RSK-Stellungnahme

(492. Sitzung der Reaktor-Sicherheitskommission (RSK) am 22.03.2017)

Randbedingungen der Nachweisführung zur Störfallbeherrschung

Inhaltsverzeichnis

1 Beratungsauftrag des BMUB und Beratungsgang

In seiner 106. Sitzung am 16.04.2015 war der RSK-Ausschuss ANLAGEN- UND SYSTEMTECHNIK (AST) über den Beratungsauftrag des BMUB zu Sicherheitsanforderungen an Kernkraftwerke zur Beherrschung des Auslegungsstörfalls „Dampferzeuger-Heizrohrleck“ informiert worden. Im Beratungsauftrag [1] bittet das BMUB die RSK um eine schriftliche Stellungnahme zu den Anforderungen an die Nachweisführung eines Ereignisses der Sicherheitsebene 3 (Störfallanalyse) und den hierbei zu unterstellenden Anfangs- und Randbedingungen, insbesondere:

1 Bis zu welchem Anlagenzustand sollte die Nachweisführung erfolgen?

2 Inwieweit können im Rahmen der Nachweisführung Nicht-Sicherheitssysteme (einschließlich von durch das Begrenzungssystem angeforderten Aktionen, wie dies z. B. beim DEHL[1] der Fall ist) in den verschiedenen Phasen nach Eintritt des Störfalls kreditiert werden (gegebenenfalls mit Festlegung von zugehörigen Bedingungen)?

   Wie sind hierbei Nicht-Sicherheitssysteme zu behandeln, die zum Zeitpunkt des Ereigniseintritts in Betrieb sind, auslegungsgemäß nicht abgeschaltet werden und den Ereignisablauf günstig oder ungünstig beeinflussen?

3 In welcher Art und Weise sind mögliche Fehlhandlungen bzw. Unterlassungen von im BHB vorgesehenen Handlungen in den Nachweisführungen zu berücksichtigen?

4 In welchem Umfang sollten die im Rahmen der Nachweisführung festgelegten Randbedingungen und betrachtete Szenarien in die Störfallkapitel des BHB einfließen?

Zur Vorbereitung der weiteren Beratung wurde in der 107. Sitzung des Ausschusses am 28.05.2015 die Ad-hoc-AG DEHL II mit der Erarbeitung eines Entwurfs für eine Stellungnahme beauftragt. Die AG ist diesem Auftrag in fünf Sitzungen nachgekommen, der Ausschuss AST verabschiedete die Stellungnahme in seiner 119. Sitzung am 13.10.2016. Die RSK beriet und verabschiedete die Stellungnahme in ihrer 492. Sitzung am 22.03.2017.

2 Sachstand

2.1 Konzept zur Störfallbehandlung und Nachweisführung bei der Errichtung der Anlagen

2.1.1 Wesentliche Prinzipien (am Beispiel DWR)

Bei der Auslegung der Anlagen, die heute noch für den Leistungsbetrieb zugelassen sind, lagen dem Konzept für die Störfallbeherrschung unter anderem folgende Prinzipen zugrunde [3]:

[1] Dampferzeugerheizrohrleck.

1 Nachweise zur Einhaltung der Nachweiskriterien für Auslegungsstörfälle:

- Für die Phase der Stabilisierung des Anlagenzustands:
  - Kreditierung nur von Sicherheitssystemen (unter Berücksichtigung der Postulate für die Unverfügbarkeit von Einrichtungen); für spezielle Störfallvarianten, die sich aus Ausfallpostulaten ergeben können, auch Kreditierung von Funktionen des Begrenzungssystems,
  - Automatische Ansteuerung mindestens derjenigen Funktionen, die innerhalb < ½ h zur Störfallbeherrschung erforderlich sind,
  - Bei Handmaßnahmen mit geringen Karenzzeiten jenseits ½ h spezielle Alarmierung („Sicherheitsgefahrenmeldung“, z. B. beim DWR bei kleinen Lecks am Primärkreis und Dampferzeugerheizrohrlecks).

- Für die Phasen der Stabilisierung der Anlage bis in den Zustand „kalt, drucklos“:
  - Kreditierung von Sicherheitssystemen, bei großen Karenzzeiten (d.h. ausreichend Zeit zum Erkennen, Analysieren, Umsetzen) und ereignisspezifisch zu erwartender Verfügbarkeit und Wirksamkeit auch Kreditierung von Nicht-Sicherheitssystemen,
  - Grundsätzlich Ansteuerung der Funktionen von Hand.

2 Vorgelagerte Nachweise zur Minimierung der Aktivitätsfreisetzung bei speziellen Störfällen (beim DWR insbesondere beim DEHL) oder zum optimierten Abfahren der Anlage:

- Kreditieren aller – den Sicherheitssystemen vorgelagerten – Funktionen, deren Verfügbarkeit ereignisspezifisch zu erwarten ist (typischerweise gestaffelter Einsatz),
- Typischerweise automatische Ansteuerung dieser Funktionen für den Zeitraum < ½ h.

Die konkrete Anwendung dieser Prinzipien wird im folgenden Abschnitt am Beispiel eines komplexeren Störfalls, dem Dampferzeugerheizohrleck (DEHL) beim DWR, erläutert.

2.1.2 Störfallbehandlung und Nachweisführung beim Dampferzeugerheizohrleck

Im Gegensatz zu den anderen Ereignissen auf der Sicherheitsebene 3 ist beim Störfall DEHL die Trennung zwischen Primär- und Sekundärseite lokal aufgehoben: Es kommt zu einem Übertrag aktivitätsführenden Kühlmittels aus dem Primärkreis (PK) auf die Sekundärseite des defekten Dampferzeugers (DE) und es stellt sich somit zusätzlich zur eigentlichen Ereignisbeherrschung die verfahrenstechnische Aufgabe, die Aktivitätsfreisetzung an die Umgebung zu minimieren.

Dieser Besonderheit wurde bei der Entwicklung des Beherrschungskonzepts für Heizrohrlecks durch die Formulierung ereignisspezifischer Auslegungsziele Rechnung getragen [3], insbesondere durch Optimierung der Störfallbeherrschung derart, dass mit dem Erkennen eines Heizrohrlecks durch den Reaktorschutz vorgelagert über das Begrenzungssystem betriebliche Einrichtungen angesteuert werden, um die Transiente möglichst abzufangen, bevor vom Reaktorschutz solche Sicherheitseinrichtungen angesteuert werden, deren Funktion ungünstig ist für eine Minimierung der Aktivitätsfreisetzung. Dies wird erreicht durch eine

- Minimierung der Eintrittswahrscheinlichkeit für die Anregung der Notkühlkriterien (und damit einer Erhöhung der Leckrate in den defekten DE).

- Entlastung der Schichtmannschaft von der Notwendigkeit, ggf. aktivierte HD-Sicherheitseinspeisepumpen unter Zeitdruck von Hand abschalten zu müssen.

- Minimierung der Ansprechhäufigkeit der Frischdampfabblase-Ventile am defekten DE.

- Vermeidung des Notstromfalls (und damit der Nichtverfügbarkeit von Turbinenkondensator und Hauptkühlmittelpumpen) durch Lastreduktion vor RESA.

Um eine in radiologischer Hinsicht optimierte Störfallbehandlung durch die Schichtmannschaft zu erzielen, werden in den Betriebshandbüchern verschiedene Fälle unterschieden, welche bezüglich der möglichen Randbedingungen bei einem Heizrohrleck einen geeigneten Rahmen aufspannen (vgl. [4], Kap. 5.2):

- Heizrohrleck ohne Notstromfall, ohne Anregung der Notkühlkriterien,
- Heizrohrleck ohne Notstromfall, mit Anregung der Notkühlkriterien,
- Heizrohrleck mit Notstromfall, ohne Anregung der Notkühlkriterien und
- Heizrohrleck mit Notstromfall, mit Anregung der Notkühlkriterien.

Für den letztgenannten Fall gliedert sich die Störfallbehandlung in drei Phasen mit folgenden Zielen:

- Phase 1: Stabilisierung des Anlagenverhaltens, Beenden der Aktivitätsfreisetzung in die Umgebung durch Isolation des defekten DE.

- Phase 2: Halten der Anlage im Zustand „unterkritisch, heiß“ bis die Netzversorgung wieder hergestellt ist.

- Phase 3: Überführen der Anlagen in den Zustand „kalt, drucklos“.

Zu Phase 1:

In Phase 1 wird durch Einrichtungen des Sicherheitssystems die Erfüllung der Schutzziele sichergestellt:

- Reaktorschnellabschaltung (RESA),

- Beenden der Aktivitätsfreisetzung in die Umgebung durch Angleichen des Primärdrucks an den sekundärseitigen Druck mit Isolation des defekten DE und

- Abfuhr der Nachzerfallsleistung über die intakten Dampferzeuger.

Das Ausmaß der Aktivitätsfreisetzung über den defekten DE hängt neben der vorhandenen Nachzerfallsleistung auch davon ab, wie schnell der Druckausgleich Primär-/Sekundärseite erreicht wird und inwieweit die Dampfabgabe aus dem defekten DE sowie ein Füllstandsanstieg dort begrenzt werden können. Im Sinne einer Minimierung der Aktivitätsfreisetzung sind daher Maßnahmen realisiert worden (z. B. raschere Druck-

absenkung im PK durch Nutzung der betrieblichen Sprühfunktionen), mit deren Hilfe der Druckausgleich und die Beendigung der Dampfabgabe aus dem defekten DE schneller erreicht werden können als bei ausschließlicher Nutzung von Sicherheitseinrichtungen. Es werden also betriebliche Einrichtungen vorgelagert oder zusätzlich zu Sicherheitseinrichtungen genutzt, wobei die betrieblichen Einrichtungen nicht die Funktion der Sicherheitseinrichtungen beeinträchtigen dürfen.

Am Ende von Phase 1 hat sich ein stationärer Anlagenzustand eingestellt, in dem die Nachweiskriterien bzgl. der Schutzziele Kontrolle der Reaktivität, Kühlung der Brennelemente und Einschluss radioaktiver Stoffe erfüllt sind.

Zu Phase 2:

Bei alleiniger Berücksichtigung der Deionatvorräte in den Notspeisebecken (somit über das Sicherheitssystem) kann die Anlage mindestens 10 h im Zustand „unterkritisch, heiß“ verbleiben. Aufgrund der Notstromversorgung der An- und Abfahrpumpe(n) wird im Störfallbehandlungskonzept jedoch zunächst angenommen, dass auch die gesicherten Deionatvorräte im Speisewasserbehälter und in den Deionatbehältern zur Dampferzeugerbespeisung verfügbar sind. Unter dieser Annahme ergibt sich, dass der Mindestdeionatvorrat von 800 Mg innerhalb der ersten 24 Stunden nach Störfallbeginn nicht unterschritten wird.

Entsprechend wird die Wiederherstellung der Netzversorgung erwartet, bevor ein Unterschreiten des Mindestdeionatvorrats das Abfahren der Anlage in den Zustand „unterkritisch, drucklos, kalt“ (Phase 3) erfordert.

