



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Kommission für die Sicherheit von Kernanlagen
Commission fédérale de la sécurité des installations nucléaires
Commissione federale della sicurezza degli impianti nucleari
Swiss Federal Nuclear Safety Commission

Oktober 2007

Zum Zwischenfall vom 25. Juli 2006 im Kernkraftwerk Forsmark 1 (Schweden)

Betrachtungen und Empfehlungen der KSA

KSA-AN-2325

Kurzfassung

Am 25. Juli 2006 ereignete sich im Kernkraftwerk Forsmark 1 (Schweden) ein Zwischenfall mit einem Verlauf, der mehrere Abweichungen vom auslegungsgemäss vorgesehenen Anlagenverhalten aufwies. Ausgelöst wurde der Zwischenfall durch Fehlhandlungen bei kraftwerksexternen Unterhaltsarbeiten des Netzbetreibers an der 400-kV-Anlage. Im weiteren Verlauf fiel im Kernkraftwerk insbesondere die Notstromversorgung in zwei von vier Strängen aus. Dies führte zu einer kritischen Situation, weil dadurch gewisse Informations- und Kommunikationssysteme beeinträchtigt waren oder ausfielen. Mit den noch verfügbaren und automatisch tätigen Sicherheitssystemen wurde der Zwischenfall aber beherrscht. Alle grundlegenden Schutzziele blieben erfüllt, doch insbesondere bezüglich des Schutzzieles "Kühlung der Brennelemente" war ein Teil der vorgesehenen gestaffelten Massnahmen ausgefallen und somit die verbleibende Marge wesentlich geschmälert.

Der Zwischenfall hat in Schweden selber und international grosse Aufmerksamkeit seitens der Betreiber, Behörden und Öffentlichkeit erweckt. Auch in der KSA wurde der Zwischenfall thematisiert; die KSA erhielt vom Bundesamt für Energie den Auftrag, den Zwischenfall vertieft zu erörtern und ihre Erkenntnisse zuhanden der Behörden festzuhalten.

Aus technischer Sicht ist die Serie von ursächlich unabhängigen Fehlfunktionen bemerkenswert. Besonders schwerwiegend ist der Ausfall der Notstromversorgung in zwei Strängen: Er weist Merkmale eines systematischen Mehrfachfehlers und damit einer besonders gefährlichen Fehlerart auf. Die direkten Ursachen für die eingetretene Sequenz von Fehlfunktionen liegen zu wesentlichen Teilen in Ausführungsmängeln und konzeptionellen Schwächen. Diese stehen in mehreren Fällen im Zusammenhang mit vorgenommenen Anlagenänderungen. Somit sind Schwächen im Änderungswesen und damit im organisatorischen Bereich angesprochen. Die Grundursachen für die Mängel und Schwächen liegen im Bereich Sicherheitskultur.

Bezüglich technischer Befunde verweist die KSA auf die Berichte der schweizerischen Aufsichtsbehörde HSK [1] und der deutschen Fachorganisation GRS [2]. Aufgrund ihrer eigenen Betrachtungen gibt die KSA die nachfolgend stichwortartig zusammengefassten Empfehlungen ab:

- Sicherstellung hinreichender Simulatorenausrüstung für Schulungen hinsichtlich gestörter Energieversorgung und Überprüfung des Schulungsumfangs
- Überprüfung der maximal zu unterstellenden Spannungstransiente
- Umfassende Inbetriebsetzungsprüfungen, Sicherstellung hinreichender Möglichkeiten für Funktionsprüfungen sowie systematische Auswertung des transienten Verhaltens
- Sicherstellung der Koordination zwischen den Betreibern von Kernkraftwerk und Übertragungsnetz im Rahmen der Neuorganisation des Strommarktes
- Grundsätzliche Überprüfung hinsichtlich Verfügbarkeit der Notstromversorgung
- Meldung aller Empfehlungen aus internationalen Expertenüberprüfungen an die Aufsichtsbehörde

Die Empfehlungen sind in den Abschnitten 5 und 6 begründet und in Abschnitt 7 im Wortlaut zusammengestellt.

