Risse, die durch kleine Erschütterungen weiter aufreißen oder ähnliches). Ein weiterer Grund für ein KMV in den Sicherheitsbehälter ist der Verlust der Dichtheit eines der RSV oder der ECCS-Ventile. Ein Ereignis, dass für Ventile in unterschiedlichen Modulen gleichzeitig auslösend ist, könnte hier möglicherweise ein Lastwechsel mit einer Druckänderung im Primärkreis darstellen. Die Gefahr für ein GVA der Dichtheit mehrerer Ventile in unterschiedlichen Modulen wird allerdings als gering eingeschätzt. Die Möglichkeit eines GVA mehrerer fehlerhaft arbeitender Druckhalterheizungen nach einer gemeinsamen Anforderung führt in KMV in die Sicherheitsbehälter

mehrerer Module. Die Häufigkeit eines Einzelfehlers einer Druckhalterheizung wird entsprechend der Häufigkeit für eine Überspeisung durch das CVCS und einer Fehlerhaften Aktivierung des ECCS (diese auslösenden Ereignisse stehen im Zusammenhang mit einem Fehler in der Komponentenansteuerung) mit 1E-05/Jahr abgeschätzt. Mit einem β-Faktor von 10 % ist man damit über dem quantitativen Auswahlkriterium und die GVA-Fehlfunktion der Druckhalterheizungen in mehreren Modulen soll in der MUPSA näher analysiert werden.

Die fehlerhafte Aktivierung des ECCS wird brandbedingt untersucht und ein mögliches GVA (außerhalb der Brandursache) liefert keinen nennenswerten Beitrag. Ein GVA für eine allgemeine Transiente in allen Modulen wird mit einem β-Faktor von 10 % untersucht

In der MUPSA werden korrelierte auslösende Ereignisse zu den Ereignissen näher betrachtet:

- Fehlerhafte Aktivierung des ECCS,
- Allgemeine Transiente,
- KMV in den Sicherheitsbehälter (eine mögliche Leckursache besteht in einer Fehlfunktion in der Druckhalterheizung, weshalb hier kein klassischer Rohrschaden vorliegt),
- Leck zwischen Reaktorbecken und Sicherheitsbehälter.

Darüber hinaus zeigt sich, dass die brandbedingte Überspeisung durch das CVCS mit Hilfe der durch Handmaßnahmen bereinigten Systeme DHRS, ECCS, RESA und RSV in allen Modulen unabhängig gut beherrscht werden kann und entsprechend unter das quantitative Auswahlkriterium fällt und damit aus der MUPSA-Betrachtung herausfällt.

Die Eintrittshäufigkeiten aller in der MUPSA zu berücksichtigenden auslösenden Ereignisse sind in Tab. 11.2 dargestellt.

Tab. 11.2 Eintrittshäufigkeiten für auslösende Ereignisse in mehreren Reaktormodulen

Auslösendes Ereignis		Eintrittshäufigkeit (pro Jahr)				
		Betroffene Module	**Übergreifendes internes auslösendes Ereignis**	**Interner Brand oder Überflutung**	**Basierend auf GVA (β-Modell)**	**Unkorreliert**
TA	Allgemeine Transiente	2	–	–	–	9,17 E-01
		3	–	–	–	3,26 E-02
		6	–	4,9 E-02	–	–
		12	–	8,3 E-01	1,3 E-01	–
TN	Ausfall der externen Stromversorgung	12	2,2 E-02	6,5 E-02	–	–
TV	Ausfall von Komponenten-hilfssystemen	6	9,1 E-03	1,9 E-02	–	–
		12	1,0 E-02	–	–	–
TL	Leck zwischen Reaktorbecken und Sicherheitsbehälter	2 bis 8	–	–	2,6 E-08 bis 2,6 E-09	–
LP	KMV in den Sicherheits-behälter	12	–	–	1,0 E-06	–
LV	Fehlerhafte Aktivierung des ECCS	12	–	3,9 E-04[46]	1,1 E-06	–

[46] Die wärmebedingte Fehlauslösung aller ECCS-Auslöseventile wird über das β-Modell mit der Wahrscheinlichkeit 7,7 E-03 quantifiziert (β-Faktor 0,1). Die gemeinsame Ursache ist der Brand und es wird angenommen, dass sich die Elektronik für alle Module im Brandabschnitt 75'Elektrisches Kabinett befindet. Die Räume könnten sich einem Zustand außerhalb der Spezifikation der Elektronik befinden, was eine gemeinsame Auslösung (auch aller Module) wahrscheinlicher macht.

In der MUPSA ergeben sich damit nur gleichzeitige Unfallabläufe in mehreren Modulen, die auf das dasselbe oder ein gleich(artig)es auslösendes Ereignis zurückzuführen sind. Diese Erkenntnis vereinfacht die MUPSA-Modellierung wesentlich, da unterschiedliche SUPSA-Ereignisabläufe nicht miteinander kombiniert werden müssen. Diese wesentliche Vereinfachung wird weiter unten deutlich.

Verifikation des quantitativen Auswahlkriteriums

Die Wahl Risikoquantifizierung für eine SMR-Anlage mit mehreren Reaktormodulen fiel auf die Größe SCDF, d. h. die Häufigkeit für Einzel- und Mehrfachkernschäden in der Anlage, weil diese Größe einen geringeren Aufwand in den Ereignisablaufanalysen darstellt als die explizite Bestimmung der MUCDF und SUCDF. Die SCDF wird zunächst sehr stark von der PSA für ein einzelnes Reaktormodul dominiert, da ein Kernschaden in einem Modul ausreicht.

Kernschäden in mehreren Modulen gleichzeitig treten vermutlich seltener auf, das gilt insbesondere dann, wenn der Einfluss der Systeme mit eingeschränkter Verfügbarkeit und die notwendigen Handmaßnahmen einen geringen Einfluss auf die Kernschadenshäufigkeit für ein einzelnes Reaktormodul haben. Für eine explizite Bestimmung der Mehrfachkernschäden könnte das gewählte quantitative Auswahlkriterium zu strikt sein, weil die Häufigkeiten für Mehrfachkernschäden, z. B. für Schäden an Kernen in fünf Modulen, möglicherweise um mehrere Größenordnungen geringer ausfallen als für einen Kernschaden in nur einem Modul. Das hängt damit zusammen, dass für Kernschäden in mehreren Modulen generell viel mehr Systeme und Komponenten ausfallen müssen als in einem einzelnen Modul.

11.2 Modellentwicklung eine Mehrblock-PSA der Stufe 1

Eine Überarbeitung der Mehrblock-Schadenskombinationen entsprechend Abb. 11.1 ist in dieser Multi-Unit PSA nicht erforderlich, da keine Schadenskombinationen explizit unterschieden werden sollen. Im Wesentlichen soll in dieser Multi-Unit PSA ein Vergleich zwischen dem Ergebnis der Single-Unit PSA und der Multi-Unit PSA erfolgen. Die Kernschadenshäufigkeiten für mehrere Kernschäden sollen auch nicht explizit ausgewiesen werden. Das Ergebnis könnte als Maß für die Verflechtung der Systeme zur Unfallbeherrschung (bzgl. Verfügbarkeit und internen Brand- und Überflutungsrisiko), des Risikos aus GVA und Fehlern der Betriebsmannschaft gedeutet werden.

11.2.1 Ereignisablaufanalysen bei der Mehrblock-PSA

Die Modellierung der -Ereignisablaufanalysen für zwölf Reaktormodule in der RiskSpectrum® -Version 1.4 erforderte eine besondere Methodik. Ein wesentlicher Aufwand in der Multi-Unit PSA stellt die Abbildung jedes einzelnen Moduls über separate Verzweigungen in den Ereignisablaufanalysen dar. So ergeben sich z. B. entweder zwölf separate Systemfunktionen (für jedes Modul eine, daraus ergeben sich 2^{12}) oder eine Systemfunktion mit 2^{12} möglichen Ausfallkombinationen/Abzweigungen. Mit Hilfe eines Übergangs von den zwölf spezifischen Modulen in der Anlage zu zwölf identischen Modulen konnten die -Ereignisablaufanalysen der Multi-Unit PSA wesentlich vereinfacht werden.

Die Idee dabei ist, die Module anhand der zugewiesenen Systemausfälle in den Cut Sets zu unterscheiden. Die Cut Sets unterscheiden demnach nicht, ob die Module in der dritten und fünften Reaktorposition im Reaktorbecken ein Ausfall der RESA erleiden oder die Module in der zweiten und siebten Bucht, usw. Insgesamt werden damit z. B. für Ausfälle in zwei von zwölf Modulen $\binom{12}{2} = 66$ mögliche Sequenzen in einer Sequenz bzw. in einem Cut Set zusammengefasst.

Darüber hinaus beschränkt sich das Modell bisher auf die konkrete Implementierung von vier Modulen, wie bereits in Abschnitt 11.1.3 diskutiert. Die Methodik der MUPSA-Ereignisablaufanalysen soll anhand eines einfachen Beispiels näher erläutert werden. Ein KMV in den Sicherheitsbehälter kann durch einen defekten in fehlerhaftem Dauerbetrieb befindliche Druckhalterheizung verursacht werden. Bei einem Lastwechsel oder ähnlichem könnten mehrere Module gleichzeitig die Druckhalterheizung in Betrieb nehmen und ein GVA der Druckhalterheizung würde in den entsprechenden Modulen zu einem KMV in den Sicherheitsbehälter führen. Das entsprechende Mehrmodulereignis wird in der Ereignisablaufanalyse Abb. 11.2 betrachtet.