Zu Phase 3:

Der Übergang in den Zustand „unterkritisch, kalt“ wird eingeleitet, sobald die Wiederherstellung der Netzversorgung das Zuschalten der Hauptkühlmittelpumpen in den intakten Loops erlaubt. Bleibt die Netzrückkehr aus, wird Phase 3 vom Unterschreiten des Mindestdeionatvorrats eingeleitet, frühestens also nach 10 h. Der Übergang auf primärseitige Nachwärmeabfuhr mit dem Nachkühlsystem erfolgt durch:

- Temperaturabsenkung im PK durch Abfahren über die intakten DE,
- Druckabsenkung im PK durch DH-Sprühen (vorgelagert durch das Volumenregelsystem, sonst durch das Zusatzboriersystem),
- Ergänzung des Kontraktionsvolumens durch boriertes Kühlmittel (vorgelagert durch das Volumenregelsystem, sonst durch Notkühl- und Zusatzboriersystem),
- Übernahme der PK-Kühlung durch das Nachkühlsystem.

Wenn die Hauptkühlmittelpumpen in den intakten Loops wieder zu Verfügung stehen, besteht während des Abfahrens kein Risiko, dass Pfropfen minderborierten Wassers aus dem defekten Dampferzeuger gebildet werden und in den Reaktorkern gelangen.

Beim Abfahren unter Naturumlaufbedingungen wird der Übertritt von Deionat in den PK durch Absenken des Druckes im defekten DE unter den PK-Druck verhindert. Die Druckabsenkung im defekten DE kann dabei durch FD-Abgabe über das FD-Abblaseregelventil, das FD-SiV oder die Anwärmleitung[2] erfolgen. Der Druck im defekten DE soll dabei jedoch nur wenig unter dem PK-Druck liegen, um ein Überströmen von Primärkühlmittel in den defekten DE zu begrenzen und damit ein Überfluten der Feinabscheider zu vermeiden, damit die Rate der Aktivitätsabgabe nicht ansteigt (Minimierungsaspekt).

Die entsprechenden Prozeduren wurden durch ingenieurmäßige Überlegungen konzipiert und in Versuchen am PKL-Versuchsstand bzw. durch Analysen mit geeigneten Rechenprogrammen validiert.

2.2 Bewertungsmaßstab

Der zur Beantwortung der BMUB-Fragen anzusetzende Bewertungsmaßstab ergibt sich insbesondere aus der RSK-Empfehlung „Regelungen zu Anlagenzuständen nach Eintritt eines Störfalls“ ([2[), den „Sicherheitsanforderungen für Kernkraftwerke (SiAnf)“ [5]) sowie der KTA 1201 „Anforderungen an das Betriebshandbuch“ ([6]). Im Anhang dieser Stellungnahme sind die wesentlichen Anforderungen und Definitionen, die bei der Beantwortung der Fragen des BMUB berücksichtigt wurden, aufgeführt.

3 Beantwortung der Fragen des BMUB

3.1 Zu Frage 1: Bis zu welchem Anlagenzustand sollte die Nachweisführung erfolgen?

3.1.1 Beantwortung der Fragestellung

Aufgabe der Nachweisführung für Ereignisse auf der Sicherheitsebene 3 (Störfallanalyse) ist es, die Einhaltung der sicherheitstechnischen Nachweisziele und der zugehörigen Nachweiskriterien nach SiAnf [5], Anhang 2, Tabellen 3.1a bis 3.1c, bezüglich der Kontrolle der Reaktivität, der Kühlung der Brennelemente und des Einschlusses radioaktiver Stoffe zu zeigen.

Gemäß [5], Anhang 2 §2 (3) muss sich die Nachweisführung vom Eintritt eines Ereignisses bis zum Erreichen eines kontrollierten Anlagenzustandes erstrecken; bei der Ermittlung eines Quellterms für radiologische Nachweise bis zur Beendigung der Freisetzung (siehe auch RSK-Empfehlung [2], Kap. 3.2.1).

Der kontrollierte Anlagenzustand ist dadurch gekennzeichnet, dass die Nachweisziele und Nachweiskriterien eingehalten sind und die relevanten Sicherheitsvariablen hinreichend stationäre Werte erreicht haben (siehe [5], Anhang 1).

Hinreichend stationär sind Zustände, in denen die Sicherheitsvariablen so stationär sind oder sich der Sicherheitsabstand zu den Nachweiskriterien stetig so vergrößert, dass ein ausreichend großer Zeitraum für die Analyse und Bewertung des Anlagenzustands zur Verfügung steht, um im Falle einer ungünstigen Änderung

[2] Siehe hierzu auch in Abschnitt 3.2.1.

von Sicherheitsvariablen weitere Maßnahmen (z. B. zur Störfallbehandlung) durchführen zu können (siehe [5], Anhang 1).

Die Störfallbehandlung erfolgt in der Regel schrittweise, also so, dass nacheinander verschiedene, kontrollierte Anlagenzustände angestrebt werden. Wenn nach Erreichen des ersten kontrollierten Zustands ereignisablaufbedingt noch Schutzzielverletzungen auftreten können (z. B. Verletzung des Schutzziels „Reaktivitätskontrolle“ infolge von Xenonzerfall oder erhöhter Moderationswirkung des Kühlmittels bei niedrigen Primärkreistemperaturen, Verletzung des Schutzziels „Kühlung der Brennelemente“ infolge von begrenzten Deionatvorräten zur Dampferzeugerbespeisung), sollte die Nachweisführung bis zum Erreichen des „letzten“ kontrollierten Anlagenzustands erfolgen.

In [5], Anhang 5, §3.2.1 (6) wird gefordert, dass sich die Nachweisführung auf den Sicherheitsebenen 2 bis 4a vom Eintritt eines Ereignisses mindestens bis zum Erreichen des kontrollierten Anlagenzustands erstrecken muss, in dem die Anlage dauerhaft verbleiben kann. Nach Ansicht der RSK wird diese Forderung durch Erreichen des letzten kontrollierten Anlagenzustands erfüllt.

In der Regel beschränken sich die ereignisspezifischen Nachweise auf das Erreichen des ersten kontrollierten Zustands. Die weiteren Nachweise bis zum Erreichen des letzten kontrollierten Zustands (z. B. Nachwärmeabfuhr über das Nachkühlsystem) können dann – regelwerkskonform - auch über Auslegungsrechnungen zur Bemessung der Sicherheitssysteme, Experimente und ingenieurmäßige Bewertungen auf Basis repräsentativer Ereignisse geführt werden, die in die Gestaltung der BHB-Strategien zum Abfahren in den Nachkühlbetrieb einfließen.

Der sichere Anlagenzustand zeichnet sich im Gegensatz zum kontrollierten Anlagenzustand dadurch aus, dass mindestens die sicherheitstechnischen Bedingungen einer im Betriebshandbuch beschriebenen, vergleichbaren Nichtleistungs-Betriebsphase eingehalten sind. Das Erreichen des sicheren Anlagenzustands, ggf. durch Wiederherstellung von Redundanz, ist nicht Gegenstand der Nachweisführung.

3.1.2 Erläuterung anhand des Beispiels „Dampferzeugerheizrohrleck“

In Abschnitt 0 wurde dargestellt, dass nach Isolation des defekten DE (Ende „Phase 1“) ein Anlagenzustand erreicht ist, in dem die Nachweisziele und -kriterien erfüllt sind. Ferner ist der Anlagenzustand hinreichend stationär, so dass ausreichend Zeit zu Verfügung steht, situationsabhängig weitere Maßnahmen einzuleiten und durchzuführen. Folglich ist dieser Zustand ein kontrollierter Anlagenzustand.

Aufgabe der Störfallanalyse ist also zunächst zu zeigen, dass dieser kontrollierte Anlagenzustand „unterkritisch, heiß, defekter DE isoliert“ erreicht wird.

Der „letzte kontrollierte Anlagenzustand“ im Sinne von RSK-Empfehlung [2], Kap. 3.2.1., ist erreicht, wenn die Nachwärme über das Nachkühlsystem dauerhaft abgeführt werden kann. Sofern ausreichend Redundanz im Nachkühlsystem vorhanden ist, ist dieser Zustand „unterkritisch, kalt“ dann auch ein sicherer Anlagenzustand.

Das Erreichen des “letzten kontrollierten Anlagenzustandes“ wird üblicherweise unter Berücksichtigung der entsprechenden BHB Prozeduren zum manuellen Abfahren aufgezeigt. Dabei ist zu berücksichtigen, dass, im

Unterschied zu anderen Störfällen, bei DE-Heizrohrlecks während des manuellen Abfahrens aus dem ersten kontrollierten Zustand noch Anlagenzustände auftreten, in denen ohne spezielle Vorkehrungen minderboriertes Wasser von der Sekundärseite auf die Primärseite gelangen kann. Es ist daher im Rahmen der Nachweisführung nachvollziehbar aufzuzeigen, dass auch während des manuellen Abfahrens in den Nachkühlbetrieb das Schutzziel „Unterkritikalität“ nicht verletzt wird.

3.1.3 Aspekte bei anderen Störfällen der Sicherheitsebene 3

In der Regel sind ereignisspezifische Nachweise zur Störfallbeherrschung nur bis zum ersten kontrollierten Anlagenzustand erforderlich, typisch also bis zum Zustand „unterkritisch, heiß“. Für das weitere Abfahren bis zum letzten kontrollierten Zustand „unterkritisch, kalt“ (Nachkühlbetrieb) ist es meist ausreichend, das Sicherstellen der Schutzziele anhand des Vorgehens bei repräsentativen Ereignissen nachzuweisen.

Aus einer von der AG vorgenommenen Durchsicht der DWR-Ereignisliste (Anhang 2 in [5]) ergibt sich, dass insbesondere die folgenden Ereignisse bzw. Ereignisgruppen vertiefte Betrachtungen zum Erreichen des letzten kontrollierten Zustands erfordern können [7]:

- DEHL (Ereignisse D3-08, D3-09, D3-19) mit dem Nachweisziel ausreichender Unterkritikalität beim Abfahren im Naturumlauf (vgl. Abschnitt 0).

- Ereignisse, bei denen der erste kontrollierte Anlagenzustand durch einen sehr hohen DH-Füllstand gekennzeichnet ist: Nachweisziel ist eine ausreichende Bemessung der Einrichtungen zur primär – und sekundärseitigen Druckabsenkung sowie zum Aufborieren des Primärkreises, so dass ein Übergang auf Nachkühlbetrieb sichergestellt ist. Beispiele sind insbesondere sekundärseitige Leckstörfälle mit nicht absperrbarem Leck (D3-05, D3-06, D3-21) und Ereignis D3-11 (Fehlerhaftes Einspeisen durch betriebliche oder Sicherheitssysteme bei Unwirksamkeit vorgesehener Begrenzungsmaßnahmen).

- Kleine Lecks innerhalb SHB (Ereignisse D3-22, D3-26, D3-28, D3-42) mit dem Nachweisziel der langfristigen Kernkühlung im Nachkühlbetrieb.