[leere Seite]

Inhaltsverzeichnis

1	Einleitung	1
2	Anlage Forsmark 1 und Zwischenfall vom 25.7.2006	1
2.1	Kernkraftwerk Forsmark 1	1
	2.1.1 Allgemeine Konzeption	1
	2.1.2 Eigenbedarfs- und Notstromanlagen	2
2.2	Grundsätzliches zur Konzeption von Sicherheitssystemen	2
2.3	Zwischenfall vom 25. Juli 2006	3
	2.3.1 Kurzschluss bei Instandhaltungsarbeiten in der Schaltanlage (kraftwerksextern)	3
	2.3.2 Trennung vom Übertragungsnetz	3
	2.3.3 Übergang auf Eigenbedarfsversorgung	3
	2.3.4 Übergang auf Notstromversorgung	4
	2.3.5 Reaktorschnellabschaltung	5
	2.3.6 Übergang auf Fremdeinspeisung für die Eigenbedarfsschienen	5
	2.3.7 Überprüfung des Anlagenzustands	5
	2.3.8 Wiederherstellung der vollständigen Stromversorgung	6
	2.3.9 Überführen in sicheren Zustand	6
2.4	Direkte Ursachen und Grundursachen	6
3	Massnahmen der schwedischen Betreiber und der Aufsichtsbehörde SKI	7
3.1	Unmittelbare Massnahmen	7
3.2	Betriebsfreigabe mit Bedingungen	7
3.3	Einstufung INES 2	7
3.4	Weitere Entwicklung	8
4	Massnahmen der schweizerischen Aufsichtsbehörde HSK	8
4.1	Untersuchungen	8
4.2	Bericht und Empfehlungen der HSK	9
5	Zu technischen Ursachen und Aspekten menschlichen Handelns	9
5.1	Anlageninterne Stromversorgung	9
	5.1.1 Generelle Konzeption	9
	5.1.2 Schulung hinsichtlich Systemausfällen	10
	5.1.3 Spannungstransiente als mögliche Ursache für Common-cause-Fehler	10
	5.1.4 Empfehlungen	11
5.2	Funktionsprüfungen und unerkannte Fehler	11
	5.2.1 Periodische Funktionsprüfungen in den schweizerischen Kernkraftwerken	11
	5.2.2 Grenzen von Funktionsprüfungen	12
	5.2.3 Massnahmen gegen unerkannte funktionale Fehler in Anlagen	13
	5.2.4 Empfehlungen	13
5.3	Informationen für das Schichtpersonal im Kommandoraum	14
	5.3.1 Allgemeine Erfordernisse	14
	5.3.2 Informationen im Kommandoraum in den schweizerischen Kernkraftwerken	14
	5.3.3 Rechnergestützte Systeme	15
5.4	Rückwirkungen aus dem Netz und liberalisierter Strommarkt	15
5.5	Verfügbarkeit von Notstromanlagen	17
5.6	Probabilistische Sicherheitsanalysen vs. Zwischenfall von Forsmark	17

6	Zu Aspekten der Sicherheitskultur im Allgemeinen	18
6.1	Bericht des Betreibers des KKW Forsmark zur Sicherheitskultur	18
6.2	Zu Aspekten der Sicherheitskultur in den schweizerischen Kernkraftwerken	19
	6.2.1 Auswertung von Ereignissen in anderen Kernanlagen	19
	6.2.2 Umsetzung von Empfehlungen aus Expertenüberprüfungen	20
	6.2.3 Gesetzliche Vorgaben im Bereich Sicherheitskultur	20
7	Zusammenfassung und Schlussfolgerungen	21
	Zusammenstellung der Empfehlungen	23
	Referenzen	25
	Abkürzungen und Begriffe	27
Abbildungen		
Abbildung 1	Schaltschema Elektroversorgung Kernkraftwerk Forsmark 1	28
Abbildung 2	Spannungstransiente an den Generatorklemmen	29
Abbildung 3	Füllstand im Reaktordruckbehälter	29