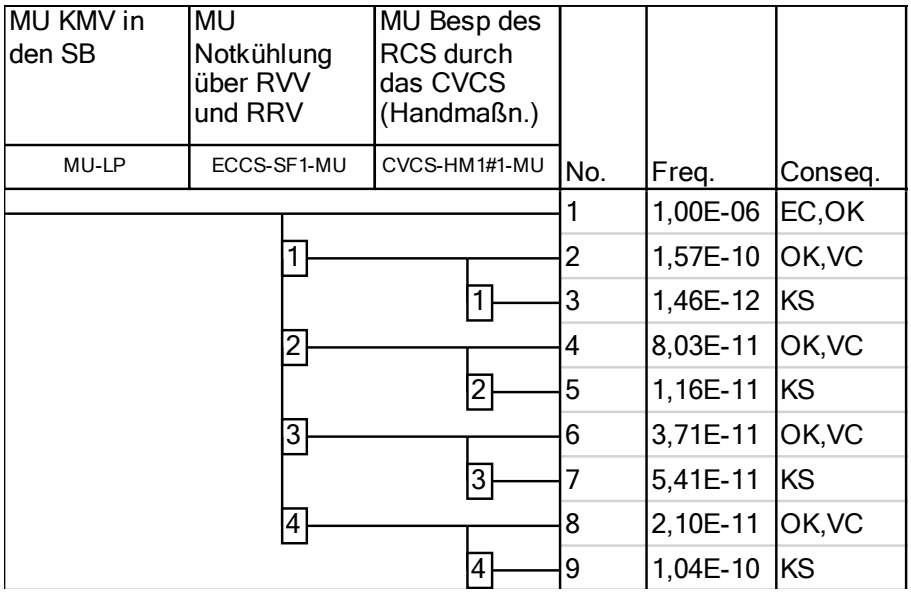


Abb. 11.2 Modellierung eines KMV in den Sicherheitsbehälter für mehrere betroffene Modulen

Die Systemfunktionen entsprechen grundsätzlich den Systemfunktionen der Single-Unit PSA in Abb. 7.13. Die Anzahl der vom auslösenden Ereignis betroffenen Module wird zu Beginn der Analyse über Hausereignisse in RiskSpectrum® festgelegt. Für die erste Systemfunktion werden die Wahrscheinlichkeiten dafür bestimmt, ob die Notkühlung in einem (erste Abzweigungsalternative), in zweien (zweite Abzweigungsalternative), in dreien (dritte Abzweigungsalternative) oder in vier (vierte Abzweigungsalternative) beliebigen Modulen der Anlage die Notkühlung ausfällt.

Im Fall der zweiten Systemfunktion, der Bespeisung über des RCS über das CVCS, ist die Logik ein wenig anders. Für die erste Abzweigungsalternative muss genau ein Modul gespeist werden, falls dies fehlschlägt, ist mit einem Kernschaden zu rechnen. Für die zweite Abzweigungsalternative müssen zwei Module gespeist werden. Wenn in einem oder beiden dieser Module die Bespeisung fehlschlägt, so muss mindestens mit einem Kernschaden in der Anlage gerechnet werden. Entsprechendes gilt für die dritte bzw. vierte Abzweigungsalternative für drei bzw. vier Module. Alle weiteren untersuchten Ereignisablaufdiagramme sind ähnlich aufgebaut, allerdings aufgrund von mehreren Systemfunktionen weitaus unübersichtlicher.

Die erste Ebene der Fehlerbäume zur Modellierung der Systemfunktionen ist aufgrund der Technik der Abzweigungsalternativen besonders stark auf die Ereignisablaufanalysen zugeschnitten. Beispielhaft soll die oberste Ebene der Fehlerbäume für den Ausfall

des ECCS in zwei Modulen und für den Ausfall der Bespeisung des RCS durch das CVCS (zweite Abzweigungsalternative) besprochen werden. Der relevante Ausschnitt der obersten Ebene der Fehlerbäume für den Ausfall des ECCS in zwei Modulen ist in Abb. 11.3 gezeigt. In diesem Fall sind die House Events M12 sowie M1 bis M4 (explizit bedeutet das, dass die möglichen Kombinationen von Modulen in der Anlage über Binominalkoeffizienten bereits berücksichtigt wurden).

Im Fall der zwölf betroffenen Module ist das noch nicht geschehen, weshalb dieser Faktor mit dem Ereignis M2V12_2 verrechnet wird, d. h. die ursprüngliche Ereigniseintrittswahrscheinlichkeit wurde um einen Faktor $\binom{12}{4} = 495$ erhöht, und wird hier auf den anzuwendenden Faktor $\binom{12}{2} = 66$ wieder reduziert. Der Grund ist, dass RiskSpectrum® in den Fehlerbäumen nur Faktoren < 1 berücksichtigen kann. Darüber hinaus muss die Notkühlung in zwei Modulen ausfallen, ECCS-P M1 und ECCS-P M2 (zugrundeliegende Fehlerbäume entsprechen denen in der SUPSA) und darf in keinem weiteren Ausfallen, in diesem Fall ist das ECCS-P M3.

Die weitere Betrachtung in der Ereignisablaufanalyse beschäftigt sich nun nur noch mit den beiden vom Ausfall des ECCS betroffenen Module, die nun explizit bestimmt sind. Für diese Module ist eine Bespeisung notwendig, der berücksichtigte Fehlerbaum ist in Abb. 11.4 dargestellt. Stehen grundsätzlich die Komponentenhilfssysteme zur Verfügung, so wird der Ausfall des CVCS in einem oder beiden Modulen über ein ODER-Glied verknüpft analysiert. Die darunterliegenden Fehlerbäumen sind nahezu identisch zu den Fehlerbäumen in der Multi-Unit PSA, berücksichtigen aber das Modell für die Zuverlässigkeit des Personals in der PSA für mehrere Module, siehe Abschnitt 11.2.3.

Für CVCS-M1 werden u. a. auch die Ereignisse XOP 1V3 berücksichtigt, die hier im Fehlerbaum wieder ausgeschlossen werden, weil nur 2 Module von einem ECCS-Versagen betroffen sind. Die einzige Ausnahme bildet hier das Ereignis eines anlageninternen Brands mit Ausfall beider Redundanzen des ESFAS – in diesem Fall müssen generell sechs Module über Handmaßnahmen gesteuert werden, dabei musste auch das ECCS schon von Hand initiiert werden.

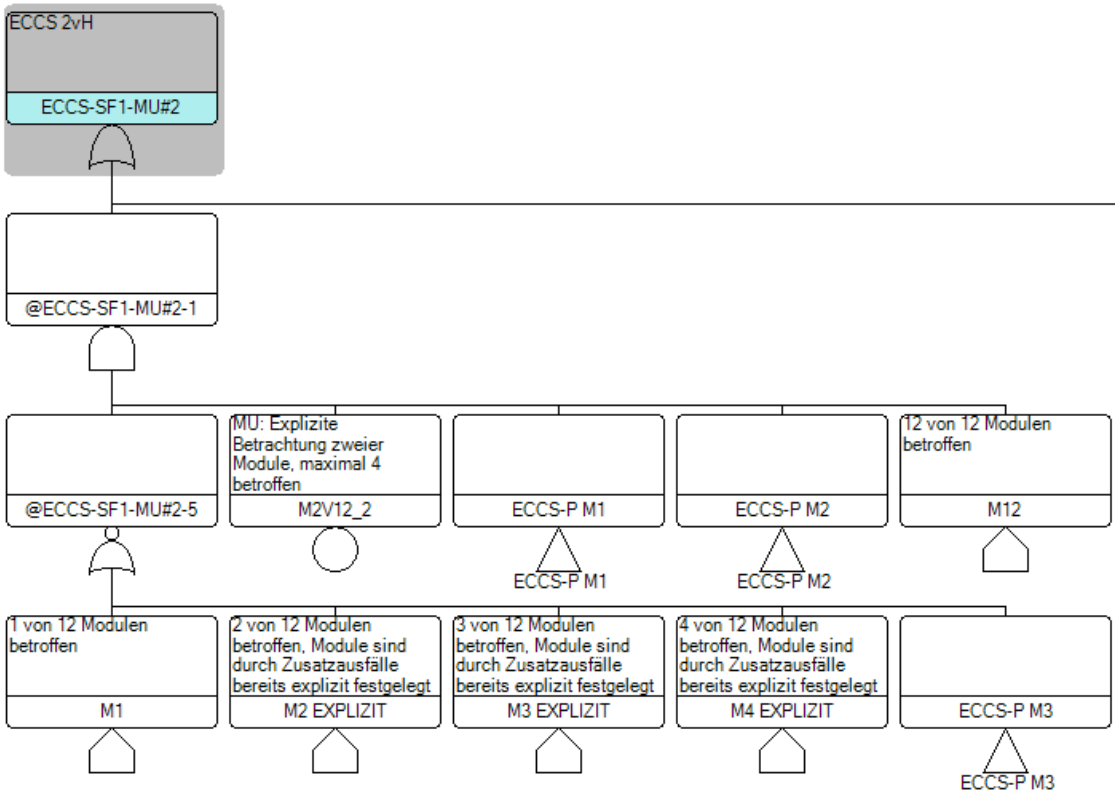


Abb. 11.3 Teil des Fehlerbaums bzgl. eines möglichen Ausfalls des ECCS in zwei Modulen bei einer Anforderung des ECCS in zwölf Modulen