3.2 Zu Frage 2: Berücksichtigung von Nicht-Sicherheitssystemen

3.2.1 Zu Frage 2a: Kreditieren von Nicht-Sicherheitssystemen

Frage des BMUB gemäß [1]:

Inwieweit können im Rahmen der Nachweisführung Nicht-Sicherheitssysteme (einschließlich von durch das Begrenzungssystem angeforderten Aktionen, wie dies z. B. beim DEHL der Fall ist) in den verschiedenen Phasen nach Eintritt des Störfalls kreditiert werden (gegebenenfalls mit Festlegung von zugehörigen Bedingungen)?

Hinweis zum Begriff „Nicht-Sicherheitssystem“:
Unter dem Begriff „Nicht-Sicherheitssystem“ werden im Folgenden aktive Einrichtungen verstanden, die nach [5], Anhang 1, nicht unter die „aktiven Sicherheitseinrichtungen“ fallen. Hierzu wurden bisher neben betrieblichen Systemen auch verschiedene Begrenzungseinrichtungen gezählt.

Nach [5], 2.1(6), sind auf der 3. Sicherheitsebene Maßnahmen und Einrichtungen vorzusehen, die den sicherheitstechnisch geforderten Zustand der Anlage unabhängig von den Maßnahmen und Einrichtungen anderer Sicherheitsebenen sicherstellen. Entsprechend ist die Nachweisführung bis zum kontrollierten Anlagenzustand (wenn relevant auch bis zum „letzten“ kontrollierten Anlagenzustand) prinzipiell unter alleiniger Berücksichtigung von Einrichtungen des Sicherheitssystems durchzuführen.

Nicht-Sicherheitssysteme können gemäß der Auffassung der RSK regelwerkskonform in folgenden Fällen kreditiert werden:

- Bei Nachweisführungen zur Wirksamkeit und Zuverlässigkeit von Vorsorgemaßnahmen, welche zur Verhinderung des Eintretens bestimmter Ereignisse vorgesehen sind (Ereignisse mit Nachweisziel „VM“ im Anhang 2 der Sicherheitsanforderungen für Kernkraftwerke [5]).

  Ein Beispiel hierfür ist das Ereignis „*Fehlerhafte Einspeisung aus einem System, das Deionat oder minderboriertes Kühlmittel führt, mit Ausfall der Begrenzungen oder vorgelagerter Maßnahmen (Externe Deborierung; homogen und heterogen)*“ (Ereignis D3-19) aus [5], für das neben den Schutzzielen R (Reaktivitätskontrolle) und K (Kühlung der Brennelemente) auch „VM“ als Option angegeben ist. Dabei ist aus Sicht der RSK zu beachten, dass die Ereignisdefinition *"mit Ausfall der Begrenzungen oder vorgelagerter Maßnahmen"* nicht für den Nachweis der Verhinderung des Ereignisses durch Erfüllung der VM-Kriterien gilt, da verfügbare Begrenzungen, wie die Einspeisekonzentrationsüberwachung (EIKO), die Steuerelement-Fahrbegrenzung (STAFAB) sowie die gesicherte Deionateinspeisesperre (GEDES), im Zusammenspiel mit vorhandenen Karenzzeiten bei dieser Nachweisführung mit herangezogen werden können.

- Gemäß [9] (Abschnitt 2.1.4) darf die „Berechnung der radiologischen Störfallfolgen (somit der Nachweis betreffend Schutzziel S gemäß Anhang 2 von [5]) „*unter Berücksichtigung der zur Schadensminimierung beitragenden betrieblichen Systeme und Einrichtungen vorgenommen werden, sofern diese Einrichtungen nach den geltenden Regeln und Richtlinien hergestellt sind und betrieben werden, geeignete Qualitätsmerkmale hinsichtlich ihrer Auslegung und Betriebsbewährung besitzen und sie nicht durch Störfallfolgen in ihrer Funktionsfähigkeit beeinträchtigt werden.“*

- Ferner ist zu beachten, dass Zustandsbegrenzungen[3] zwar nicht hinsichtlich der Auslösung von Schutzaktionen kreditiert werden, wohl aber hinsichtlich der bei den Störfallanalysen anzusetzenden Anfangs- und Randbedingungen (vgl. [5], Anhang 1).

Zum Zeitpunkt der Errichtung der Anlagen wurde den Informationen der AG DEHL II zufolge (siehe Kapitel 2.1.1) allerdings davon ausgegangen, dass in der Nachweisführung für die kurzfristige Störfallbehandlung

[3] Zustandsbegrenzungen begrenzen Werte von Prozessvariablen derart, dass Ausgangszustände für zu berücksichtigende Störfälle eingehalten werden. (siehe [5]).

in einzelnen speziellen Fällen sowie für die mittel- und langfristige Störfallbehandlung bei Vorhandensein ausreichend großer Karenzzeiten auch Nicht-Sicherheitssysteme berücksichtigt werden können, falls

(1) ihre Funktionsfähigkeit infolge des Störfalls nicht infrage gestellt ist,
(2) ihr Einsatz ohne Rückwirkungen auf die sicherheitstechnische Funktion und Zuverlässigkeit von Sicherheitseinrichtungen möglich ist,
(3) die Karenzzeiten für ihren Einsatz hinreichend groß sind und
(4) bestimmte Qualitätsanforderungen erfüllt werden.

Der Umfang der in der Nachweispraxis kreditierbaren Nicht-Sicherheitssysteme war durch die genannten Forderungen begrenzt. Vor diesem Hintergrund wurde seitens der Ad-hoc AG DEHL II für die DWR-Ereignisse in Anhang 2 der „Sicherheitsanforderungen an Kernkraftwerke“ [5] eine exemplarische Auswertung hinsichtlich der folgenden Kriterien vorgenommen[4] [7]:

(1) Charakterisierung des ersten kontrollierten Zustands und Identifizierung der zum Erreichen dieses Zustands notwendigen Maßnahmen und Einrichtungen.
(2) Charakterisierung des letzten kontrollierten Zustands, sofern für die Nachweisführung relevant (vgl. Kapitel 0), und Identifizierung der zum Erreichen dieses Zustands notwendigen Maßnahmen und Einrichtungen.
(3) Zuordnung der identifizierten Einrichtungen zum Sicherheits- bzw. Nicht-Sicherheitssystem.

Auf Basis der Auswertung der AG DEHL II kommt die RSK zu folgenden Ergebnissen:

- Bei einem Erdbeben mit unterstellten Folgeschäden (Bruch von Frischdampfleitungen außerhalb des Reaktorgebäudes mit schnell erfolgendem Sekundärkreisabschluss) kann es zu einer Drucktransiente im Primärkreis kommen. In der Nachweispraxis wird hierbei das Öffnen und spätere Wiederschließen der DH-Abblasestation kreditiert. Die Ansteuerung der Abblasestation erfolgt über die Kühlmitteldruckbegrenzung (MADTEB) aus dem gesicherten Bereich und ist auf Funktion nach induzierten Erschütterungen aus Erdbeben ausgelegt. Aus dem gleichen Grund ist auch das DH-Abblaseabsperrventil auf Funktion nach Erdbeben ausgelegt und wird auch aus dem gesicherten Bereich über die MADTEB angesteuert. Bei postuliertem Nichtschließen des DH-Abblaseventils stellt das Abblaseabsperrventil die Dichtheit des Primärkreises sicher.

  Anmerkung: Ohne Kreditierung *des Öffnens des DH-Abblaseventils steigt der Druck im PK ggf. bis zum Ansprechdruck der DH-SiV. Bei postuliertem Einzelfehler an einem DH-SiV (schließt nicht) käme es zu einer Transiente mit Kühlmittelverlust in den SHB. Mit der oben begründeten Verwendung der MADTEB ist dieses Szenarium nicht zu unterstellen.*

- Im Rahmen der Diskussionen zur Ausbildung und Auswirkung eines Deionatpfropfens beim Dampferzeugerheizrohrleck (siehe [4]) kam die Frage auf, inwieweit ein Öffnen der Ventile der Anwärmleitung (zur DE Druckabsenkung bei postulierter Nichtverfügbarkeit des Abblaseregelventils am defekten DE wegen des Einzelfehlers, bzw. wegen erforderlicher Simulationen im Reaktorschutz zum Öffnen des FD-SiV siehe auch Abschnitt 2.1.2) kreditiert werden darf.

[4] Ereignisse im Hinblick auf die Kühlung des Brennelementlagerbeckens wurden seitens der AG nicht bewertet, vgl. hierzu [8].

Da die hierfür verwendeten Motorarmaturen und ihre Antriebe in Bezug auf den Sekundärkreisabschluss Teil des Sicherheitssystems sind, weisen sie eine hinreichende Qualität hinsichtlich der Öffnungsfunktion auf und können daher bei der Ereignisanalyse kreditiert werden. Die Kreditierbarkeit setzt allerdings voraus, dass adäquate Verfügbarkeitsanforderungen im Betriebsreglement festgelegt sind.

- Die RSK weist weiter darauf hin, dass in den Nachweisen zur Störfallbeherrschung implizit auch Hilfssysteme kreditiert werden, welche längerfristig zum Absichern des Betriebs der Sicherheitssysteme dienen, wie z. B. Heizungs- und Lüftungssysteme zur Einhaltung der Umgebungsbedingungen. Diese Hilfssysteme werden kreditiert, da ihre Eignung zur Unterstützung der Sicherheitssysteme im Rahmen von Systembewertungen bei der Errichtung festgestellt wurde. Dies gilt auch für so genannte „autarke“ Leittechniksysteme.

- Darüber hinaus haben sich keine Hinweise darauf ergeben, dass eine Kreditierung von Nicht-Sicherheitssystemen für die Beherrschung von Störfällen, für die eine solche Kreditierung gemäß Regelwerk nicht erfolgen soll, zwingend vorzunehmen wäre.

  Es ist allerdings auf die Nachweisführung bei Störfällen im Hinblick auf die Kühlung des Brennelementlagerbeckens zu verweisen, bei der die Kreditierung von Nicht-Sicherheitssystemen ggf. erforderlich wird (siehe gesonderte RSK-Stellungnahme [8]).

Vor diesem Hintergrund kommt die RSK im Hinblick auf die o.g. Frage 2a des BMUB zusammenfassend zu folgenden Ergebnissen:

1 Nachweise zur Störfallbeherrschung sind gemäß [5], Nr. 2.1 (6) und [2], Kapitel 3.2.1, bis zum kontrollierten Anlagenzustand (wenn relevant auch bis zum „letzten kontrollierten Anlagenzustand“) prinzipiell unter alleiniger Berücksichtigung von Einrichtungen des Sicherheitssystems, durchzuführen.

2 Gemäß übergeordnetem Regelwerk zulässige Ausnahmen davon sind:

- In Nachweisen zur Wirksamkeit und Zuverlässigkeit von Vorsorgemaßnahmen, welche zur Verhinderung des Eintretens bestimmter Ereignisse vorgesehen sind (Ereignisse mit Nachweisziel „VM“ in Anhang 2 von [5]) dürfen auch Nicht-Sicherheitssysteme kreditiert werden.