1 Einleitung

Am 25. Juli 2006 ereignete sich im schwedischen Kernkraftwerk (KKW) Forsmark 1 ein Zwischenfall mit einem Verlauf, der mehrere Abweichungen vom auslegungsgemäss vorgesehenen Anlagenverhalten aufwies. Ausgelöst wurde das Ereignis durch Fehlhandlungen bei kraftwerksexternen Unterhaltsarbeiten des Netzbetreibers an der 400-kV-Anlage. Für den nachfolgenden irregulären Verlauf waren Ausführungsmängel und Schwächen im Bereich der Eigenbedarfs- und Notstromanlagen massgebend, die teilweise im Zuge von Nachrüstungen eingebaut worden waren. Das Ereignis wurde in der Folge nach der internationalen Ereignisskala für Kernanlagen (International Nuclear Event Scale, INES) der Stufe INES 2, Zwischenfall, zugeordnet.

In Schweden selber und international hat der Zwischenfall grosse Aufmerksamkeit seitens der Betreiber, Behörden und Öffentlichkeit erweckt. Auch in der Schweiz hat die Hauptabteilung für die Sicherheit der Kernanlagen (HSK) von den Betreibern der schweizerischen KKW umgehend Abklärungen eingefordert, die Situation analysiert und in einem Bericht [1] ihre Erkenntnisse und Empfehlungen dargelegt.

Der Zwischenfall wurde auch in der Eidgenössischen Kommission für die Sicherheit von Kernanlagen (KSA) thematisiert, zuerst in den Fachausschüssen und am 28. August 2006 erstmals in der Gesamtkommission. Mit dem danach eingetroffenen Brief vom 23. August 2006 [3] erhielt die KSA vom Bundesamt für Energie (BFE) formell den Auftrag, den Zwischenfall vertieft zu erörtern und einen Bericht zuhanden des BFE zu verfassen. Die weitere Bearbeitung erfolgte hauptsächlich in den KSA-Fachausschüssen "Ingenieurwesen" sowie "Personal und Organisation", deren Fachgebieten die massgebenden Faktoren des Zwischenfalls zugeordnet sind.

2 Anlage Forsmark 1 und Zwischenfall vom 25.7.2006

2.1 Kernkraftwerk Forsmark 1

In Forsmark betreibt der schwedische Energiekonzern Vattenfall eine Kraftwerksanlage mit drei KKW-Blöcken. Eigentümer ist die Forsmarks Kraftgrupp AB (FKA), an der Vattenfall selber eine Mehrheitsbeteiligung von 66% hält.

2.1.1 Allgemeine Konzeption

Der Block Forsmark 1 hat einen Siedewasser-Reaktor und ist seit 1980 im kommerziellen Betrieb. Er liefert eine elektrische Leistung von 1016 MW aus den beiden Turbinen-Generator-Einheiten (fortan: *Turbosätzen*) TA11 und TA12. Die elektrische Energie wird über eine 400-kV-Schaltanlage, an die auch der Block Forsmark 2 angeschlossen ist, ins schwedische Übertragungsnetz eingespeist.

Die nuklearen Sicherheitssysteme von Forsmark 1 sind viersträngig aufgebaut, d.h. die erforderlichen Funktionen werden durch vier voneinander unabhängige Systeme bzw. Systemgruppen (Stränge A, B, C, D) erfüllt, welche grundsätzlich dieselben Funktionen abdecken. Wesentliche Anforderung an nukleare Sicherheitssysteme ist u.a. die sichere Abfuhr der Nachzerfallswärme¹. Jeder der vier Stränge verfügt über 50% der im Notfall

¹ Nachzerfallswärme: nach Abschaltung des Reaktors infolge verzögerter, spontaner Kernreaktionen freigesetzte Energie. Ungefährer Anteil der thermischen Nominalleistung (100%) des Reaktors: ca. 7% unmittelbar nach Abschaltung, ca. 4% nach 1 Minute, ca. 1,5% nach 1 Stunde, < 1% nach 1 Tag.

maximal erforderlichen Kühlkapazität (Kurzform: $4 \times 50\%$). Sind zwei Stränge verfügbar, so sind 100% und damit die maximal erforderliche Systemleistung sichergestellt.