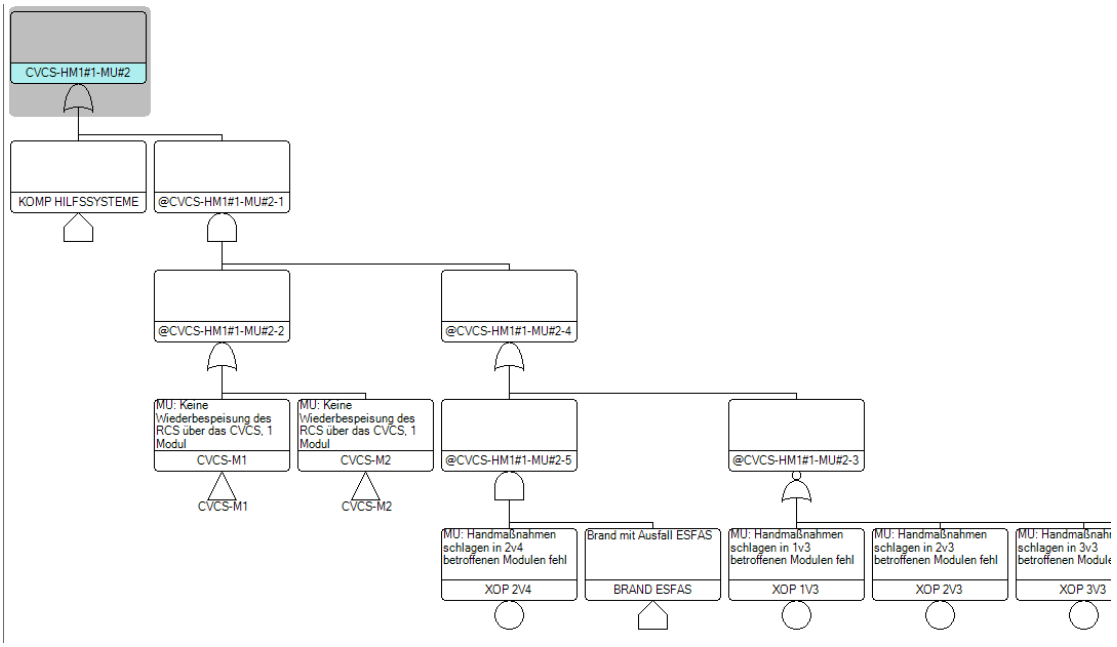


Abb. 11.4 Fehlerbaum zum Ausfall des CVCS in einem oder beiden betroffenen Modulen, abgeschnitten sind die vier Basisereignisse XOP 1v4 bis 4v4

In Abb. 11.2 zeigt sich zudem ein Aspekt der Mehrblock-PSA, der noch zu diskutieren ist. Ein Argument für eine Beschränkung der expliziten Modellierung von nur vier der zwölf Module mit Fehlerbäumen ist die abnehmende Wahrscheinlichkeit für Systemausfälle in mehreren Modulen. Das Ergebnis in der Spalte ‘Freq.‘, das in die Abbildung mit eingeflossen ist, zeigt allerdings für vier Module in Sequenz 9 höhere Kernschadenshäufigkeiten als für drei oder zwei Module, siehe Sequenzen 7 und 5. Dieses Ergebnis zeigt sich nur in dieser Ereignisablaufanalyse, hier könnte die MUPSA noch für Ausfälle in mehr als vier Modulen erweitert werden.

11.2.2 Systemanalysen der Mehrblock-PSA

Die Systemanalysen der Multi-Unit PSA entsprechen im Wesentlichen der Modellierung in der Single-Unit PSA, die für vier Module vervielfältigt wurde. Darüber hinaus musste das Modell zur Zuverlässigkeit des Personals entsprechend dem nachfolgenden Abschnitt 11.2.3 verändert und die Basisereignisse für GVA auf größere Komponentengruppen (siehe Abschnitt 11.2.4) erweitert werden, die alle Module einschließen.

11.2.3 Untersuchung der Zuverlässigkeit des Personals einer PSA für mehrere Reaktormodule

Eine detaillierte Untersuchung der Zuverlässigkeit des Personals im Hinblick auf die gleichzeitige Zuständigkeit für zwölf Reaktormodule konnte im Rahmen dieses Projektes noch nicht durchgeführt werden. Für die Implementierung der Zuverlässigkeit des Personals in der MUPSA wurden deshalb sehr vereinfachte Abschätzungen getroffen. Im Fall von mehr als vier betroffenen Modulen, die eine Handmaßnahme benötigen, werden im weiteren Unfallablauf vier betroffene Module weiter betrachtet.

Tab. 11.3 Bewertung der Zuverlässigkeit des Personals zur Durchführung benötigter Handmaßnahmen in mehreren Modulen der Anlage

Anzahl Module mit fehlerhaften Handmaßnahmen	**Fehlerwahrscheinlichkeiten, wenn x Module eine Handmaßnahme benötigen**			
	1 Modul	**2 Module**	**3 Module**	**4 Module**
1 Modul	Analog zur PSA für ein Modul	0,1	0,50	0,70
2 Module	–	0,01	0,10	0,24
3 Module	–	–	0,01	0,05

Anzahl Module mit fehlerhaften Handmaßnahmen	Fehlerwahrscheinlichkeiten, wenn x Module eine Handmaßnahme benötigen			
	1 Modul	2 Module	3 Module	4 Module
4 Module	–	–	–	0,01
1 bis 4 Module (Summe)	Analog zur PSA für ein Modul	0,11	0,61	1,00

11.2.4 GVA und Fragility Analysis

Die Betrachtungen zur GVA beruhen auf der Erweiterung der Komponentengruppen auf die baugleichen Komponenten in allen Modulen. Beispielsweise verfügt das ECCS über sechs ECCS-Auslöseventile in einem Modul. Die Komponentengruppe wächst für 12 Module auf 6 * 2 = 72 Ventile an. Lösen die Ventile in vier betroffenen Modulen aus, dann ergeben sich die Ausfallraten für 1 von 24 bis 24 von 24 betroffenen Ventilen unter der Berücksichtigung der Komponentenuntergruppe. Das bedeutet, dass z. B. für 24 von 24 betroffenen Ventilen mehrere mögliche Konstellationen zwischen 24 von 72 (genau eine Konstellation) bis 72 von 72 versagenden Ventilen bzgl. der vier betroffenen Modulen das gleiche Ergebnis (ein Ausfall aller benötigten Auslöseventile) hervorrufen.

Die unterschiedlichen Konstellationen, die zum gleichen Ergebnis führen, werden für die Quantifizierung des GVA entsprechend addiert, um die Ausfallwahrscheinlichkeiten für die Komponentenuntergruppen zu berechnen. Eine Fragility Analysis wurde nicht durchgeführt, da ein Erdbeben als auslösendes Ereignis nicht in die SUPSA und MUPSA integriert wurde. Der Ereignisfall eines Erdbebens sollte allerdings unbedingt in die MUPSA integriert werden, es stellt ein wichtiges auslösendes Ereignis für mehrere gleichzeitig betroffene Module dar.

11.3 Modell und Quantifizierung der Mehrblock-PSA

Das Modell der Multi-Unit PSA wurde bereits während des Erstellungsprozesses in das SUPSA-Modell integriert. Es liegt damit ein kombiniertes Modell in RiskSpectrum® vor. Die GVA und die Modellierung der Zuverlässigkeit der Betriebsmannschaft gehen für den Fall eines betroffenen Moduls in die SUPSA-Modellierung über, weshalb der separate Schritt der MUPSA Modellintegration, siehe Abb. 11.1, entfällt. Für die Quantifizierung der Mehrblock-PSA werden die entsprechenden Möglichkeiten in RiskSpectrum® verwendet.

11.4 Ergebnisse der Mehrblock-PSA

Die Kernschadenshäufigkeiten aus der Mehrblock-PSA sind in Tab. 11.4 nach den auslösenden Ereignissen aufgeschlüsselt angegeben. Es wird unterschieden zwischen Einzelmodulauslösern, deren Ergebnis ungefähr[47] zwölf Mal dem Ergebnis der SUPSA, Tab. 10.1, entspricht und Multi-Modul-Auslösern. Einige Auslöser der SUPSA kommen nicht als Einzelauslöser in der MUPSA vor, z. B. Ausfall der externen Stromversorgung, da von diesem Ausfall immer alle Module betroffen sind. Der Parameter Multi-Module Correlation Factor (MMCF) bildet sich aus dem Verhältnis zwischen den Kernschadenshäufigkeiten des MUPSA-Gesamtergebnisses und dem Ergebnis aus 12-mal dem SUPSA-Ergebnis. Er gibt damit an, inwieweit aus den einfachen SUPSA-Ergebnissen durch eine einfache Erweiterung auf 12 äquivalente Module ohne eine Berücksichtigung von Abhängigkeiten geschlossen werden kann. Darüber hinaus lässt sich damit quantifizieren, wie stark die Module bzgl. der Unfallsicherheit miteinander korreliert sind. Ein MMCF nahe 1 wäre ein sehr gutes Ergebnis und würde bedeuten, dass zwölf Einzelmodulanlagen an zwölf unterschiedlichen Standorten die gleiche gemeinsame Kernschadenshäufigkeit haben wie eine Anlage mit zwölf Reaktormodulen.

[47] Die präsentierten Größen geben den Mittelwert der Unsicherheitsverteilung an. Dieses Ergebnis weicht teilweise leicht von der Rechnung mit Einzelwerten ab, insbesondere ergibt sich hier teilweise eine leichte Verschiebung vom rechnerischen Ergebnis aus zwölf Mal dem SUPSA-Ergebnis. Die Einzelwertergebnisse in RiskSpectrum® sind präzise zwölffach größer.

Tab. 11.4 Ergebnisse der Mehrblock-PSA der Stufe 1 für alle Endzustände mit möglichen Brennelementschäden

Kürzel	Kernschaden nach/im …	KSZ-Häufigkeiten (pro Jahr)				Hauptbeiträge der Systeme
		12-mal Einzel-auslöser	Multi-Modul-Auslöser	Gesamt	MMCF	
LB	Leistungsbetrieb	9,3 E-07	3,3 E-06	4,2 E-06	2,99	1. Betriebsmannschaft 2. ECCS
T	Transienten	6,1 E-07	2,2 E-07	8,3 E-07	1,17	1. RCS 2. DHRS
TA	Allgemeine Transiente	1,5 E-08	3,0 E-08	4,5 E-08	2,97	1. DHRS 2. RSV
TN	Ausfall der externen Stromversorgung		6,1 E-08	6,1 E-08	0,74	1. ECCS 2. Notstrom
TD	EDSS-Ausfall	3,2 E-09		3,2 E-09	1,00	1. CIS 2. ECCS
TS	Leitungsleck im Sekundärkühlkreis	2,2 E-11		2,2 E-11	1,00	1. RSV 2. DHRS
TÜ	Dampferzeuger-Überspeisung	4,7 E-12		4,7 E-12	1,00	1. RSV 2. DHRS
TH	Überspeisung durch das CVCS	2,0 E-12		2,0 E-12	1,00	1. CIS/CVCS 2. ECCS
TV	Ausfall von Komponentenhilfssystemen		9,3 E-08	9,3 E-08	7,83	1. DHRS 2. RSV
TL	Leck zwischen Reaktorbecken und Sicherheits-behälter	3,5 E-10	4,0 E-08	4,1 E-08	117	1. Betriebsmannschaft 2. CIS
TF	Funktionales Versagen des Naturumlaufes	5,9 E-07		5,9 E-07	1,00	1. RCS 2. RTS
R	Reaktivitätsstörfälle	3,2 E-08	0,0E+00	3,2 E-08	1,00	1. RTS 2. ESFAS
RS	Fehlausfahren der Steuerstäbe	3,2 E-08		3,2 E-08	1,00	1. RTS 2. ESFAS
L	Kühlmittelverluststörfälle	4,6 E-08	5,2 E-10	4,7 E-08	1,01	1. CIS 2. CVCS
LC	Leck der CVCS-Einspeiseleitung in den Sicher-heitsbehälter	3,2 E-09		3,2 E-09	1,00	1. CIS/CVCS 2. ECCS
LR	Leck der CVCS-Entnahmeleitung in das Reak-torgebäude	6,6 E-12		6,6 E-12	1,00	1. RSV 2. DHRS