- Die Berechnung der radiologischen Störfallfolgen darf nach [9], Abschnitt 2.1.4, unter Berücksichtigung von Nicht-Sicherheitssystemen erfolgen, sofern diese bestimmte Qualitätsanforderungen erfüllen.

- Zustandsbegrenzungen werden hinsichtlich der bei den Störfallanalysen anzusetzenden Anfangs- und Randbedingungen (vgl. [5], Anhang 1) kreditiert.

3 Sofern darüber hinaus Nicht-Sicherheitssysteme in der Nachweisführung kreditiert werden, wie in o. g. Fällen, sollte diese Abweichung begründet werden.

  Dabei ist zu zeigen, dass die Anforderungen des gestaffelten Sicherheitskonzepts eingehalten sind.

Das bedeutet, dass auch dann gestaffelte Maßnahmen zur Vermeidung von Störungen, zur Verhinderung von Störfällen und zu deren Beherrschung vorhanden sein müssen. Die Nicht-Sicherheitssysteme, die auf Sicherheitsebene 3 berücksichtigt werden, dürfen daher nicht schon hinsichtlich der Verhinderung des betrachteten Ereignisses in den Sicherheitsebenen 1 und 2 kreditiert werden.

Zudem muss für die Nicht-Sicherheitssysteme, die auf Sicherheitsebene 3 berücksichtigt werden, gezeigt sein, dass die Zuverlässigkeit und Wirksamkeit der kreditierten Nicht-Sicherheitssysteme ausreichend sind, um mit Blick auf die Anforderungen an die zur Störfallbeherrschung erforderliche Sicherheitsfunktion eine Sicherheitseinrichtung zu ersetzen. Dabei sind jedenfalls folgende Merkmale darzulegen:

3a Die Wirksamkeit der Maßnahmen hinsichtlich der gewünschten Funktion ist nachgewiesen.

3b Die zum Durchführen der Maßnahme benötigten Einrichtungen sind durch den Störfall, bei dem sie herangezogen werden sollen, nicht beeinträchtigt.

3c Die benötigten Einrichtungen weisen eine hohe Qualität auf (je nach Einsatzzweck z. B. Auslegung gegen Bemessungserdbeben, Notstromversorgung, Störfallfestigkeit oder Betriebsbewährung unter vergleichbaren Druck- und Temperaturbedingungen, die den Anforderungen beim Störfall ähnlich sind). Die Erfüllung der erforderlichen Sicherheitsfunktion ist auch bei Anwendung des Einzelfehlerkonzepts auf die Gesamtheit der erforderlichen Einrichtungen sichergestellt.

3d Die leittechnische Ansteuerung ist ausreichend zuverlässig, z. B.

- bei von Hand ausgelösten Maßnahmen:
  Ansteuerung von der Warte, Möglichkeit der Erfolgskontrolle durch Rückmeldungen der Stellung von Armaturen, geeignete Instrumentierung zur Verfolgung der relevanten Anlagenparameter, wie z.B. DE-Füllstand, ausreichend Zeit für Kontrolle und ggf. Korrektur.

- bei automatischen Maßnahmen:
  Ausführung der Leittechnik mindestens entsprechend den Anforderungen an leittechnische Funktionen der Kategorie B, wenn kein besonderes Potenzial für das Auftreten eines systematischen Fehlers im Anforderungsfall vorliegt.

3e Die Maßnahmen sind vorgedacht und in geeigneter Weise im Betriebshandbuch verankert (vgl. auch Antwort zu Frage 4, Kap. 0). Die RSK-Empfehlung [2], Abschnitt 3.2.4, hinsichtlich „Simulationen im Reaktorschutz“, „Unscharfmachen“ und „besonderen Schalthandlungen“ wird beachtet.

3f Die benötigten Einrichtungen werden in geeigneten Zeitintervallen für die gewünschte Funktionalität getestet oder sind dauerhaft in Betrieb. Ihre Verfügbarkeit im Anforderungsfall ist durch entsprechende Vorgaben im BHB sichergestellt.

3g Der Einfluss der Nichtverfügbarkeit der kreditierten Einrichtungen auf die Häufigkeit von Gefährdungszuständen sollte probabilistisch bewertet sein (z.B. Sensitivitäts- bzw. Importanzanalysen).

3.2.2 Zu Frage 2b: Günstige/Ungünstige Einflüsse von Nicht-Sicherheitssystemen

Frage des BMUB gemäß [1]:

Wie sind hierbei Nicht-Sicherheitssysteme zu behandeln, die zum Zeitpunkt des Ereigniseintritts in Betrieb sind, auslegungsgemäß nicht abgeschaltet werden und den Ereignisablauf günstig oder ungünstig beeinflussen?

Berücksichtigung günstiger Einflüsse von Nicht-Sicherheitssystemen:

Ein Ausfall von betrieblichen Systemen, die bei Ereigniseintritt in Betrieb sind, mit dem einleitenden Ereignis bzw. im Ereignisablauf wird in der Nachweisführung jedenfalls dann unterstellt, wenn ein kausaler Zusammenhang mit dem einleitenden Ereignis besteht, z. B. wenn die für den Betrieb erforderlichen Hilfs-, Versorgungs- und Energiesysteme ausfallen (z. B. elektrische Stromversorgung, Steueröldruck für Turbinen- und Umleitventile). Dies ist insbesondere dann gegeben, wenn im Zusammenhang mit dem Ereigniseintritt der Notstromfall überlagert wird (nach RESA/TUSA). Betriebliche Systeme, die auf diese Weise ausgefallen sind, werden auch dann nicht wieder kreditiert, wenn die erforderlichen Hilfs-, Versorgungs- und Energiesysteme nach Start der Notstromdieselaggregate wieder verfügbar sind.

Es gibt jedoch auch betriebliche Funktionen, die mit dem unterstellten Notstromfall nicht oder nicht direkt abgeschaltet werden.

Nachweise zur Störfallbeherrschung sind prinzipiell unter alleiniger Berücksichtigung von Einrichtungen des Sicherheitssystems durchzuführen (vgl. 3.2.1). Vor diesem Hintergrund müssten auch unabhängig vom zu unterstellenden Notstromfall laufende betriebliche Systeme in der Nachweisführung "künstlich" abgeschaltet werden. Sofern sie jedoch sowieso von betrieblichen leittechnischen Systemen in der Folge abgeschaltet werden, kann die Analyse auch auf ein vorheriges "künstliches" Abschalten verzichten. Es muss dabei aber sichergestellt sein, dass dies nicht zu substantiell günstigeren Ereignisabläufen führt. Hierzu sind ggf. verschiedene Varianten von Ereignisabläufen zu analysieren.

Berücksichtigung ungünstiger Einflüsse von Nicht-Sicherheitssystemen:

Gemäß SiAnf, Anhang 5, 3.2.4 (5), ist *das ordnungsgemäße Wirksamwerden von Maßnahmen und Einrichtungen der Sicherheitsebenen 1 und 2 zu unterstellen, sofern sich hieraus relevante ungünstige Einflüsse auf den Ereignisablauf ergeben.*

Mit der Vorgabe, das ordnungsgemäße Wirksamwerden zu unterstellen, wird ein Wirksamwerden aufgrund von zufälligen Fehlsignalen während des Störfallablaufs nicht angenommen. Dies ist gerechtfertigt, da eine fehlerhafte Ansteuerung betrieblicher Einrichtungen aufgrund von Fehlsignalen zu Anlagentransienten füh-

ren kann. Somit entspräche die Annahme einer fehlerhaften Ansteuerung betrieblicher Einrichtungen während des Störfallablaufs einer Überlagerung eines zusätzlichen, vom Störfall unabhängigen Ereignisses. Dies ist nicht zu unterstellen.

Wie vorstehend beschrieben, ergibt sich der Ausfall der meisten betrieblichen Funktionen, wenn mit RESA/TUSA nach Ereigniseintritt der Notstromfall unterstellt wird. Allerdings ist die Annahme „Notstromfall und damit Ausfall der nicht notstromgesicherten betrieblichen Funktionen“ nicht notwendigerweise immer eine ungünstige Randbedingung: Im Einzelfall kann es relevante Einflüsse auf den Störfallablauf geben, wenn kein Notstromfall eintritt und viele betriebliche Einrichtungen weiterlaufen, soweit sie nicht durch vorrangige Leittechnik abgeschaltet werden. Die Störfallbeherrschung ist deshalb auch für den Fall zu zeigen, dass es nicht zum Notstromfall kommt. Für diese Analyse wird ein Weiterlaufen oder ordnungsgemäßes Zuschalten der betrieblichen Einrichtungen berücksichtigt, soweit sie nicht auslegungsgemäß durch den Reaktorschutz, Begrenzungen oder den Aggregateschutz (wieder) abgeschaltet werden. In diesen Fällen sollte jedoch, überprüft und bewertet werden, inwieweit auch bei einer angenommenen Unwirksamkeit der Begrenzungen bzw. des Aggregateschutzes eine Ereignisbeherrschung gegeben ist. Andernfalls sind zur zuverlässigen Abschaltung der in Rede stehenden Nicht-Sicherheitssysteme die von der RSK in Abschnitt 3.2.1 formulierten Anforderungen an die Kreditierung von Nicht-Sicherheitssystemen zu erfüllen.

Anmerkung: In diesem Zusammenhang wären konstruierte Randbedingungen durch „selektiertes“ Ausfallenlassen aller betrieblichen Funktionen mit evtl. günstigen Auswirkungen und Weiterbetrieb aller betrieblichen Funktionen mit evtl. ungünstigen Auswirkungen nach Auffassung der RSK allerdings so hypothetisch, dass dies nicht unterstellt werden muss.

Ungünstige Einflüsse von Nicht-Sicherheitssystemen infolge von Fehlsignalen sind als kausale Folge von Erdbeben zu berücksichtigen. Eine explizite Berücksichtigung in den Störfallanalysen ist jedoch nicht erforderlich, wenn diese Einflüsse durch Maßnahmen der vorrangigen Leittechnik beherrscht werden und diese gegen das Bemessungserdbeben oder „Fail-safe“ ausgelegt ist.

Die Festlegung der Randbedingungen, welche sich durch den Ausfall oder Nicht-Ausfall von nicht gegen Erdbeben ausgelegten Einrichtungen ergeben, erfordert ggf. eine ingenieurmäßige Bewertung. Beispielsweise wäre die Annahme unplausibel, dass nach einem Erdbeben die elektrische Eigenbedarfsversorgung verfügbar bleibt und die Hauptkühlmittelpumpen weiterlaufen, während gleichzeitig die Kühlung der Pumpendichtungen sowie der überwachende Aggregateschutz erdbebenbedingt ausfallen. Eine auf diese Weise „konstruierte“ Zerstörung der Pumpendichtungen mit möglichem Folgeleck am Primärkreis ist nicht zu unterstellen, da sowohl der Aggregateschutz als auch die Kühlung der Pumpendichtungen ausfallen müssten und beide im Vergleich zur Eigenbedarfsversorgung als seismisch robuster einzustufen sind.