2.1.2 Eigenbedarfs- und Notstromanlagen

Da die Stränge der Sicherheitssysteme voneinander unabhängig sein müssen, spiegelt sich die viersträngige Konzeption von Forsmark 1 auch in den elektrotechnischen Anlagen (Abbildung 1). Für jeden Strang von Sicherheitssystemen ist eine Notstromanlage vorhanden, die bei Ausfall der Eigenproduktion oder der Netzanbindung diesen Strang sowie fallweise andere wichtige, möglicherweise nicht mehrfach vorhandene Systeme ab Notstrom-Dieselmotoren (fortan: *Notstromdiesel*) versorgen kann. Besonders wichtige Verbraucher können darüber hinaus innerhalb der Notstromanlage ab Batterie versorgt werden, und zwar über die gesicherte Wechselstromschiene und die Gleichstromschiene. Dies soll einen Unterbruch, z.B. während der Startphase der Notstromdiesel, in der Versorgung von wichtigen Mess-, Steuer- und Regeleinrichtungen vermeiden oder fallweise deren Funktion selbst bei Ausfall der Notstromdiesel sicherstellen. Im Normalfall werden die Notstromanlagen und die weiteren betrieblichen Verbraucher, z.B. prozesstechnische Einrichtungen, Hilfs- und Nebenbetriebe, über die ebenfalls in vier Stränge gegliederten Eigenbedarfsschienen (Spannung 6 kV) versorgt. Diese werden normalerweise ab den beiden eigenen Generatoren bzw. dem Übertragungsnetz (400 kV) angespeist, können aber bei Bedarf durch das 70-kV-Fremdnetz versorgt werden, das in Forsmark nötigenfalls durch eine Gasturbine gestützt ist. Schaltungs-technisch ist jeder der beiden Turbosätze jeweils zwei Strängen zugeordnet: TA11 den Strängen A und C, TA12 den Strängen B und D; siehe auch Abbildung 1. In dieser Zuordnung erfolgt die Versorgung des Kraftwerks im Normal- oder gegebenenfalls im Eigenbedarfsbetrieb.

2.2 Grundsätzliches zur Konzeption von Sicherheitssystemen

Die Konzeption der Sicherheitssysteme mit $4 \times 50\%$ geht von der Zielsetzung aus, dass bei Ausfall von zwei Strängen immer noch die maximal erforderliche Leistungsfähigkeit zur Verfügung stehen soll. Typischerweise wird für die Störfallanalyse unterstellt, dass ein Strang infolge Unterhaltsarbeiten nicht verfügbar ist und ein zweiter Strang infolge Fehlfunktion versagt.

Die mehrfache und über die auslegungsgemäss erforderliche Leistung hinausgehende Ausführung von Systemen für die gleichen Funktionen wird mit *Redundanz* bezeichnet. Funktionen, die mit hohem Grad an Redundanz umgesetzt werden, sind bezüglich zufallsabhängiger Fehler mit hoher Verlässlichkeit sichergestellt.

Falls redundante oder andere mehrfach vorhandene Systeme oder Systemteile gleichartig aufgebaut sind, kann ein systematischer Fehler dazu führen, dass gleichzeitig mehrere oder gar alle entsprechenden Systeme oder Systemteile beeinträchtigt sind (systematischer Mehrfachfehler; *Common Cause Failure*, CCF). Dieser Fehlertyp kann bei redundanten Systemen oder Systemteilen bestmöglich vermieden werden, indem die entsprechenden Funktionen mit physikalisch oder technisch verschiedenartig konzipierten Systemen realisiert werden. Die verschiedenartige Umsetzung der gleichen Funktion wird mit *Diversität* bezeichnet. Grösstmögliche technische Sicherheit für eine bestimmte Funktion wird durch hinreichend redundante und diversitäre Gesamtsysteme erreicht. In der Praxis werden redundante Systeme oft gleich ausgeführt. Die somit fehlende Diversität kann indirekt kompensiert werden durch die nachfolgend erwähnten gestaffelten Massnahmen.