Kürzel	Kernschaden nach/im …	KSZ-Häufigkeiten (pro Jahr)				Hauptbeiträge der Systeme
		12-mal Einzel-auslöser	Multi-Modul-Auslöser	Gesamt	MMCF	
LE	Leck der CVCS-Einspeiseleitung in das Reak-torgebäude	1,7 E-10		1,7 E-10	1,00	1. CIS/CVCS 2. CFDS
LP	KMV in den Sicherheitsbehälter	4,3 E-08	2,4 E-10	4,3 E-08	1,01	1. CIS/CVCS 2. ECCS
LH	Dampferzeuger-Bypassleck	2,7 E-11		2,7 E-11	1,00	1. DHRS 2. RSV
LV	Fehlerhafte Aktivierung des ECCS	2,3 E-10	2,9 E-10	5,2 E-10	2,26	1. ECCS 2. Betriebsmannschaft
IB	Interner Brand	2,5 E-07	3,0 E-06	3,3 E-06	5,39	1. Betriebsmannschaft 2. ECCS
IB-TA	IB - Allgemeine Transiente	1,5 E-08	2,6 E-06	2,6 E-06	170	1. Betriebsmannschaft 2. DHRS
IB-TN	IB - Ausfall der Versorgung		3,7 E-07	3,7 E-07	1,08	1. ECCS 2. ELVS/Notstrom
IB-TH	IB - Überspeisung durch das CVCS	5,6 E-08		5,6 E-08	1,00	1. DHRS 2. RSV
IB-LV	IB - Fehlerhafte Aktivierung des ECCS	1,8 E-07	1,0 E-07	2,8 E-07	1,58	1. ECCS 2. Betriebsmannschaft
IÜ	Interne Überflutung	0	2,7 E-08	2,7 E-08	1,92	1. RSV 2. DHRS
IÜ-TA	IÜ - Allgemeine Transiente		6,9 E-09	6,9 E-09	24,5	1. DHRS 2. RSV
IÜ-TV	IÜ - Ausfall von Komponentenhilfssystemen		2,1 E-08	2,1 E-08	1,47	1. RSV 2. DHRS
NLB	Nichtleistungsbetrieb	1,0 E-06	0,0E+00	1,0 E-06	1,00	1. Kran 2. Betriebsmannschaft
NF	Fall eines Moduls, POS3&5	1,0 E-06		1,0 E-06	1,00	-
NÜ	Überdruck im kalten RCS, POS2&6	1,5 E-09		1,5 E-09	1,00	1. ECCS 2. IAB
NLB-TF	Funktionales Versagen des Naturumlaufes	7,0 E-11		7,0 E-11	1,00	1. Kran 2. Betriebs-mannschaft
	Gesamt	2,0 E-06	3,3 E-06	5,3 E-06	2,16	1. Betriebsmannschaft 2. RCS

Es zeigt sich, dass für einzelne auslösende Ereignisse die gemeinsame Betrachtung aller Module der Anlage für das Ergebnis relevant ist, dies ist mit MMCF > 100 für eine allgemeine Transiente in allen Modulen bei einem anlageninternen Brand und für ein Leck zwischen dem Reaktorbecken und dem Sicherheitsbehälter der Fall, zu sehen auch in Abb. 11.5. Auf das Gesamtergebnis gesehen relativieren sich die zusätzlichen Beiträge aus dem Gesamtanlagenbetrachtung im Vergleich zu einer Betrachtung von zwölf Einzelmodulanlagen. Das Gesamtergebnis liegt mit einem MMCF von 2,16 in der gleichen Größenordnung zum einfachen Ergebnis in zwölf Einzelmodulanlagen.

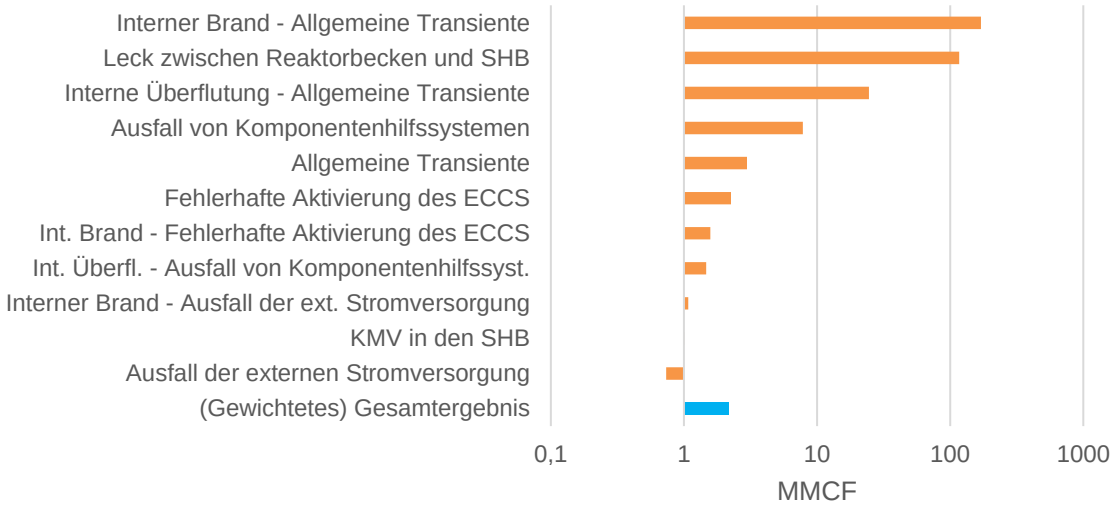


Abb. 11.5 Multi-Module Correlation Factor (MMCF) für die unterschiedlichen auslösenden Ereignisse

Der MMCF kann auch kleiner als 1 sein, wie im Fall des Ausfalls der externen Versorgung. Beiträge zum MMCF sind insbesondere:

- Beiträge, die den MMCF erhöhen:
  - höhere Fehlerrate der Betriebsmannschaft aufgrund zusätzlicher Aufgaben in anderen Modulen,
  - GVA in mehreren Modulen,
  - gemeinsam genutzte Systeme und eine begrenzte Ausrüstung,
- Beiträge, die den MMCF erniedrigen:
  - Geringere Fehlerentdeckungszeiten für GVA,

– Gemeinsame auslösende Ereignisse haben nur eine Eintrittshäufigkeit (z. B. Ausfall der externen Versorgung, welche in Einzelmodulanlagen an zwölf unterschiedlichen unabhängigen Standorten einzeln zusammengerechnet werden müsste, es ergibt sich damit ein Faktor 1/12).

Die Beiträge aus den einzelnen auslösenden Ereignissen an der Gesamtkernschadenshäufigkeit, 5,3 E-06/a, sind in Abb. 11.6 gezeigt.

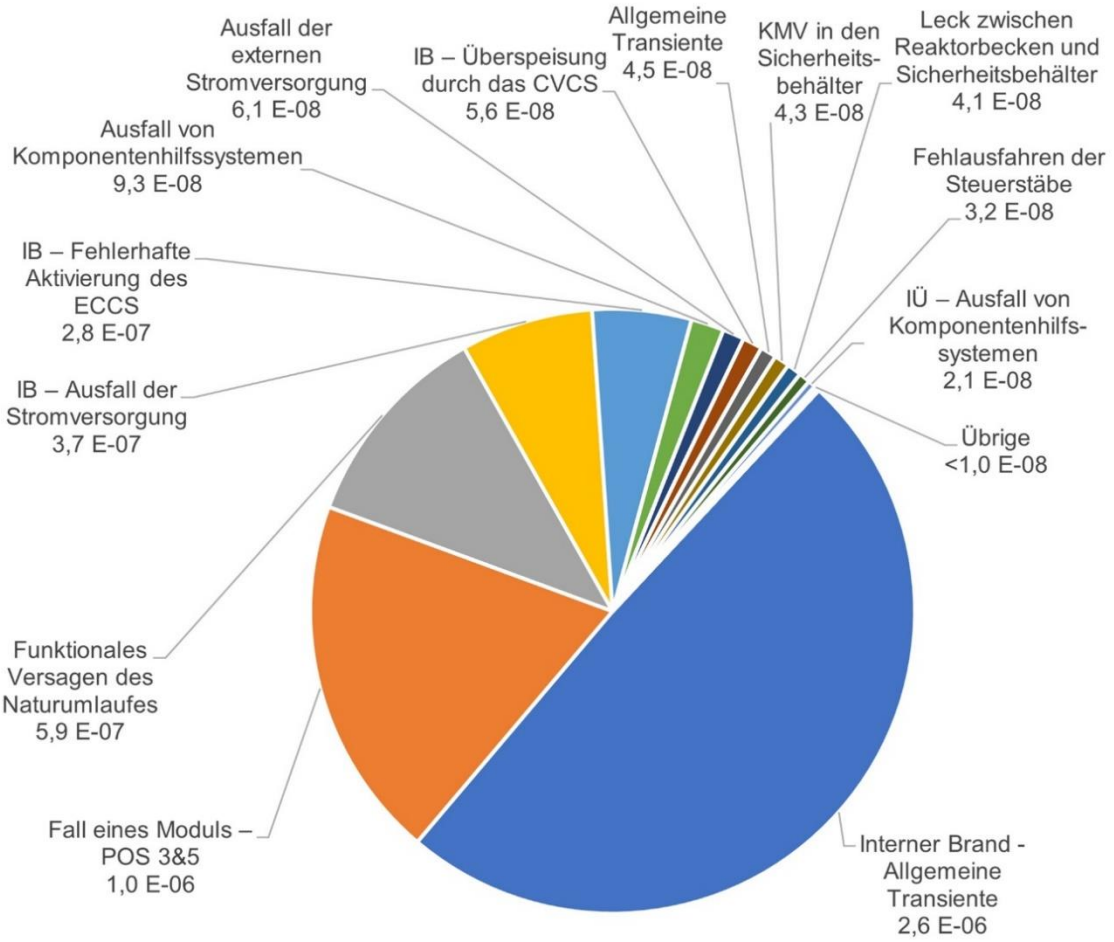


Abb. 11.6 Beiträge der einzelnen auslösenden Ereignisse zur Kernschadenshäufigkeit bei der Mehrblock-PSA