Zusammenfassend kommt die RSK bei der Beantwortung der Frage 2b zu folgenden Ergebnissen:

- Für günstige Einflüsse von Nicht-Sicherheitssystemen gilt:

  Nachweise zur Störfallbeherrschung sind prinzipiell unter alleiniger Berücksichtigung von Einrichtungen des Sicherheitssystems durchzuführen (vgl. 3.2.1). Vor diesem Hintergrund müssten auch unabhängig vom zu unterstellenden Notstromfall laufende betriebliche Systeme in der Nachweisführung "künstlich" abgeschaltet werden. Sofern sie jedoch sowieso von betrieblichen leittechnischen Systemen in der Folge abgeschaltet werden, kann die Analyse auch auf ein vorheriges "künstliches" Ab-

schalten verzichten. Es muss dabei aber sichergestellt sein, dass dies nicht zu substantiell günstigeren Ereignisabläufen führt. Hierzu sind ggf. verschiedene Varianten von Ereignisabläufen zu analysieren.

- Für ungünstige Einflüsse von Nicht-Sicherheitssystemen gilt, dass in der Nachweisführung Zuschaltungen von durch im Ereignisablauf vorgesehenen Signalen oder ein Weiterbetrieb zu berücksichtigen sind, soweit sie nicht auslegungsgemäß durch Eingriffe des Reaktorschutzes, von Begrenzungen oder des Aggregateschutzes verhindert oder unwirksam gemacht werden.

  Ungünstige Einflüsse von Nicht-Sicherheitssystemen infolge von zufälligen Fehlsignalen sind während des Störfallablaufs nicht anzunehmen, da die Annahme einer fehlerhaften Ansteuerung betrieblicher Einrichtungen einer Überlagerung eines zusätzlichen, vom Störfall unabhängigen Ereignisses bedeuten würde. Dies ist nicht zu unterstellen. Kausal bedingte Fehlsignale sind auch als Folge von Erdbeben nicht zu berücksichtigen, wenn diese Einflüsse durch Maßnahmen der vorrangigen Leittechnik verhindert werden und diese Leittechnik gegen das Bemessungserdbeben oder „Fail-safe“ ausgelegt ist.

  Es sollte jedoch überprüft und bewertet werden, inwieweit bei einer angenommenen Unwirksamkeit der Abschaltung betrieblicher Einrichtungen durch leittechnische Funktionen, die nicht vom Reaktorschutz durchgeführt werden, eine Ereignisbeherrschung gegeben ist. Andernfalls sind zur zuverlässigen Abschaltung der in Rede stehenden Nicht-Sicherheitssysteme die von der RSK in Abschnitt 3.2.1 formulierten Anforderungen an die Kreditierung von Nicht-Sicherheitssystemen zu erfüllen.

Anmerkung: Eine manuelle Abschaltung ungünstig wirkender Nicht-Sicherheitssysteme darf in der Störfallanalyse nach [5], 3.1.3h, frühestens 30 min nach Ereigniseintritt kreditiert werden.

3.3 Zu Frage 3: Berücksichtigung von Fehlhandlungen bzw. Unterlassungen von im BHB vorgesehenen Handlungen in den Nachweisführungen

In welcher Art und Weise sind mögliche Fehlhandlungen bzw. Unterlassungen von im BHB vorgesehenen Handlungen in den Nachweisführungen zu berücksichtigen?

Für das Konzept zum Vermeiden oder Beherrschen von Fehlhandlungen bzw. Unterlassungen durch das Anlagenpersonal ist nach folgenden Fehlerarten unterschieden worden:

(1) Bedienfehler in einem Strang (z. B. Pumpe wird ohne Hilfssystem gestartet)
(2) Nichtdurchführung bzw. verspätete Durchführung vorgesehener Maßnahmen
(3) Den Ablauf verschlimmernde Handlungen, z. B. aufgrund falscher Diagnose, Isolierung eines falschen DE, Auswahl eines falschen Pfads im BHB.

Zu (1):

Eine Fehlbedienung, die einen Ausfall einer Komponente oder einer Redundante in einer Sicherheitseinrichtung zur Folge hat, ist einem Einzelfehler gleichgesetzt (Definition SiAnf).

Da die Maßnahmen und Einrichtungen, einschließlich ihrer Hilfs- und Versorgungssysteme, mit denen die Sicherheitsfunktionen der Sicherheitsebene 3 gewährleistet werden, unter Berücksichtigung des Einzelfehlerkonzepts ausgelegt sind, führen solche Fehlbedienungen nicht zu einer unzulässigen Verringerung der Zuverlässigkeit und Wirksamkeit dieser Funktionen.

Durch die Ausfallpostulate entsprechend dem Einzelfehlerkonzept sind in der Nachweisführung derartige Fehler berücksichtigt.

Hinweis: Es ist Sorge zu tragen, dass ein entsprechender Bedienfehler nicht in mehr als einem Strang gleichzeitig auftreten kann (z.B. Erkennbarkeit, Karenzzeit, Gruppensteuerung).

Zu (2):

Nach dem Störfallbeherrschungskonzept sind kurzfristig erforderliche Funktionen zu automatisieren, d. h. die Ansteuerung erfolgt über zuverlässige und vorrangig wirkende Sicherheitsleittechnik. Dies gilt grundsätzlich für alle Funktionen, deren Auslösung innerhalb von ½ h erforderlich ist.

In der Auslegung der Anlagen sind darüber hinaus auch vielfach Funktionen automatisiert, für deren Auslösung eine Karenzzeit besteht, die über ½ h liegt (z. B. 1-2 h). Damit wurde erreicht, dass auch nach Ablauf der ½ h nach Störfalleintritt, in der keine Handmaßnahmen zur Störfallbeherrschung kreditiert werden dürfen, nicht kurzfristig eine größere Anzahl von Handmaßnahmen durch das Anlagenpersonal erforderlich wird.

Ausgehend von diesem Automatisierungskonzept ist für Handeingriffe des Anlagenpersonals folgender Ablauf vorgesehen:

- Beim DWR wird das Personal über den Störfallentscheidungsbaum im BHB anhand der anstehenden Reaktorschutz-Kriterien zu dem zutreffenden Ereigniskapitel geführt. Es wird geprüft, ob der mit der Instrumentierung dokumentierte Ablauf den Beschreibungen entspricht. Beim SWR erfolgt die Entscheidung, welche Maßnahmen zu treffen sind, über die Störfallleitschemata und die Überprüfung des Störfallablaufs anhand des Schutzziel-BHB.

  Anschließend werden die im BHB beschriebenen Handmaßnahmen unter Anwendung des Vier-Augen-Prinzips abgearbeitet und anhand der Rückmeldungen aus der Anlageninstrumentierung permanent auf ihre erwartete Wirksamkeit kontrolliert.

  Abweichungen vom erwarteten Ablauf werden dabei erkannt. Sollte sich bei weiteren Maßnahmen und Kontrollen nicht der erwartete Ablauf einstellen, werden die weiteren Maßnahmen nach dem Schutzziel-BHB vorgenommen. Darin sind verschiedene Möglichkeiten beschrieben, mit denen eine Einhaltung der Schutzzielparameter möglich ist.

- Bei den SWR-Anlagen wird ausschließlich nach dem Schutzziel-BHB vorgegangen, sodass beginnende Abweichungen von den Schutzzielparametern erkannt werden und durch die beschriebenen Maßnahmen gegengesteuert werden kann.

Insgesamt geht die RSK aufgrund der qualitätssichernden Maßnahmen bei der Entwicklung des BHB, der zur Verfügung stehenden Zeit und verschiedener vorhandener Kriterien zur Ereigniserkennung sowie aufgrund der Absicherung der Entscheidungsfindung durch mehrere Personen, die ihre Fachkunde durch Simulator-Schulungen regelmäßig zu validieren haben, davon aus, dass die Zuordnung des eingetretenen Ereignisses und der sich dabei einstellenden Anlagenzustände zu dem zutreffenden BHB-Kapitel (ereignis- oder schutzzielorientiertes BHB) rechtzeitig und zuverlässig erfolgt.

Bei einzelnen, relativ bald nach Ablauf von ½ h erforderlichen Ansteuerungen von Hand wird die Erkennung des Ereignisses durch besondere, akustisch und optisch signalisierte Meldungen (Sicherheitsgefahrenmeldungen) abgesichert. Bei der überwiegenden Zahl der Handmaßnahmen liegen die Karenzzeiten im Bereich > 1 h. Damit ist der zeitliche Spielraum dafür gegeben, dass mit der kontinuierlichen Überwachung durch mehrere Personen, die den Ereignisablauf sowohl mit dem zu erwartenden Ablauf vergleichen als auch die Einhaltung der Kriterien des Schutzziel-BHBs überwachen, unterbliebene Maßnahmen rechtzeitig erkannt und dann korrigiert werden. Die Unterlassung der Korrektur oder des Übergangs in das Schutzziel-BHB wäre daher einem weiteren Fehler gleichzusetzen, der nicht zu unterstellen ist.

Wenn die Notwendigkeit einer Maßnahme aber erst zeitlich verzögert durch die Schutzzielkontrolle erkannt wird, kann dies den Ereignisablauf möglichweise in ungünstiger Richtung beeinflussen. Dies könnte insbesondere bei Maßnahmen, die zum Erreichen des ersten kontrollierten Zustands notwendig sind, der Fall sein (wie beispielsweise beim DEHL oder bei Ereignissen im NLB). Die RSK geht davon aus, dass im Rahmen der Anlagenauslegung oder probabilistischer Analysen übergeordnet gezeigt wurde, dass die Ergebnisse der Störfallanalysen auch bei zu unterstellenden verspäteten Durchführungen vorgesehener Handmaßnahmen gültig sind. Hierbei muss bei Annahme einer deutlich verspäteten Durchführung kein Einzelfehler in den aktiven Sicherheitseinrichtungen angesetzt werden.

Die Wirksamkeit von Handmaßnahmen wird auch im Rahmen von probabilistischen Sicherheitsanalysen (PSA) regelmäßig überprüft. In der PSA werden die Handmaßnahmen modelliert und ihre – nach eventuellen Korrekturen („Recovery-Maßnahmen“) – verbleibende Unverfügbarkeit bewertet. Im Falle nennenswerter Beiträge zu Gefährdungszuständen aufgrund von nicht oder verspätet ausgeführten Handmaßnahmen wurden Änderungen zur weiteren Verbesserung der Zuverlässigkeit vorgenommen. Bei Anlagenänderungen bzw. neuen Erkenntnissen werden evtl. neu erforderliche Handmaßnahmen überprüft.

Insgesamt geht die RSK wegen der oben genannten Gründe davon aus, dass die Nichtdurchführung bzw. verspätete Durchführung vorgesehener Handmaßnahmen in der Störfallanalyse nicht unterstellt zu werden braucht.