Mit *gestaffelten Massnahmen* (englisch: defence in depth) wird eine allfällige Fehlfunktion durch Vorkehrungen aufgefangen, die im weiteren Verlauf eines Prozesses oder Ereignisses wirksam werden. Damit werden Konsequenzen der Fehlfunktion zumindest begrenzt oder im Idealfall kompensiert. Das Prinzip der gestaffelten Massnahmen ist grundlegendes Element des sicherheitstechnischen Basiskonzepts von KKW.

2.3 Zwischenfall vom 25. Juli 2006

Der nachfolgende Beschrieb basiert auf verschiedenen Quellen [1][2][4][5]. Er ist darauf ausgerichtet, die Sequenz von Unregelmässigkeiten im Verlauf des Zwischenfalls darzulegen. In diesem Sinn wird auf verschiedene, für die Sicherheit durchaus wichtige Begebenheiten und Zusammenhänge nicht oder nur kurz eingegangen. Dies betrifft grundsätzlich die ordnungsgemässen Abläufe, namentlich die auslegungsgemäss erfolgte Leistungsreduktion bzw. Abschaltung des Reaktors, die Sicherstellung der Kernkühlung (inkl. Druckentlastung des Reaktordruckbehälters und Abblasen in die Druckabbaukammer), die Auslösung von einer Anzahl von Schutzkriterien, einige Umschaltungen in der Stromversorgung sowie vor allem auch die Arbeit der Schichtmannschaft. Einzelheiten können u.a. den angegebenen Unterlagen entnommen werden.

2.3.1 Kurzschluss bei Instandhaltungsarbeiten in der Schaltanlage (kraftwerksextern)

Am 25. Juli führten Spezialisten von Svenska Kraftnät (SvK), der Eigentümer und Betreiber-gesellschaft des schwedischen Übertragungsnetzes, Instandhaltungsarbeiten in der 400-kV-Schaltanlage aus.

Unregelmässigkeit 1 / Auslösendes Ereignis (kraftwerksextern)

Aufgrund von Fehlhandlungen wurde ein Netztrenner unter Last geöffnet. Ein Trenner darf (im Gegensatz zu einem Schalter) nicht unter Strom geöffnet werden.

Folge

Zweiphasiger Kurzschluss in der 400-kV-Schaltanlage (25.7.2007, ca. 13:20 Uhr)

Unregelmässigkeit 2 (kraftwerksextern)

Normalerweise müsste bei einem Kurzschluss der Sammelschienenschutz ansprechen und den vom Kurzschluss betroffenen Leitungsabgang innerhalb von 100 ms von der Sammelschiene trennen. Der Sammelschienenschutz reagierte aber nicht.

Folge

Ausserordentlich tiefes Absinken der Spannung an den Generatorklemmen des KKW

2.3.2 Trennung vom Übertragungsnetz

Durch den anstehenden Kurzschluss sank die Spannung an der Sammelschiene der Schaltanlage massiv, bis nach 300 Millisekunden im KKW der Unterspannungsschutz der beiden Generatoren auslöste und die Kraftwerksanlage vom Übertragungsnetz trennte. Nachdem die Spannungsregelung der Generatoren während des anstehenden Kurzschlusses der Unterspannung entgegengewirkt hatte, überschwang die Spannung an den Generatorklemmen unmittelbar nach der Trennung vom Übertragungsnetz und erreichte kurzzeitig maximal etwa 120% der Nominalspannung. Abbildung 2 zeigt den Spannungsverlauf: Auf einen scharfen Abfall auf etwa 60% folgte ein steiler Wiederanstieg mit Überschwingen auf maximal etwa 120% der Nominalspannung. Diese *Spannungstransiente* wirkte sich über die Eigenbedarfs- und Notstromanlagen (Abbildung 1) auf die gesamte elektrische Versorgung des Kraftwerks aus, insbesondere auch auf die Versorgung von sicherheitsrelevanten Systemen.