11.4.1 Wichtige Minimalschnitte der PSA für mehrere Reaktormodule

In der Analyse der wichtigsten Minimalschnitte zeigt sich ein besonders wichtiger Minimalschnitt, bei welchem beide Redundanzen des ESFAS durch den Auslöser, ein interner Brand, in sechs Modulen nicht zur Verfügung stehen. In der weiteren Modellierung wird angenommen, dass alle Maßnahmen zur Unfallbeherrschung aufgrund der

Überforderung der Betriebsmannschaft, die alle Notfallmaßnahmen in allen betroffenen Modulen von Hand initiieren muss, nicht ausgeführt werden, d. h. kein DHRS, kein ECCS usw. Die weiteren Minimalschnitte der MUPSA sind überwiegend ähnlich zu den Ergebnissen der SUPSA, allerdings mit häufig zwölffach höheren Eintrittshäufigkeiten für Einzelmodulauslöser. So ist das Gesamtergebnis der MUPSA auch eine Größenordnung über dem Gesamtergebnis der SUPSA.

Tab. 11.5 Minimalschnitte mit dem größten Einfluss auf das MUPSA-Ergebnis, beginnend mit dem einflussreichsten Ereignis

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	Häufigkeit [1/a]
Interner Brand: Allgemeine Transiente in 6 Modulen, Zusatzausfall: beide Redundanzen des ESFAS	Fehlerhafte Durchführung von Handmaßnahmen in mindestens einem Modul			2,4 E-06 (50 %)
Funktionales Versagen des Naturumlaufes	Naturumlauf stabilisiert sich nach RESA nicht			6,0 E-07 (12 %)
Absturz eines Moduls in den Beladebereich, POS5				3,7 E-07 (8 %)
Absturz eines Moduls in den Beladebereich, POS3				3,0 E-07 (6 %)
Absturz eines Moduls in den Operationsbereich, POS5				1,9 E-07 (4 %)
Absturz eines Moduls in den Operationsbereich, POS3				1,5 E-07 (3 %)
Interner Brand: Allgemeine Transiente in allen Modulen	GVA MSIV und Backup-Ventile in 4 Modulen	GVA RSV in 3v4 Modulen		3,9 E-08 (0,8 %)
Interner Brand: Fehlerhafte Aktivierung des ECCS in allen Modulen	GVA RRV IAB blockiert in 4 Modulen	RRV1/2 passive Öffnungsfunktion versagt in allen Modulen	Betriebsmannschaft agiert fehlerhaft 1v4 Module	1,6 E-08 (0,3 %)
Fehlausfahren der Steuerstäbe	GVA Abschaltstäbe fallen nicht ein			1,6 E-08 (0,3 %)
Interner Brand: Überspeisung durch das CVCS	GVA CIV des CES	RSV sprechen im Unfallverlauf an	RSV1 schließt nicht wieder	1,4 E-08 (0,3 %)

1. Ausfall/ Ereignis	2. Ausfall/ Ereignis	3. Ausfall/ Ereignis	4. Ausfall/ Ereignis	Häufigkeit [1/a]
Interner Brand: Fehlerhafte Aktivierung des ECCS in allen Modulen	GVA RRV IAB blockiert in 3 Modulen	RRV1/2 passive Öffnungsfunktion versagt in allen Modulen	Betriebsmannschaft agiert fehlerhaft 1v3 Module	1,0 E-08 (0,2 %)

11.4.2 Besonders relevante Parameterwerte

Die 25 wichtigsten Parameter für die Kernschadenshäufigkeit sind in Tab. 11.6 entsprechend ihres anteiligen Beitrags (fractional contribution) sortiert, beginnend mit dem relevantesten Parameter. Einige Parameter sind bereits aus der PSA für nur ein reaktormodulbekannt und treten hier in einer etwas veränderten Reihenfolge auf. Spezifisch für die PSA für mehrerer Reaktormodule sind u. a. die Fehler der Betriebsmannschaft in einem oder mehreren Modulen und die GVA für das passive Öffnen aller ECCS-Ventile. Vereinfachend wurden (konservative Expertenabschätzung) die GVA für das passive Öffnen der ECCS-Ventile von einem Modul auf alle Module übertragen. Aufgrund der besonderen Relevanz sollte die entsprechende Konservativität aus dieser Modellierung möglichst herausgenommen werden. Interessanterweise finden sich sonst keine GVA über mehrere Module in der Liste der 25 wichtigsten Parameter, diese folgen dann auf den Plätzen 26 bis 29 und 31 bis 32.

Tab. 11.6 Parameterwerte mit hoher Relevanz für die Kernschadenshäufigkeiten in der PSA für mehrere Reaktormodule

Parameter	Parametermittelwert
Interner Brand mit allgemeiner Transiente in 6 Modulen und Ausfall beider Redundanzen des ESFAS	2,4 E-06 /a
Fehler der Betriebsmannschaft in 1v4 Modulen	0,7
Fehlerentdeckungszeit: 1 Monat	6,72 E+02 h
Häufigkeit eines Funktionalen Versagens des RCS (1v12 Modulen)	1,20 E-06 /a
Naturumlauf stabilisiert sich nach Kernabschaltung nicht	0,5
Fehler der Betriebsmannschaft in 2v4 Modulen	0,24
Häufigkeit für den Fall eines Moduls im Beladebereich, POS5	3,10 E-08 /a
GVA passives Öffnen aller ECCS-Ventile	1,00 E-02
RSV spricht im Betrieb des DHRS an	0,5
Häufigkeit für den Fall eines Moduls im Beladebereich, POS3	3,00 E-07 /a

Parameter	Parametermittelwert
Fehlerentdeckungszeit: 5 Monate	3,36 E+03 h
Missionszeit	72 h
Gasturbine BV	2,45 E-03 /h
Interner Brand mit Ausfall der Stromversorgung	6,5 E-02 /a
Häufigkeit für den Fall eines Moduls im Operationsbereich, POS5	1,86 E-07 /a
Interner Brand als Auslöser einer allgemeinen Transiente in allen Modulen	7,88 E-01 /a
Häufigkeit für den Fall eines Moduls im Operationsbereich, POS3	1,50 E-07 /a
Test- und Wartungsintervall: 3 Monate	2,19 E+03 h
GVA Dieselgeneratoren BV	1,50 E-04 /h
Fehler der Betriebsmannschaft in 3v4 Modulen	0,05
Passives Öffnen eines ECCS-Ventils	1,00 E-01
Test- und Wartungsintervall: Abfahren der Anlage	8,76 E+03 h
Test- und Wartungsintervall: 40 Monate	2,92 E+04 h
Wiederöffnen eines geschlossenen Ventils	1,10 E-06 /h
RSV Wiederverschluss nach Öffnung	5,01 E-08 /h

11.4.3 Diskussion der PSA-Ergebnisse für mehrere Reaktormodule

Die Ergebnisse der Mehrblock-PSA lassen einen wesentlichen zusätzlichen Beitrag zur Kernschadenshäufigkeit gegenüber der SUPSA erkennen. Ein interner Brand, der zum Ausfall beider Redundanzen des ESFAS in sechs Modulen führt, birgt die Gefahr einer Überforderung der Betriebsmannschaft. Vereinfacht wurde für diesen Fall eine Fehlerwahrscheinlichkeit von 1 angenommen.

Mit Hilfe einer verbesserten Modellierung der Fehler der Betriebsmannschaft bei gleichzeitigen Anforderungen in mehreren Modulen könnte die Aussagekraft der MUPSA-Ergebnisse erhöhen und Konservativität reduzieren. Darüber hinaus sind die weiter durchzuführenden Überarbeitungspunkte der SUPSA, um an den wesentlichen Stellen die Konservativität der Abschätzungen zu reduzieren, auch für die MUPSA gültig, da die gleichen Minimalschnitte auch in der MUPSA einen wesentlichen Beitrag zur Gesamtkernschadenshäufigkeit zeigen. Aufgrund der wesentlich anderen Methodik zur Abschätzung der Multi-Modul-Kernschadenshäufigkeit von NuScale /NUS 20/ lässt sich kein direkter Vergleich der Ergebnisse bzw. der Minimalschnitte durchführen.

12 Zusammenfassung und Ausblick

Im Rahmen des Forschungs- und Entwicklungsvorhabens RS1596 wurde ein methodischer Ansatz zur Durchführung einer PSA der Stufe 1 für SMR entwickelt. Basierend auf einer repräsentativen Anlage vom Typ SMR mit mehreren Reaktormodulen konnten alle notwendigen Schritte zur Erstellung einer vollständigen Standort-PSA identifiziert werden. Die meisten dieser Schritte hin zu einer Standort-PSA konnten in einem ersten Modell erfolgreich umgesetzt werden.