Zu (3):

Das Konzept zur Vermeidung bzw. Beherrschung von Personalhandlungen, die den Ablauf verschlimmern könnten, besteht aus folgenden Bausteinen:

- Für den Zeitbereich bis zu ½ h, in den meisten Fällen aber auch darüber hinaus, wird die Störfallbeherrschung durch Sicherheitsleittechnik durchgeführt und überwacht, die vorrangig vor Handansteuerungen wirkt. Relevante „verschlimmernde“ Handansteuerungen werden insoweit blockiert oder automatisch korrigiert.

- In Phasen der Störfallbehandlung, in denen Handmaßnahmen vorgesehen sind, können zwar unter genau definierten Bedingungen Reaktorschutzsignale zurückgesetzt werden. Werden aber als Folge von Fehlhandlungen Reaktorschutzgrenzwerte erreicht, so übernimmt der Reaktorschutz wieder die Störfallbeherrschung. Auf diese Weise werden Auswirkungen „verschlimmernder" Handansteuerungen durch die Sicherheitsleittechnik begrenzt (ein Beispiel hierfür ist das Rücksetzen der Notkühlkriterien, um bei einem DEHL die HD-Sicherheitseinspeisepumpen abschalten zu können. Wenn ungewollt der DH-Füllstand zu stark absinken würde, würden die Pumpe durch den Reaktorschutz bei Erreichen des Anregekriteriums „DH-Füllstand tief" wieder zugeschaltet.).

- Für längerfristige Abläufe in der Störfallbeherrschung ist zu berücksichtigen, dass es nicht nur die vorstehend in (2) beschriebene kontinuierliche Überwachung des Ablaufs und der Schutzzielkriterien einschließlich des Vier-Augen-Prinzips gibt, sondern auch die Verfolgung und Bewertung des Ablaufs durch mehrere sachkundige Mitglieder der Schicht und der Bereitschaftshabenden. Damit werden „verschlimmernde" Handansteuerungen, die nicht von der Sicherheitsleittechnik verhindert werden und erkennbare Auswirkungen auf den Störfallablauf haben könnten, genauso wie unterbliebene Ansteuerungen mit hoher Zuverlässigkeit erkannt und korrigiert.

Insgesamt sind damit auch den Ablauf verschlimmernde Handlungen durch das Sicherheitskonzept abgedeckt und müssen daher in den Störfallanalysen nicht explizit betrachtet werden.

3.4 Zu Frage 4: In welchem Umfang sollten die im Rahmen der Nachweisführung festgelegten Randbedingungen und betrachtete Szenarien in die Störfallkapitel des BHB einfließen?

Die für den Betrieb der Anlage wichtigen Prozessgrößen werden durch Regelungen und Zustandsbegrenzungen innerhalb bestimmter Toleranzbereiche gehalten. Diese sind als Rand- bzw. Ausgangsbedingungen in die Störfallanalysen eingeflossen und müssen auch im BHB in Form von Regelwerten, Meldewerten und Grenzwerten enthalten sein. Weitergehende Grenzwerte, z. B. aus höherwertigen Begrenzungen oder aus dem Reaktorschutzsystem, sind so im BHB zu übernehmen, wie sie in den Störfallanalysen zum Nachweis der Einhaltung der Nachweisziele verwendet wurden.

Die aus den Störfallanalysen resultierenden Randbedingungen – Parameter zur Erkennung des Ereignisses, Einleitungsbedingungen für Maßnahmen, zur Verfügung stehende Systeme und zu erreichende Parameter – sind im Störfall-BHB bzw. bei SWR-Anlagen analog auch im Schutzziel-BHB vollständig zu berücksichtigen. Insbesondere fließen diese Parameter in die Schutzzielkontrolle, die Kontrolle der Systemfunktionen und die Wirksamkeitskontrollen ein. Damit sind ggf. das Einleiten weiterer Maßnahmen und die Kontrolle des Erreichens des kontrollierten Zustands möglich.

Grundsätzlich ist die Beherrschung eines Störfalls nur mit dem Sicherheitssystem zu zeigen. Die erforderlichen Handlungsanweisungen sollen im BHB an geeigneter Stelle enthalten sein. Allerdings sind im BHB entsprechend der Aufgabenstellung Störfälle detaillierter behandelt als in den Störfallanalysen, da in der Regel alle vorhandenen Einrichtungen verfügbar sind. Insofern sollen die Beschreibungen im BHB die zu erwartenden Abläufe realitätsnah wiedergeben. Maßnahmen, die sich durch Veränderungen von Abläufen, die sich durch das Auftreten von Fehlern oder Ausfällen ergeben, wie sie in den Nachweisen zu unterstellen

sind, sind entweder auch ereignisablauf- oder aber schutzzielorientiert zu behandeln. Zu letzterem sind im Schutzziel-BHB Maßnahmen und Einrichtungen aufgeführt, mit denen die Schutzziele eingehalten werden können. Diese müssen auch die in den Nachweisen kreditierten Maßnahmen und Einrichtungen beinhalten.

Wenn aus der Analyse des Ereignisablaufs keine Handlungsanweisungen resultieren, zum Beispiel bei Reaktivitätsstörfällen durch Fehlfahren von Steuerelementen, ist im BHB keine detaillierte Behandlung von Prozeduren erforderlich. Die Kontrolle der Schutzziele ist ein übergeordneter Prozess.

4 Beratungsunterlagen

[1] Beratungsauftrag des BMUB
Sicherheitsanforderungen an Kernkraftwerke zur Beherrschung des Auslegungsstörfalles „Dampferzeuger-Heizrohrleck"
17.03.2015

[2] RSK-Empfehlung (439. Sitzung am 07.07.2011)
Regelungen zu Anlagenzuständen nach Eintritt eines Störfalls

[3] Beherrschung des Störfalles DE-Heizrohrleck – Übersichtsbericht
KWU-Arbeitsbericht R10/2012/81b vom 14.10.1987

[4] Stellungnahme des RSK-Ausschusses ANLAGEN- UND SYSTEMTECHNIK
11.12.2014
Ausbildung und Auswirkungen eines Deionatpfropfens beim Dampferzeugerheizrohrleck

[5] Sicherheitsanforderungen an Kernkraftwerke, 03. März 2015, BAnz AT 30.03.2015 B2

[6] KTA 1201
Anforderungen an das Betriebshandbuch
Fassung 2009-11

[7] Ad-hoc-AG DEHL II
Tabellarische Zusammenfassung von Auswertungen zur Störfallbeherrschung anhand der DWR Ereignisliste aus den „Sicherheitsanforderungen an Kernkraftwerke“, April 2016

[8] RSK-Empfehlung (479. Sitzung der Reaktor-Sicherheitskommission (RSK) am 09.12.2015)
Anforderungen an die Brennelement-Lagerbeckenkühlung

[9] Störfallberechnungsgrundlagen für die Leitlinien zur Beurteilung der Auslegung von Kernkraftwerken mit DWR gemäß § 28 Abs. 3 StrlSchV und Neufassung der „Berechnung der Strahlenexposition“ vom 29. Juni 1994 (BAnz. 1994, Nr. 222a)

5 Zusammenstellung relevanter Anforderungen und Definitionen aus RSK-Empfehlungen und dem Regelwerk

5.1 Zu Frage 1 („Bis zu welchem Anlagenzustand sollte die Nachweisführung erfolgen?“)

5.1.1 Definition des kontrollierten Anlagenzustands

In der RSK-Empfehlung [2], Kap. 3.1, wird der **kontrollierte Anlagenzustand** nach Eintreten eines Ereignisses der Sicherheitsebene 3 wie folgt definiert:

Nach dem Eintritt eines Störfalls ist ein kontrollierter Anlagenzustand dadurch gekennzeichnet, ***dass*** *die Nachweisziele und Nachweiskriterien eingehalten sind und die relevanten Sicherheitsvariablen* ***hinreichend stationäre Werte*** *erreicht haben.*

Im Weiteren wird erläutert:

Hinreichend stationär *sind Zustände, in denen die Sicherheitsvariablen so stationär sind oder sich der Sicherheitsabstand zu den Nachweiskriterien stetig so vergrößert,* ***dass ein ausreichend großer Zeitraum für die Analyse und Bewertung des Anlagenzustands zur Verfügung steht****, um im Falle einer ungünstigen Änderung von Sicherheitsvariablen weitere Maßnahmen (z. B. zur Störfallbehandlung) durchführen zu können.* ***Außerdem muss der Zeitraum ausreichen, um im Anschluss an die Analyse diese Maßnahmen vorbereiten und durchführen zu können.***

Diese Definitionen und Erläuterungen wurden in die „Sicherheitsanforderungen an Kernkraftwerke“ [5], Anhang 1, übernommen.

Ferner erläutert die RSK-Empfehlung [2], Kap. 3.1:

Der - insbesondere bei Störfällen mit Ausgangszustand Leistungsbetrieb - ***anfänglich stark transiente Anlagenzustand wird in einen kontrollierten Anlagenzustand überführt, in der Regel mittels der automatischen Maßnahmen der Sicherheitseinrichtungen, ggf. auch unter Beachtung des 30-Min-Kriteriums mittels von in den Störfallanweisungen definierten Handmaßnahmen*** *- insbesondere bei Störfällen mit Ausgangszustand „Nichtleistungsbetrieb“. Bei ereignisorientierten Störfallprozeduren wird der jeweils anzustrebende kontrollierte Anlagenzustand in den Prozeduren angegeben,* ***im Verlauf der Störfallbehandlung kann es auch mehrere nacheinander anzustrebende kontrollierte Anlagenzustände geben […].***

5.1.2 Definition des sicheren Anlagenzustands

In der RSK-Empfehlung [2], Kap. 3.1, wird der ***sichere Anlagenzustand*** nach Eintreten eines Ereignisses der Sicherheitsebene 3 wie folgt definiert:

*Nach dem Eintritt eines Störfalls ist ein sicherer Anlagenzustand dadurch gekennzeichnet, dass ein **kontrollierter Anlagenzustand** vorliegt und mindestens die sicherheitstechnischen Bedingungen einer im Betriebshandbuch beschriebenen, vergleichbaren Nichtleistungs-Betriebsphase eingehalten sind.*

Diese Definition wurde in die „Sicherheitsanforderungen an Kernkraftwerke“, Anhang 1, übernommen.
Weiterhin wird in [2], Kap. 3.1 ausgeführt:

Langfristiges Ziel der weiteren Störfallbehandlung nach Erreichen eines kontrollierten Anlagenzustands ist es, die Anlage in einen diesen Anforderungen entsprechenden – sicheren – Zustand zu überführen. Damit ist gewährleistet, dass im Sinne des „Defense in Depth-Konzepts“ die Anlage auch in einer möglicherweise länger dauernden Phase der Störfallfolgenbehandlung (s. u.) evtl. auftretende Ausfälle bzw. Ereignisse beherrscht […].