2.3.3 Übergang auf Eigenbedarfsversorgung

Aufgrund der Trennung vom Übertragungsnetz wurde die Reaktorleistung auslegungsgemäss automatisch auf 25% heruntergefahren. Die beiden Generatoren hätten nun auf die Leistung geregelt werden müssen, die dem aktuellen Bedarf der kraftwerkseigenen Einrichtungen entspricht (Eigenbedarfsversorgung).

Unregelmässigkeit 3

Als Folge der durchlaufenen Spannungstransiente fiel der Druck in einem Teil des ölhydraulischen Regelsystems der Turbine von TA11 zu tief ab. Sie wurde deshalb etwa 5 Sekunden nach Ereigniseintritt automatisch abgeschaltet.

Die Turbine von TA12 blieb etwa eine halbe Minute länger verfügbar, bis sie wegen zu hohen Kondensatordrucks automatisch abgeschaltet wurde.

Folge

Längerfristig stabile Eigenbedarfsversorgung nicht möglich

Der weitere Verlauf war bei beiden Turbosätzen und der angeschlossenen Stromversorgung grundsätzlich gleich, aber bei den einzelnen Schaltungen fallweise um etwa 15 bis etwa 30 Sekunden zeitlich versetzt.

Auslegungsgemäss blieben die Generatorschalter in beiden Fällen vorerst geschlossen, sodass die Eigenbedarfsversorgung in den einzelnen Strängen weiterhin ab dem jeweils zugeordneten Generator erfolgen konnte. Zur Stromerzeugung wird in dieser Situation die Rotationsenergie des auslaufenden Turbosatzes genutzt, wobei Frequenz und Spannung absinken.

2.3.4 Übergang auf Notstromversorgung

Bei einer Drehfrequenz von 47,5 Hz hätte auslegungsgemäss der Generatorschalter öffnen sollen. Damit verbunden wäre eine automatische Umschaltung auf Einspeisung ab 70-kV-Fremdnetz.

Unregelmässigkeit 4

Wegen eines Verdrahtungsfehlers im Messumformer für die Frequenzüberwachung unterblieb das Öffnen der Generatorschalter bei 47,5 Hz.

Folge

Die automatische Umschaltung auf Fremdeinspeisung ab dem verfügbaren 70-kV-Fremdnetz unterblieb vorerst.

Die Frequenz sank weiter, bis 3 Sekunden nach Erreichen eines zweiten Grenzwertes (47 Hz) die Notstromschienen von der Eigenbedarfsversorgung getrennt und die Notstromdiesel für die Selbstversorgung gestartet wurden (24 Sekunden nach Ereigniseintritt: Stränge A und C; 37 Sekunden: Stränge B und D).

Unregelmässigkeit 5

Während der Spannungstransiente zu Beginn des Ereignisses waren in den Notstromanlagen A und B die Gleich- und Wechselrichter der unterbrechungsfreien Stromversorgung (USV) für die gesicherten Wechselstromschienen durch ungünstig gesetzte Schutzkriterien ausgeschaltet worden.

Folgen

Die Batteriespeisung der gesicherten Wechselstromschienen A und B war nicht möglich. Dies hatte eine Reihe von Ausfällen sowie Auslösungen von Schutzkriterien und -massnahmen zur Folge.

Insbesondere war die ab den gesicherten Wechselstromschienen angespeiste Drehzahlregelung der Notstromdiesel A und B stromlos. Die angelaufenen Notstromdiesel A und B konnten deshalb nicht aufgeschaltet werden. Aufgrund des Kriteriums "zu lange Startzeit" wurde das Aufstartverfahren dann abgebrochen. Somit blieben die Notstromschienen A und B ohne Spannung.

In den Strängen A und B konnten also weder die USV noch die Notstromschienen auf die gesicherten Wechselstromschienen einspeisen. Die daran angeschlossenen sicherheitsrelevanten Verbraucher der Stränge A und B fielen deshalb aus.