Darüber hinausgehende fehlende Beiträge, u. a. die Bestimmung der Ausfallraten einiger Komponenten der Eintrittshäufigkeiten verschiedener auslösender Ereignisse, ebenso wie verschiedene Experteneinschätzungen oder die Modellierung der Fehlerwahrscheinlichkeiten der Betriebsmannschaft, wurden mit Hilfe der öffentlich zugänglichen Modellbeschreibung und den PSA-Ergebnissen von NuScale /NUS 20/ ergänzt, um die Qualität des entwickelten eigenen methodischen Ansatzes zu bewerten.

Insbesondere konnten die Ausfallwahrscheinlichkeiten der passiven Systeme nicht vollständig quantifiziert werden, da das thermohydraulische Modell für die Berechnungen nicht vorlag. Allerdings konnten mit Hilfe der entwickelten Methodik die ergebnisrelevanten auslösenden Ereignisse für ein einzelnes Reaktormodul und darüber hinaus die auslösenden Ereignisse, die mehrere Module gleichzeitig betreffen, bestimmt werden.

Die Kernschadenszustände der PSA der Stufe 1, welche die Schnittstelle zu einer PSA der Stufe 2 darstellen, wurden über die möglichen Anlagenendzustände mit Kernschaden oder einem Hochdruckversagen der druckführenden Umschließung festgelegt. Es wurden sieben Endzustände unterschieden, die auch als Basis für eine PSA der Stufe 2 dienen können. Insbesondere werden der Zustand des Sicherheitsbehälters, eine mögliche Umgehung des Sicherheitsbehälters und der Druck im Reaktorkühlsystem (RCS) bei Eintritt des Kernschadens unterschieden.

Des Weiteren wurden Ereignisablaufanalysen zu den auslösenden Ereignissen erstellt und die Systemfunktionen mit Fehlerbaumanalysen unterlegt, um die Eintrittshäufigkeiten für die unterschiedlichen Anlagenendzustände zu bestimmen. Über die Fehlerbäume konnte außerdem die vergleichsweise hohe Zuverlässigkeit der passiven Systeme DHRS, RCS und ECCS quantitativ belegt werden.

Ein erster Ansatz zur Durchführung einer Mehrblock-PSA mit zwölf Reaktormodulen wurde entwickelt und erfolgreich getestet. Damit konnte eine Transiente bzw. ein Minimalschnitt, der einen wesentlichen Beitrag zur Gesamtkernschadenshäufigkeit der Anlage zeigt, ermittelt werden. Wesentliche methodische Ansätze, die dabei verfolgt wurden, waren die Erweiterung der Ausfälle mehrerer Ventile oder Pumpen aus gemeinsamer Ursache in einem Modul zu Komponentengruppen von Ventilen oder Pumpen in mehreren Modulen. Hier konnten die Fachkunde der GRS-Experten sowie die bei der GRS im Zusammenhang mit der Betriebserfahrung deutscher Anlagen vorliegenden GVA-Daten genutzt werden.

Die Methoden und Ergebnisse der PSA für mehrere SMR-Reaktormodule wurden bei der 34th European Conference on Safety and Reliability (ESREL 2024) /OBE 24/ und der IAEA-Konferenz „International Conference on Small Modular Reactors and Their Application“ /OBE 24b/ vorgestellt. Dabei zeigten die Ergebnisse der PSA für mehrere SMR-Module insbesondere einen Minimalschnitt, der in der PSA für ein einzelnes Reaktormodul einen wesentlich geringeren Einfluss auf das Ergebnis hat. Nach einem anlageninternen Brand besteht die Gefahr eines Ausfalls beider Redundanzen des ESFAS in sechs Reaktormodulen, was eine erhebliche Herausforderung für die Betriebsmannschaft bedeutet, da alle Maßnahmen von Hand eingeleitet werden müssen.

Darüber hinaus zeigen in der PSA für mehrere SMR-Module die gleichen Minimalschnitte einen großen Einfluss auf das Gesamtergebnis wie in der PSA für ein einzelnes Reaktormodul. Für einige auslösende Ereignisse, z. B. ein Leck zwischen Sicherheitsbehälter und Reaktorbecken, übersteigt allerdings die Kernschadenshäufigkeit für mehrere Reaktormodule wesentlich die entsprechend summierten Häufigkeiten unabhängiger Module aufgrund der geteilten Systeme und Ausfälle aus gemeinsamer Ursache.

In einigen Punkten ist die von der GRS entwickelte Einzelblock- wie auch die Mehrblock-PSA der Stufe 1 für SMR allerdings noch nicht vollständig ausgereift. Die Methodik zur Quantifizierung der Fehler der Betriebsmannschaft ist bisher zu einfach modelliert und der entsprechende Beitrag zur Gesamtkernschadenhäufigkeit über den Minimalschnitt mit Ausfall beider Redundanzen des ESFAS in sechs Modulen könnte mit einer weniger konservativen Modellierung geringer werden. Des Weiteren werden thermohydraulische Unfallanalysen benötigt, um die Zeitbudgets für Handmaßnahmen und die Zuverlässigkeit der Naturumläufe zu quantifizieren. Entsprechende Entwicklungsarbeiten sind bereits ebenso wie die Erweiterung dieser PSA der Stufe 1 um eine PSA der Stufe 2 geplant.

Literaturverzeichnis

/ALR 22/ Alrammah, I.: Application of probabilistic safety assessment (PSA) to the power reactor innovative small module (PRISM), Nuclear Engineering and Technology, 54, 3324-3335, April 2022.

/ANV 15/ Authority for Nuclear Safety and Radiation Protection (ANVS): Safety Guidelines, Guidelines on the Safe Design and Operation of Nuclear Reactors, Den Haag, Niederlande, April 2023, https://english.autoriteitnvs.nl/topics/guidelines-on-the-safe-design-and-operation-of-nuclear-reactors/documents/publication/2023/04/05/guidelines-safe-design-and-operation-of-nuclear-reactors-and-dsr.

/BAE 18/ Bäckström, O., et al.: SITRON – Site risk assessment approach developed for Nordic countries, in: Proceedings of 14th International Probabilistic Safety Assessment and Management Conference (PSAM14), Los Angeles, CA, USA, September 2018.

/BEC 17/ Becker, B.: Methoden zur Zuverlässigkeitsbewertung passiver Systeme, Bericht zum Vorhaben 3614R01520, AP 8: Wissenschaftlich-technische Untersuchungen zur nuklearen Sicherheit und Wirksamkeit regulatorischer Systeme im Ausland (insbesondere in Osteuropa und bei INSC-Partnern) – Reaktorbaulinien und Wissensnetze, GRS-V-3614R01520-1/2017, Köln, Januar 2017.

/BMU 05/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU): Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes - Leitfaden Probabilistische Sicherheitsanalyse, 31. Januar 2005, Bekanntmachung vom 30. August 2005, Bundesanzeiger, Jahrgang 57, Nummer 207a, ISSN 0720-6100, 3. November 2005, https://www.bfe.bund.de/SharedDocs/Downloads/BfE/DE/rsh/3-bmub/3_74_3.pdf?__blob=publicationFile&v=1.

/BMU 15/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB): Sicherheitsanforderungen an Kernkraftwerke, Bekanntmachung vom 3. März 2015, BAnz AT 30.02.2015 B2, https://www.base.bund.de/SharedDocs/Downloads/BASE/DE/rsh/3-bmub/3_0_1.pdf?__blob=publicationFile&v=1.

/BOA 14/ Boarin, S., M: E. Ricotti: An Evaluation of SMR Economic Attractiveness, Science and Technology of Nuclear Installations, 1-8, 2014, https://onlinelibrary.wiley.com/doi/pdf/10.1155/2014/803698.

/BOT 18/ Botha, D., B. Bristol, A. Callaway: Shutdown Capability of the NuScale Power Module, NuScale Power LLC, Corvallis, Oregon, Vereinigte Staaten von Amerika, Januar 2018, https://www.nrc.gov/docs/ML1801/ML18019A161.pdf.

/BUC 15/ Buchholz, S., D. von der Cron, A. Schaffrath: System codes improvements for modelling passive safety systems and their validation, in: Proceedings of Eurosafe Forum 2015, European Technical Safety Organisations Network (ETSON), Brüssel, Belgien, November 2015.

/BUC 15a/ Buchholz, S., et al.: Studie zur Sicherheit und zu internationalen Entwicklungen von Small Modular Reactors (SMR), GRS-376, ISBN 978-3-944161-57-0, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Mai 2015, https://www.grs.de/sites/default/files/publications/grs-376.pdf.

/BUC 16/ Buchholz, S., D. von der Cron, A. Schaffrath: System code improvements for modelling passive safety systems and their validation, Kerntechnik 81, S. 535-542, München, 2016.

/DAU 05/ D'Auria, F.: Natural circulation and boron dilution process in PWR, 2nd CRP RCM, Corvallis, OR, USA, 29. August – 2. September 2005.

/DOY 20/ Doyle, J., et al.: Highly Available Nuclear Power for Mission-Critical Applications, Nuclear Technology, 206:7, S. 1059-1074, Februar 2020, DOI: 10.1080/00295450.2019.1699382.

/DOY 21/ Doyle, J.: Highly Available Nuclear Power in Microgrid Configuration for the ORNL Distribution System, Nuclear Technology, 208:6, S. 1012-1026, November 2021, DOI: 10.1080/00295450.2021.1985912.

/FAK 05/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, ISBN 3-86509-414-7, Bundesamt für Strahlenschutz (BfS), Salzgitter, Oktober 2005, https://doris.bfs.de/jspui/handle/urn:nbn:de:0221-201011243824.

/FAK 05a/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BfS-SCHR-38/05, ISBN -86509-415-5Bundesamt für Strahlenschutz (BfS), Salzgitter, Oktober 2005, https://doris.bfs.de/jspui/handle/urn:nbn:de:0221-201011243838.

/FAK 16/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden und Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: Mai 2015, BfS-SCHR-61/16, Bundesamt für Strahlenschutz (BfS), Salzgitter, September 2016, https://doris.bfs.de/jspui/handle/urn:nbn:de:0221-2016091314090.