Zu beachten ist, dass nach Störfällen Anlagenbedingungen bestehen können, die bei den o. g. Festlegungen nicht berücksichtigt wurden, da diese im bestimmungsgemäßen Nichtleistungsbetriebszustand nicht vorliegen, z. B. die fehlende Aktivitätsbarriere „Primärkreislauf“ nach KMV-Ereignissen. Sofern daraus zusätzliche Anforderungen an die Verfügbarkeit sicherheitstechnischer Einrichtungen zur Gewährleistung eines sicheren Zustands resultieren, sind diese ereignis- bzw. schutzzielspezifisch festzulegen […].

Der Zeitraum zwischen dem Erreichen eines kontrollierten und dem Erreichen eines sicheren Anlagenzustands hängt von der Art des Ereignisses und insbesondere von dem Umfang an verfügbaren Sicherheitseinrichtungen ab. Es ist in der Regel zu erwarten, dass sich bei Störfällen im Hinblick auf die Verfügbarkeitsanforderungen der „sichere Anlagenzustand“ zeitgleich mit dem „kontrollierten Anlagenzustand“ einstellt, da die der Auslegung zu Grunde liegenden Ausfälle von Sicherheitseinrichtungen nicht eingetreten sind.

Sofern infolge von Ausfällen oder ereignisbedingten Einwirkungen die für den sicheren Zustand notwendigen sicherheitstechnischen Einrichtungen nicht im erforderlichen Umfang zur Verfügung stehen oder andere sicherheitstechnisch erforderliche Bedingungen nicht erfüllt sind, sollen die betrieblichen Vorschriften gem. der KTA 1201, Kap. 7 [6], Anweisungen (z. B. Instandsetzungsmaßnahmen, Überführung in andere NLB – Phasen, Änderung von Bedingungen etc.) für das Herstellen eines sicheren Betriebszustands enthalten. Sofern bereits frühzeitig erkennbar ist, dass zur Herstellung eines „sicheren Zustands“ Instandsetzungen oder andere Maßnahmen erforderlich werden, können solche Maßnahmen während der Störfallbehandlung jederzeit eingeleitet werden, wenn dadurch das Erreichen des kontrollierten Zustands nicht beeinträchtigt wird, d. h. die hierfür zusätzlich erforderlichen Ressourcen zur Verfügung stehen.

5.1.2.1 Anforderungen an die Nachweisführung bezüglich des Erreichens des kontrollierten Anlagenzustands

In der RSK-Empfehlung [2], Kap. 3.2.1, werden folgende Anforderungen an die Nachweisführung gestellt:
*Für die Nachweisführung im Genehmigungsverfahren (Störfallanalysen) dürfen - dem deterministischen Auslegungskonzept für das Erreichen des **kontrollierten** Zustands folgend - nur Sicherheitseinrichtungen kreditiert werden. Dabei sind die Redundanzanforderungen des kerntechnischen Regelwerks zu berücksichtigen.*

Die Störfallanalysen müssen unter den o. g. Randbedingungen mindestens bis zum Erreichen eines kontrollierten Zustands – im Falle von mehreren in zeitlicher Abfolge anzustrebenden kontrollierten Zuständen bis zum Erreichen des letzten „kontrollierten Zustands" durchgeführt werden*. Dies betrifft insbesondere die neutronenphysikalischen und thermohydraulischen Analysen.*

Unabhängig von der Nachweisführung im Rahmen der Störfallanalysen können im Ereignisfall auch betriebliche Einrichtungen für eine optimierte Störfallbehandlung benutzt werden, sofern diese zur Verfügung stehen und deren Einsatz ohne Rückwirkungen auf die sicherheitstechnische Funktion und die Zuverlässigkeit der Sicherheitseinrichtungen – insbesondere der Reaktorschutzfunktionen - möglich ist. Sie dürfen jedoch sicherheitstechnisch nicht erforderlich sein. Die Ausführungen in Kapitel 3.2.4 sind hierbei zu beachten.

Erläuterung:

So ist unabhängig von dem Nachweis, dass der kontrollierte Zustand allein mit Sicherheitseinrichtungen erreicht werden kann, für Analysen zum Nachweis einer Minimierung der Auswirkungen des unterstellten Störfalls die Berücksichtigung betrieblicher Einrichtungen zulässig, wenn dadurch nicht die Zuverlässigkeit der Sicherheitseinrichtungen beeinträchtigt ist.

In Anhang 6 der „Sicherheitsanforderungen an Kernkraftwerke", Abschnitt 3.2.1 (6), wird gefordert:
Die Nachweisführung auf den Sicherheitsebenen 2 bis 4a muss sich vom Eintritt eines Ereignisses mindestens bis zum Erreichen ***des kontrollierten Anlagenzustands erstrecken, in dem die Anlage dauerhaft*** *verbleiben kann.*

In Bezug auf radiologisch repräsentative Ereignisse wird im Anhang 2 der „Sicherheitsanforderungen an Kernkraftwerke", Abschnitt 2(3), ergänzt:

Die Nachweisführung muss sich vom Eintritt eines Ereignisses bis zum Erreichen eines kontrollierten Anlagenzustandes erstrecken; bei der Ermittlung eines Quellterms für radiologische Nachweise bis zur Beendigung der Freisetzung.

5.1.2.2 Anforderungen an die Nachweisführung bezüglich des Erreichens des sicheren Anlagenzustands

In der RSK-Empfehlung [2], Kap. 3.2.2, werden folgende Anforderungen bezüglich des Erreichens des sicheren Zustands gestellt:

Nach dem Erreichen eines kontrollierten Zustandes ist die Anlage, in der Regel unter Zuhilfenahme von Handmaßnahmen, in einen sicheren Zustand zu überführen, sofern dieser sich nicht bereits mit dem Erreichen des kontrollierten Zustands ergeben hat.

Störfallanweisungen müssen alle Schritte bis zum Erreichen eines sicheren Anlagenzustands beinhalten.

Sofern für das Herstellen eines sicheren Zustands notwendig, sollte die Wiederherstellung ausgefallener Sicherheitseinrichtungen durch Instandsetzungsmaßnahmen erfolgen. Die Übernahme von Funktionen der Sicherheitssysteme durch betriebliche Systeme in dieser Phase ist zulässig, wenn diese zur Verfügung stehen und deren Einsatz ohne Rückwirkungen auf die sicherheitstechnische Funktion und die Zuverlässigkeit der Sicherheitseinrichtungen möglich ist. Sie sollte mit Priorität erfolgen, wenn die Inbetriebnahme der betrieblichen Einrichtungen kurzfristiger möglich ist als die Instandsetzung ausgefallener Sicherheitseinrichtungen.

5.1.3 Anforderungen an Methoden der Nachweisführung

Die „Sicherheitsanforderungen an Kernkraftwerke“ [5]stellen folgende Anforderungen an Methoden der Nachweisführung:

5 (2): *Zur Nachweisführung der Erfüllung der technischen Sicherheitsanforderungen sind deterministische Methoden sowie die probabilistische Sicherheitsanalyse heranzuziehen:*

Die deterministischen Methoden umfassen

a) die rechnerische Analyse von Ereignissen oder Zuständen,
b) die Messung oder das Experiment,
c) die ingenieurmäßige Bewertung.

5 (6) *Eine Messung oder ein Experiment kann als Nachweis herangezogen werden, wenn*

a) die Übertragbarkeit der experimentellen Bedingungen auf die Anlagenzustände des jeweiligen Anwendungszusammenhangs qualifiziert ist und

b) die mit der Messung verbundenen Unsicherheiten quantifiziert sind.

5 (7) *Ingenieurmäßige Bewertungen können bei Nachweisführungen herangezogen werden, wenn hierzu ein Bewertungsmaßstab vorliegt, der auf technisch-wissenschaftlich nachvollziehbaren Grundlagen beruht.*

5.2 Zu Frage 2 (Berücksichtigung von Nicht-Sicherheitssystemen)

Das *Sicherheitssystem* und die zugehörigen *Sicherheitseinrichtungen* werden in Anhang 1 der „Sicherheitsanforderungen für Kernkraftwerke“ [5] definiert:

Schutzaktion:
Die Betätigung oder der Betrieb von aktiven Sicherheitseinrichtungen, die zur Beherrschung von Ereignissen erforderlich sind.

Sicherheitseinrichtung
Einrichtung des Sicherheitssystems, die der Beherrschung von Störfällen dient.

Sicherheitseinrichtung, aktive
Einrichtung des Sicherheitssystems, die Schutzaktionen ausführt.

Sicherheitssystem

Gesamtheit aller Einrichtungen, die die Aufgabe haben, die Anlage vor unzulässigen Einwirkungen zu schützen und bei auftretenden Störfällen deren Auswirkungen auf das Betriebspersonal, die Anlage und die Umgebung in vorgegebenen Grenzen zu halten.

Die Rolle *der Begrenzungseinrichtungen* ist nach Anhang 1 der „Sicherheitsanforderungen für Kernkraftwerke“ [5]wie folgt:

Begrenzungseinrichtung

Leittechnische Einrichtung mit einer der folgenden Funktionen:

- *Betriebsbegrenzung: Begrenzung von Prozessvariablen auf vorgegebene Werte, um die Verfügbarkeit der Anlage zu erhöhen.*

- *Schutzbegrenzung: Auslösung von solchen Schutzaktionen, die überwachte Sicherheitsvariablen auf einen Wert zurückführen, bei dem eine Fortführung des bestimmungsgemäßen Betriebs zulässig ist.*

- *Zustandsbegrenzung: Begrenzung der Werte von Prozessvariablen, um Ausgangszustände für zu berücksichtigende Störfälle einzuhalten.*

Zu den bei der der Nachweisführung zu berücksichtigenden Systemen sind insbesondere folgende Bestimmungen in den „Sicherheitsanforderungen für Kernkraftwerke“ [5] relevant:

Abschnitt 2.1(6):
Auf den Sicherheitsebenen 2 und 3 sind Maßnahmen und Einrichtungen derart vorzusehen, dass beim Versagen von Maßnahmen oder Einrichtungen auf den Ebenen 1 oder 2 die Maßnahmen und Einrichtungen auf der nachfolgenden Sicherheitsebene unabhängig von den Maßnahmen und Einrichtungen anderer Sicherheitsebenen den sicherheitstechnisch geforderten Zustand der Anlage herstellen.
Maßnahmen und Einrichtungen, die auf allen oder mehreren dieser Sicherheitsebenen wirksam sein müssen, sind gemäß den Anforderungen auszulegen, die auf der Sicherheitsebene mit den jeweils höchsten Anforderungen gelten.

Anhang 5, 3.2.4 (3):
Bei allen zur Störfallbeherrschung erforderlichen Maßnahmen und Einrichtungen ist auch, sofern es den Ereignisablauf nachteilig beeinflusst, ereignisabhängig ein gleichzeitiger oder zeitlich versetzter Ausfall der elektrischen Eigenbedarfsversorgung zu unterstellen. Die Berücksichtigung der Notstromversorgung in der Analyse soll entsprechend dem Zuschaltprogramm der mit Notstrom versorgten Aggregate erfolgen.