Die USV der Notstromanlagen C und D waren nicht ausgefallen. Die Notstromdiesel C und D starteten und versorgten die daran angeschlossenen Verbraucher auslegungsgemäss. Grundsätzlich standen mit $2 \times 50\%$ für den Reaktor genügend Einspeise- und Kühlleistung zur Verfügung. Schwierigkeiten für die Schichtmannschaften ergaben sich vor allem bei nicht redundant vorhandenen Messwerten und Anzeigen im Kommandoraum sowie Kommunikationseinrichtungen, die von den ausgefallenen Strängen angespeist waren.

2.3.5 Reaktorschnellabschaltung

Nach 35 Sekunden erfolgte eine automatische Reaktorschnellabschaltung, ausgelöst durch vorübergehende Spannungslosigkeit, die bis dahin auf den gesicherten Wechselstromschienen A und B aufgetreten war. Diese Spannungsunterbrüche standen im Zusammenhang mit auslegungsgemässen Umschaltungen, die ihrerseits eine Folge des Ausfalls der USV in den Notstromanlagen A und B waren (siehe Unregelmässigkeit 5).

Weitere Schutzmassnahmen wurden auslegungsgemäss automatisch ausgelöst, u.a. Abschluss des Primärcontainments, Abschaltung der Speisewasser- und Kondensatpumpen, Start der Notspeisewasserpumpen sowie Öffnen von Sicherheits- und Entlastungsventilen. Allerdings starteten bzw. öffneten wegen der Unregelmässigkeit 5 jeweils nur die Einheiten der Stränge C und D.

2.3.6 Übergang auf Fremdeinspeisung für die Eigenbedarfsschienen

36 bzw. 63 Sekunden nach Ereigniseintritt unterschritt die Generatorleistung von TA11 bzw. TA12 das Kriterium für den sogenannten *Rückwattschutz* (verhindert, dass Generator als Motor wirkt). Deshalb wurde der entsprechende Generatorschalter geöffnet und die zugehörigen Eigenbedarfsschienen (nicht aber die von den Eigenbedarfsschienen abgetrennten Notstromschienen) wurden automatisch auf das 70-kV-Fremdnetz geschaltet.

Im Zug dieser Umschaltung wurden die Eigenbedarfsschienen vorübergehend spannungslos. Die Spannungslosigkeit hätte eine externe Gasturbinenanlage starten sollen, die als Redundanz zum 70-kV-Fremdnetz vorhanden ist.

Unregelmässigkeit 6

Ein Startbefehl für die Gasturbinenanlage wurde zwar ausgegeben, aber nicht umgesetzt, weil ein Prozessor wegen Fehlern in der internen Stromversorgung und teilweisen Softwareverlusts nicht funktionierte. Die Startautomatik war seit Bau der Gasturbinenanlage nie planmässig geprüft worden.

Folgen

Keine (Das 70-kV-Fremdnetz war stets verfügbar.)

2.3.7 Überprüfung des Anlagenzustands

Bezüglich Stromversorgung blieb die Situation für die folgenden rund 20 Minuten unverändert und präsentierte sich als Resultat der oben beschriebenen Abläufe wie folgt: Sämtliche Eigenbedarfsschienen (6 kV) wurden ab dem 70-kV-Fremdnetz gespeist. Die Stränge C und D der Notstromanlage wurden über die entsprechenden Notstromdiesel gespeist. In den Strängen A und B standen nur die batterieversorgten Gleichstromschienen zur Verfügung; die Notstromschienen und die gesicherten Wechselstromschienen der Stränge A und B waren nicht verfügbar (siehe Unregelmässigkeit 5).

Grundsätzlich ist auslegungsgemäss in den ersten 30 Minuten keine Operateurhandlung notwendig. Die Schichtmannschaft benötigte etwa 20 Minuten, um sich über den Zustand der Anlage Klarheit zu verschaffen und sich zu vergewissern, dass die wichtigsten Schutzziele (Reaktorabschaltung, Kernkühlung) eingehalten waren. Die Arbeit der Schichtmannschaft im Kommandoraum erwies sich als recht schwierig, da durch den Ausfall der gesicherten

Wechselstromschienen A und B auch die dazu gehörenden Messeinrichtungen sowie deren Registrierung, Anzeige und Überwachung ausgefallen waren. Die Anzeigen der Eigenbedarfsanlage waren komplett ausgefallen; übergeordnete Anzeigen, die Resultat von Verknüpfungen mehrerer Signale sind, funktionierten nur teilweise.