/HAG 21/ Hage, M., G. Mayer, M. Röwekamp: Vorgehen bei Erweiterungen einer Site-Level PSA bis hin zur Stufe 2, Technischer Fachbericht, GRS-637, ISBN: 78-3-949088-26-1, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Juli 2021, https://www.grs.de/publikationen/grs-637.

/HAN 18/ Han, S. H., et al.: AIMS-MUPSA software package for multi-unit PSA, Nuclear Engineering and Technology, 50, S. 1255-1265: Juni 2018.

/HEN 19/ Henneke, D., J. Li: Simplified Methodology for Multi-Unit Probabilistic Safety Assessment (PSA) Modelling, in: Proceedings of ANS PSA 2019 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Charleston, SC, USA, April 27 – May 3, 2019, on CD-ROM, American Nuclear Society, LaGrange Park, IL, USA, 2019.

/IAE 91/ International Atomic Energy Agency (IAEA): Safety related terms for advanced nuclear plants, IAEA-TECDOC-626, ISSN 1011-4289, Wien, September 1991, https://www-pub.iaea.org/MTCD/Publications/PDF/te_626_web.pdf.

/IAE 05/ International Atomic Energy Agency (IAEA): Natural circulation in water cooled nuclear power plants – Phenomena, models, and methodology for system reliability assessment, IAEA-TECDOC-1474, ISBN 92-0-110605-X, Wien, November 2005, https://www-pub.iaea.org/MTCD/Publications/PDF/TE_1474_web.pdf.

/IAE 12/ International Atomic Energy Agency (IAEA): Natural Circulation Phenomena and Modelling for Advanced Water Cooled Reactors, IAEA-TECDOC-1677, ISBN 978-92-0-127410-6, Wien, März 2012, https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1677_web.pdf.

/IAE 14/ International Atomic Energy Agency (IAEA): Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors, IAEA-TECDOC-1752, ISBN 978-92-0-108614-3, Wien, September 2014, https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1752_web.pdf.

/IAE 16/ International Atomic Energy Agency (IAEA): Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (Rev. 1), TI/PUB/1715, ISBN 978–92–0–109315–8, Wien, Februar 2016, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf.

/IAE 16a/ International Atomic Energy Agency (IAEA): Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (Rev. 1), TI/PUB/1715, ISBN 978–92–0–109315–8, Wien, Februar 2016, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf.

/IAE 17/ International Atomic Energy Agency (IAEA): Instrumentation and Control Systems for Advanced Small Modular Reactors, IAEA Nuclear Energy Series, No. NP-T-3.19, STI/PUB/1770, ISBN 978-92-0-101217-3, Wien, Juli 2017, https://www-pub.iaea.org/MTCD/Publications/PDF/P1770_web.pdf.

/IAE 18/ International Atomic Energy Agency (IAEA): Advances in Small Modular Reactor Technology Developments, A Supplement to: IAEA Advanced Reactors Information System (ARIS), Wien, September 2018, https://aris.iaea.org.

/IAE 19/ International Atomic Energy Agency (IAEA): Technical approach to probabilistic safety assessment for multiple reactor units, Safety Reports Series, No. 96, STI/PUB/1820, ISBN 978-92-0-102618-7, Wien, Mai 2019, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1820_web.pdf.

/IAE 21/ International Atomic Energy Agency (IAEA): Multi-unit probabilistic safety assessment, IAEA Safety Reports Series No. 110, Wien, 2021, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1974_web.pdf.

/IAE 21a/ International Atomic Energy Agency (IAEA): Technology Roadmap for Small Modular Reactor Deployment, IAEA Nuclear Energy Series, No. NR-T-1.18, STI/PUB/1944, ISBN 978-92-0-110021-4, Wien, August 2021, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1944_web.pdf.

/IAE 24/ International Atomic Energy Agency (IAEA): Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, IAEA Safety Standards Series No. SSG-3, Rev. 1, STI/PUB/2056, ISBN 978-92-0-130723-1, Wien, März 2024, https://www-pub.iaea.org/MTCD/Publications/PDF/p15318-PUB2056_web.pdf.

/JAN 18/ Jang, S., Y. Seo, M. Jae: A Case study of Methodology for Common Cause Failure modelling in Multi-unit PSA model, Transactions of the Korean Nuclear Society Autumn Meeting, Yeosu, Republik Korea, Oktober 2018.

/KIM 00/ Kim, S. J.: Turbulent film condensation of high pressure steam in a vertical tube of passive secondary condensation system, Dissertation, Korea Advanced Institute of Science and Technology, Republik Korea, Februar 2000.

/KIM 18/ Kim, D.-S., et al.: Multi-unit Level 1 probabilistic safety assessment: Approaches and their application to a six-unit nuclear power plant site, Nuclear Engineering and Technology, 50, S. 1217-1233: Januar 2018.

/KIM 20/ Kim, D.-S., J: H. Park, H.-G. Lim: A pragmatic approach to modeling common cause failures in multi-unit PSA for nuclear power plant sites with a large number of units, Reliability Engineering & System Safety, Vol. 195, S. 106739, März 2020.

/LIM 18/ Lim, H.-G., et al.: Development of logical structure for multi-unit probabilistic safety assessment, Nuclear Engineering and Technology, 50, S. 1210-1216: Oktober 2018.

/LIN 01/ von Linden, J., et al.: Bewertung des Unfallrisikos fortschrittlicher Druckwasserreaktoren in Deutschland, Methoden und Ergebnisse einer umfassenden Probabilistischen Sicherheitsanalyse (PSA), GRS-175, ISBN 3-931995-43-7, Köln, Oktober 2001.

/LYU 11/ Lyubarskiy, A., I. Kuzmina, M. El-shanawany: Notes on Potential Areas for Enhancement of the PSA Methodology Based on Lessons Learned from the Fukushima Accident, In: UK’s 2nd Probabilistic Safety Analysis/Human Factors Assessment Forum, The Park Royal Hotel, Warrington, Großbritannien, 8. – 9. September 2011.

/MAR 05/ Marquès, M., et al.: Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment, Nuclear Engineering and Design 235, 2612-2631, April 2005.

/MEZ 14/ Mezio, F., et al.: Overview of two CAREM Passive Safety System Functional Reliability Assessments, using RMPS methodology, SOP Transactions on statistics and analysis, Vol. 1, No. 2, Scientific Online, Juli 2014.

/MUE 04/ Müller, C., H. Glaeser: Zuverlässigkeitsmethoden für passive Sicherheitsfunktionen, Abschlussbericht zum Vorhaben RS1131, GRS-A-3179, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Januar 2004.

/NAY 07/ Nayak, A. K., et al.: Passive system reliability analysis using the APSRA methodology, Nuclear Engineering and Design 238, S. 1430-1440, November 2007.

/NAY 09/ Nayak, A. K., et al.: Reliability assessment of passive isolation condenser system of AHWR using APSRA methodology, Reliability Engineering and System Safety 94, S. 1064-1075, Januar 2009.

/NIE 17/ Niedrée, D., H. Schmidt: Beschreibung der kleinen und modularen Reaktorkonzepte CAREM-25, SMART, NuScale und Westinghouse SMR, Technische Notiz, GRS - V - 3614R01510 - 01/2017, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Juni 2017.

/NIE 17a/ Niedrée, D.: Herausforderungen bei der Realisierung von kleinen, modularen Reaktoren (SMR), Technical Note, GRS - V - 3614R01520 - 03/2017, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Mai 2017.

/NUS 19/ NuScale Power LLC: Long-Term Cooling Methodology, Licensing Technical Report, TR-0916-51299-NP, Revision 1, Corvallis, OR, USA, August 2019, © NuScale Power, LLC, https://www.nrc.gov/docs/ML1921/ML19218A147.pdf.

/NUS 20/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 19: Probabilistic Risk Assessment and Severe Accident Evaluation, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A508.pdf.

/NUS 20a/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 7: Instrumentation and Controls, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A495.pdf.

/NUS 20b/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 15: Transient and Accident Analyses, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A504.pdf.

/NUS 20c/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 5: Reactor Coolant System and Connecting Systems, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A493.pdf.

/NUS 20d/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 9: Auxiliary Systems, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A498.pdf.

/NUS 20e/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 6: Engineered Safety Features, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A494.pdf.

/NUS 20f/ NuScale Power LLC: Non-Loss-of-Coolant Accident Analysis Methodology, NuScale Topical Report TR-0516-49416, Revision 3, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2018/ML20181A431.pdf.

/NUS 20g/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 3: Design of Structures, Systems, Components and Equipment, Revision 3, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20225A154.html.

/NUS 20h/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 1: Introduction and General Description of the Plant, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A481.pdf.

/NUS 20i/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 10: Steam and Power Conversion System, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A499.pdf.

/NUS 20j/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 8: Electric Power, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A497.pdf.

/NUS 20k/ NuScale Power LLC: NuScale Standard Plant Design Certification Application, Part 2, Chapter 4: Reactor, Revision 5, Corvallis, OR, USA, Juli 2020, © NuScale Power, LLC, https://www.nrc.gov/docs/ML2022/ML20224A492.pdf.

/OBE 24/ Obergfell, M., F. Berchtold: Small Modular Reactor Multi-Module PSA, in: Advances in Reliability, Safety and Security, ESREL 2024 Contributions, Part 1 – Part 10, Academic Press Book Series, Krakau, Polen, Juni 2024.

/OBE 24a/ Obergfell, M., et al.: Erweiterung des Quelltermprognosewerkzeugs FaST-Pro zu Planung anlagenexterner Notfallmaßnahmen unter Berücksichtigung aller Radionuklidquellen an einem Kernkraftwerksstandort, Technischer Bericht, GRS-782, ISBN 978-3-910548-75-6, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, September 2024, https://www.grs.de/sites/default/files/2025-09/GRS-782.pdf.

/OBE 24b/ Obergfell, M., F. Berchtold.: Small Modular Reactor Multi-Module PSA, in: Proceedings of the International Conference on Small Modular Reactors and their Applications, International Atomic Energy Agency (IAEA), Wien, in Vorbereitung, 2024.