Anhang 5, 3.2.4 (5):
Bei den Nachweisführungen sind zusätzlich zu den Ausfallannahmen des Einzelfehlerkonzepts störfallbedingte Folgeausfälle von Maßnahmen und Einrichtungen, die im Sinne des Nachweisziels ungünstige Auswirkungen auf den Störfallablauf haben, zu berücksichtigen.
Das ordnungsgemäße Wirksamwerden von Maßnahmen und Einrichtungen der Sicherheitsebenen 1 und 2 ist zu unterstellen, sofern sich hieraus relevante ungünstige Einflüsse auf den Ereignisablauf ergeben.

Die „Störfallberechnungsgrundlagen für die Leitlinien zur Beurteilung der Auslegung von Kernkraftwerken mit DWR“ [5] führen in Anhang 5, 3.2.4 (3), aus, dass unter bestimmten Bedingungen betriebliche Systeme bei der Ermittlung der radiologischen Störfallfolgen herangezogen werden können:

Berücksichtigung betrieblicher Systeme :Die Berechnung der Störfallfolgen darf unter Berücksichtigung der zur Schadensminimierung beitragenden betrieblichen Systeme und Einrichtungen vorgenommen werden, sofern diese Einrichtungen nach den geltenden Regeln und Richtlinien hergestellt sind und betrieben werden, geeignete Qualitätsmerkmale hinsichtlich ihrer Auslegung und Betriebsbewährung besitzen und sie nicht durch Störfallfolgen in ihrer Funktionsfähigkeit beeinträchtigt werden.

5.3 Zu Frage 3 (Berücksichtigung von Handmaßnahmen)

5.3.1 Deterministische Nachweisführung

Entsprechend den „Sicherheitsanforderungen für Kernkraftwerke“ [5], 3.1 (3), sind von Hand ausgelöste Schutzaktionen in der Störfallanalyse grundsätzlich nicht vor Ablauf von 30 Minuten zu kreditieren („30-Min-Kriterium“):

Zur Gewährleistung einer ausreichenden Zuverlässigkeit der Einrichtungen der Sicherheitsebene 3 (Sicherheitseinrichtungen) sind zusätzlich zu der Nummer 3.1 (2) folgende Auslegungsgrundsätze anzuwenden:
[…]
h) Automatisierung (in der Störfallanalyse sind von Hand auszulösende Schutzaktionen grundsätzlich nicht vor Ablauf von 30 Minuten zu kreditieren).

Nach 3.1 (6) ist die Zuverlässigkeit und Wirksamkeit von Sicherheitsfunktionen der Sicherheitsebene 3 durch Maßnahmen und Einrichtungen, einschließlich ihrer Hilfs- und Versorgungssysteme, auch bei Ausfällen oder Unverfügbarkeiten gemäß dem Einzelfehlerkonzept nach Nummer 3.1 (7) sicherzustellen. Anhang 1 präzisiert hierzu:

Ein Einzelfehler liegt vor, wenn ein Systemteil der Einrichtung seine Funktion bei Anforderung nicht erfüllt. Eine betrieblich mögliche Fehlbedienung, die eine Fehlfunktion in der Einrichtung zur Folge hat, ist einem Einzelfehler gleichgesetzt.

5.3.2 Probabilistische Sicherheitsanalysen

Die grundlegenden Methoden und Randbedingungen zur Erstellung von probabilistischen Sicherheitsanalysen (PSA) sowie die Anforderungen an deren Dokumentation sind im „Leitfaden Probabilistische Sicherheitsanalysen“ beschrieben. Bezüglich der Nichtverfügbarkeit von Handmaßnahmen sind insbesondere folgende Passagen relevant:

Leitfaden PSA, Kap 3.1 – PSA der Stufe 1 für den Leistungs- und Nichtleistungsbetrieb
Abhängigkeiten zwischen Systemfunktionen, gemeinsam verursachte Ausfälle sowie Personalhandlungen sind zu berücksichtigen.

Leitfaden PSA, Kap. 3.3.6 – Personalhandlungen
Die Analyse von Personalhandlungen beinhaltet die Identifizierung, Modellierung und probabilistische Bewertung von fehlerhaften Handlungen des Betriebspersonals, die Auswirkungen auf Ereignisabläufe haben. Die im Zuge eines Ereignisablaufes geforderten Funktionen können auf verschiedene Weise von Personalhandlungen abhängen.

Leitfaden PSA, Kap. 4 - Bewertung der Ergebnisse
*Die Ergebnisse der PSA sollen **ergänzend zur deterministischen Überprüfung des Sicherheitsstatus der Anlage zur Bewertung der Ausgewogenheit des Sicherheitskonzeptes dienen** und zur Festlegung der Notwendigkeit und Dringlichkeit erforderlicher Sicherheitsverbesserungen herangezogen werden.*
*… [Es sind Analysen] durchzuführen, um relevante Einflüsse von Unsicherheiten bei der Ermittlung von Zuverlässigkeitskenngrößen von Komponenten bzw. bei der Ermittlung von Wahrscheinlichkeiten für gemeinsam verursachte Ausfälle und **fehlerhafte Personalhandlungen** auf das Ergebnis aufzuzeigen.*

Vorschläge zur Bewertung von Handmaßnahmen im Rahmen der PSA werden in den „Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“, Kap. 3.4, „Personalhandlungen“ gemacht:

„Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“, Kap. 3.4.:
*Neben der systemtechnischen Analyse stellt die probabilistische Analyse von Maßnahmen des Betriebspersonals einen wesentlichen Bestandteil der PSA dar. Dabei besteht die **Zielsetzung, Personalhandlungen zu identifizieren und probabilistisch zu bewerten, die die ergebnisrelevanten Sequenzen der PSA beeinflussen.***

Es wird im Weiteren unterschieden zwischen folgenden Handlungskategorien:

(A) Personalhandlungen vor Eintritt eines auslösenden Ereignisses während des bestimmungsgemäßen Betriebs der Anlage,
(B) Personalhandlungen, die ein auslösendes Ereignis zur Folge haben; insbesondere jene, die zusätzlich den Ausfall sicherheitsrelevanter Systeme verursachen,
(C) Personalhandlungen nach Eintritt eines auslösenden Ereignisses.

Innerhalb der Kategorie C werden ferner unterschieden:
(C1) Sicherheitsmaßnahmen auf der Grundlage von Anweisungen (procedural safety action),

(C2) [die Situation] verschlimmernde Maßnahmen/Fehler (aggravating actions/errors),
(C3) nicht geplante Korrektur/Reparatur-Maßnahmen (improvising recovery / repair actions).

Bezüglich der Bewertung der Ausfallwahrscheinlichkeiten wird dann festgestellt:

Angesichts des Mangels an belastbaren Methoden zur Analyse der Typen C2 und C3 wird im Rahmen des vorliegenden Dokuments lediglich die Analyse von Handlungen des Typs C1 behandelt.

Bei der Analyse einer Handlung vom Typ C1 sind Auslassungsfehler (Handlung oder Teilhandlung nicht eingeleitet) und Ausführungsfehler (eingeleitete Handlung und Teilhandlung falsch ausgeführt, z. B. Verwechslungs-Fehler, Reihenfolge-Fehler, Zeitpunkt-Fehler) zu berücksichtigen, ***die zum Versagen der Maßnahme selber führen****.*

5.4 Zu Frage 4 (Anforderungen an das BHB)

Bezüglich der Gestaltung des Betriebshandbuches zu Ereignissen auf der Sicherheitsebene 3 sind die insbesondere die Forderungen aus KTA 1201 ([6])**,** Kapitel 8, „Anforderungen an Teil 3 des Betriebshandbuchs (Störfälle)“ relevant:

(1) In diesem Teil des Betriebshandbuchs sind die Schutzziele darzustellen.

(2) Es sind die Maßnahmen zu beschreiben, die bei Störfällen automatisch eingeleitet werden, sowie diejenigen, die von der Schichtgruppe manuell eingeleitet werden müssen.

(3) Die zu betrachtenden Störfälle des Leistungs- und Nichtleistungsbetriebs müssen enthalten sein.

(4) Folgende Vorgehensweisen zur Störfallbeherrschung sind zulässig:
zustandsorientierte (schutzzielorientierte) Störfallbehandlung,
ereignisorientierte Störfallbehandlung.

(5) Die zustandsorientierte (schutzzielorientierte) Vorgehensweise darf alleine, aber auch in Kombination mit der ereignisorientierten Vorgehensweise angewendet werden.

(6) Es ist eine Vorgehensweise (z. B. Störfall-Leitschema) anzugeben, nach der entschieden werden kann,
a. welches der beiden Verfahren in welcher Weise beim Eintreten eines Störfalles anzuwenden ist,
b. wie im Verlauf eines Störfalls der Übergang vom ereignisorientierten zum zustandsorientierten Teil erfolgt und
c. wie der Übergang zu den Notfallmaßnahmen (d. h. vom BHB in das Notfallhandbuch) erfolgt, wenn ein Schutzziel nicht mehr eingehalten werden kann.

(7) In den zustandsorientierten (schutzzielorientierten) Kapiteln des BHB sind aufzunehmen:
a. eine Beschreibung der einzuhaltenden Schutzziele und der schutzzielübergreifenden Hilfsfunktionen,

b. eine Strategie für das Vorgehen zur Einhaltung der Schutzziele,
c. eine Beschreibung konkreter Maßnahmen mit der Vorgabe einer systematischen Vorgehensweise zu deren Abarbeitung und mit Angaben zur Mindestwirksamkeit dieser Maßnahmen,
d. Angaben zur Kontrolle der Wirksamkeit der Maßnahmen mit Angabe der Anlagenparameter, deren Einhaltung besonders überwacht werden muss sowie
e. die Beschreibung des Übergangs vom BHB in die entsprechenden Notfallmaßnahmen […].

(8) In den ereignisorientierten Kapiteln des BHB sind zu den jeweiligen Anlagenzuständen oder Ereignissen Unterlagen zu erstellen, die in übersichtlicher und möglichst kurzer Form (sogenannte Kurzfassung) die folgenden Informationen enthalten müssen:
a. Kriterien zum Erkennen des Anlagenzustands oder des Ereignisses,
b. eine Nennung der sicherheitstechnisch wichtigen automatisch ablaufenden Maßnahmen,
c. eine Nennung der wesentlichen, zur Beherrschung des Störfalls erforderlichen, von der Schichtgruppe manuell einzuleitenden Maßnahmen und
d. Angaben zur Kontrolle der Wirksamkeit der Maßnahmen mit Angabe der Anlagenparameter, deren Einhaltung besonders überwacht werden muss.

(9) Sowohl in den zustandsorientierten Teil als auch in den ereignisorientierten Teil des BHB ist eine Beschreibung des Zustands, in den die Kraftwerksanlage zu bringen und zu halten ist, aufzunehmen.

H i n w e i s :
Die Angaben des anzustrebenden Anlagenzustands sind so zu formulieren, dass das Schichtpersonal die Wirkung seiner Maßnahmen kontrollieren und Abweichungen erkennen kann.