/PIS 21/ Pistner, C., et al.: Sicherheitstechnische Analyse und Risikobewertung einer Anwendung von SMR-Konzepten (Small Modular Reactors), BASE-Forschungsberichte zur Sicherheit der nuklearen Entsorgung, Berlin, März 2021, https://www.base.bund.de/shareddocs/downloads/de/berichte/kt/gutachten-small-modular-reactors.html.

/QUE 14/ Quester, C., et al.: Störungen im Stromnetz und Notstromfälle in Kernkraftwerken in den Jahren 2003 bis 2012, GRS-317, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Juli 2014, https://www.grs.de/sites/default/files/publications/grs-317.pdf.

/SCH 89/ Schäfer, H.: Auswertung von amerikanischen PRA-Richtlinien zur Bewertung abhängiger Ausfälle (Common Cause Failure) in probabilistischen Sicherheitsanalysen, GRS-A-1608, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, August 1989.

/SCH 19/ Schaffrath, A., S. Buchholz: SMRs - Overview on International Developments and Safety Features, atw, International Journal for Nuclear Power, 6,7, S. 336-347, Juli 2019.

/SCH 20/ Schmidt, H.: Konzeptbeschreibung NuScale, Technical Note, Bericht zum Vorhaben 4717R01520, AP 4, GRS – V – 4717R01520, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, März 2020.

/SCH 21/ Schaffrath, A.: Kleine modulare Reaktoren (SMRs), Folienpräsentation als Beitrag zur Online-Veranstaltung „SMRs und andere neue Reaktoren“, Kerntechnische Gesellschaft, Fachgruppe Betrieb und Sicherheit, Mai 2021.

/SCH 21a/ Schmidt, H.: NuScale Power, Seminar zu „Neue Reaktoren: Konzepte und Bauprojekte“, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, März 2021.

/SMI 12/ Smith, C., et al.: A Framework to Expand Advanced Probabilistic Risk Assessment to Support Small Modular Reactors, INL/EXT-12-27345, Idaho National Laboratory (INL), Idaho Falls, ID, USA, September 2012.

/SMI 13/ Smith, C., et al.: Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) Detailed Technical Framework Specification – Describing the framework to support the implementation of a state-of-the-art PRA to predict the performance of safety, security, and safeguards of SMRs, INL/EXT-13-28974, Idaho National Laboratory (INL), Idaho Falls, ID, USA, April 2013.

/SMI 14/ Smith, C., S. Prescott, S, Koonce: Advanced Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) Demonstration, INL/EXT-14-31876, Idaho National Laboratory (INL), Idaho Falls, ID, USA, April 2014.

/STU 14/ Stutzke, M. A.: Scoping estimates of multiunit accident risk, in: Proceedings of 12th International Probabilistic Safety Assessment and Management Conference (PSAM12), Honolulu, HI, USA, Juni 2014, https://www.iap-sam.org/psam12/proceedings/paper/paper_96_1.pdf.

/STU 17/ Stuart, N.: Rapid reaction: small factory-built nuclear reactors could be delivered by lorry, The Engineer, März 2017, https://www.theengineer.co.uk/rapid-reaction-the-small-factory-built-nuclear-reactors-could-be-delivered-on-the-back-of-a-lorry/.

/SWA 83/ Swain, A. D., H: E. Guttmann: Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Application, Final Report, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories (NIST), Albuquerque, NM und Livermore, CA, USA, August 1983, https://www.nrc.gov/docs/ML0712/ML071210299.pdf.

/UMM 10/ Umminger, K., T. Mull, B. Brand: Integralversuche in der PKL-Anlage mit internationaler Beteiligung, atw 55, Jg., Heft 3, S. 162-167, März 2010.

/UPA 13/ Upadhyaya, B. R., et al.: Remote monitoring of equipment in small modular reactors, Chem. Eng. Tran. 33, 2013.

/VGB 12/ VGB PowerTech e.V.: Zentrale Zuverlässigkeits- und Ereignisdatenbank – Zuverlässigkeitskenngrößen für Kernkraftwerkskomponenten, TW 805-13, Essen, Dezember 2012.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

APSRA	Englisch: assessment of passive system reliability; Methode zur Bestimmung der Zuverlässigkeit eines passiven Systems
ATWS	Englisch: anticipated transient without scram; Transiente ohne RESA, Ausfall der RESA
BMU	Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit
BMUV	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
BMWi	Bundesministerium für Wirtschaft und Energie
BWR	Englisch: Boiling Water Reactor; Siedewasserreaktor
CDF	Englisch: core damage frequency; Kernschadenshäufigkeit
CDP	Englisch: core damage probability; Kernschadenswahrscheinlichkeit
CES	Englisch: containment evacuation system; Sicherheitsbehälter-Vakuumsystem
CF	Erfolgreiche Wärmeabfuhr über den Sicherheitsbehälter mit Hilfe der Sicherheitsbehälterflutung mit dem Flut- und Drainagesystem CFDS
CFDS	Englisch: containment flooding and drain system; Flut- und Drainagesystem des NuScale-SMR-Sicherheitsbehälters
CIS	Englisch: containment isolation system; Sicherheitsbehälterabschlusssystem
CIV	Sicherheitsbehälterabsperrventil (Englisch: Containment Isolation Valve)
CVCS	Volumenregelsystem des NuScale-SMR (Englisch: Chemical and Volume Control System)
DE	Dampferzeuger (Englisch: Steam Generator)
DHRS	Englisch: decay heat removal system; Nachzerfallswärmeabfuhrsystem des NuScale-SMR
DWR	Druckwasserreaktor
EC	Erfolgreiche Wärmeabfuhr durch das ECCS
ECCS	Englisch: emergency core cooling system; Notkühlsystem
EDSS	Englisch: highly reliable DC power system; hochzuverlässiges Gleichstromnetz
EHVS	Englisch: 13.8 kV and switchyard system; Hochspannungs-Wechselstromnetz mit 13,8 kV und Umschaltanlage
ELVS	Englisch: low voltage AC electrical distribution system; Niederspannungs-Wechselstromnetz
EMVS	Englisch: medium voltage AC electrical distribution system; Mittelspannungs-Wechselstromnetz
ESFAS	Englisch: engineered safety features actuation system; System zur automatischen Auslösung von Sicherheitsfunktionen
FD	Englisch: main steam; Frischdampf

FDF	Englisch: fuel damage frequency; Brennstabschadenshäufigkeit
FDP	Englisch: fuel damage probability; Brennstabschadenswahrscheinlichkeit
FWIV	Englisch: feedwater isolation valve; Speisewasserabsperrventil
GDCS	Passives Kühlsystem zur Kernkühlung des SBWR von GE
GE	General Electric
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
GVA	gemeinsam verursachter Ausfall (Englisch: common cause failure (CCF))
HD	Hochdruck
HR	Erfolgreiche Wärmeabfuhr durch das DHRS
IAB	Englisch: inadvertent actuation block; Schutz vor unbeabsichtigter Aktivierung der Notkühlung
IE	Englisch: initiating event; auslösendes Ereignis
KMV	Kühlmittelverluststörfall (Englisch: loss of coolant accident (LOCA))
KS	Kernschaden
KSZ	Kernschadenszustand
LBLOCA	Kühlmittelverlust durch ein großes Leck im Reaktorkühlsystem
LTOP	Englisch: low temperatur overpressure protection; Überdruckschutz des RCS bei niedrigen Temperaturen, Sprödbruchabsicherung
MSIV	Englisch: main steam isolation valve; Frischdampfabsperrventil
MUCDF	Englisch: multi-unit core damage frequency; Mehrblock-Kernschadenhäufigkeit
MUPSA	Englisch: Multi-Unit PSA; PSA für mehrere Reaktorblöcke an einem Standort
NLB	Nichtleistungsbetrieb
NPM	NuScale Power Modules
PCCS	Passives Sicherheitskühlsystem des SBWR von GE
POS	Englisch: plant operational state; Anlagenbetriebszustand
PSA	Probabilistische Sicherheitsanalyse
RBMK	Siedewasser-Druckröhrenreaktor sowjetischer Bauart
RCS	Englisch: reactor coolant system; Reaktorkühlsystem, bestehend aus dem RDB, dem Primärkühlkreislauf, dem Druckhalter, zwei Dampferzeugern, den Reaktoreinbauten und den zugehörigen Ventilen
RDB	Reaktordruckbehälter (Englisch: Reactor Pressure Vessel (RPV))
RESA	Englisch: rector scram; Reaktorschnellabschaltung
RMPS	Zuverlässigkeitsmethoden für passive Sicherheitsfunktionen (ausführlich in /BEC 17/ und /MUE 04/ beschrieben)
RRV	Englisch: reactor recirculation valve; ECCS-Rücklaufventil
RSV	Englisch: reator safety valve; Reaktorsicherheitsventil

RTS	Englisch: reactor trip system; Reaktorabschaltsystem, System zur Ausführung einer RESA
RVV	Englisch: reactor vent valve; ECCS-Abblaseventil
SB	Sicherheitsbehälter (Englisch: Containment oder Containment Vessel)
SBLOCA	KMV durch ein kleines Leck im RCS
SBO	Englisch: station black-out; Ausfall der externen Stromversorgung und aller Stromgeneratoren
SBWR	Englisch: Simplified Boiling Water Reactor (von GE)
SCDF	Englisch: site core damage frequency; Standort-Kernschadenhäufigkeit
SMR	Englisch: small modular reactor; kleiner modularer Kernreaktor
SP	Englisch: suppression pool (des SBWR von GE)
SUCDF	Einzelblock-Kernschadenhäufigkeit (von)
SUPSA	Englisch: Single-Unit PSA; PSA für einen einzelnen Reaktorblock an einem Standort
SWR	Siedewasserreaktor
UHS	Englisch: ultimate heat sink; Wärmesenke bestehend aus den zusammengeschlossenen Wasserbecken: dem Reaktor-, Brennelementlager- und Brennelementwechselbecken
VC	Erfolgreiche Kernkühlung mit Hilfe einer Einspeisung über das CVCS mit Wärmeabfuhr in den Sicherheitsbehälter
VVER	Druckwasserreaktor sowjetischer Bauart

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-910548-74-9