Die erfolgreiche Abschaltung des Reaktors und dessen Unterkritikalität konnten vom Schichtpersonal anhand der Neutronenflussinstrumentierung festgestellt werden. Auch konnten die korrekte Funktion der verbleibenden 2 Notstränge, im Speziellen der Notspeisewassersysteme, und die Stabilisierung des Wasserniveaus im Reaktordruckbehälter auf minimal 1,9 m über Kernoberkante beobachtet werden, siehe Abbildung 3.

2.3.8 Wiederherstellung der vollständigen Stromversorgung

Ca. 20 Minuten nach Ereigniseintritt war das Störfalleitschema (Notfallanweisungen in der Art von Checklisten) abgearbeitet. Die Schichtmannschaft diskutierte die möglichen Massnahmen für eine Wiederherstellung der Wechselstromversorgung auf den Strängen A und B der Notstromanlage. Sie entschied sich für die Zuschaltung der entsprechenden Notstromschienen auf die Eigenbedarfsschienen, die ihrerseits vom 70-kV-Fremdnetz gespeist waren (vgl. Abschnitt 2.3.6). Dies verlief erfolgreich und somit waren etwa 22 Minuten nach Ereigniseintritt sämtliche Schienen der Eigenbedarfs- und Notstromanlagen wieder unter Spannung. Somit waren auch die Anzeigen im Kommandoraum wieder verfügbar und die Notsysteme in allen vier Strängen wieder in Betrieb.

2.3.9 Überführen in sicheren Zustand

30 Minuten nach Ereigniseintritt war der sichere Füllstand "extra-hoch" (4,7 m über Kernoberkante) im Reaktordruckbehälter erreicht (vgl. Abbildung 3). Etwa 45 Minuten nach Ereigniseintritt war der zweite Durchgang durch das Störfalleitschema abgeschlossen. Die Anlage befand sich im stabilen Zustand "heiss abgestellt" und wurde vorläufig so belassen.

Am Vormittag des darauf folgenden Tages wurde die Anlage in den Zustand "kalt abgestellt" abgefahren, um Massnahmen gegen zwischenzeitlich erkannte oder vermutete Defizite, namentlich in den Eigenbedarfs- und Notstromanlagen, zu ergreifen.

2.4 Direkte Ursachen und Grundursachen

Die direkten Ursachen für die eingetretene Sequenz von Fehlfunktionen liegen gemäss Ergebnis der Abklärungen zu wesentlichen Teilen in Ausführungsmängeln und konzeptionellen Schwächen. Diese stehen in mehreren Fällen im Zusammenhang mit vorgenommenen Anlagenänderungen, womit Schwächen im Änderungswesen und damit im organisatorischen Bereich angesprochen sind.

In einem grösseren Zusammenhang ist ein Grossteil der festgestellten Mängel und Schwächen als Ausdruck mangelnder Sicherheitskultur zu verstehen. Somit ist eine mangelhafte Sicherheitskultur als wesentliche Grundursache zu sehen. Dies geht aus einem internen Bericht der Betreibergesellschaft FKA vom 23.10.2006 hervor, der der Aufsichtsbehörde Statens Kärnkraftinspektion (SKI) zugespielt und damit anfangs 2007 publik geworden ist [6]. Gewisse Mängel und Schwächen, die für den Ereignisablauf massgebend waren, sollen sogar bekannt gewesen sein. Sie seien aber im betrieblichen Alltag zu Selbstverständlichkeiten geworden oder nicht mit der notwendigen Dringlichkeit und Konsequenz angegangen worden. Siehe dazu Abschnitt 6.1.

3 Massnahmen der schwedischen Betreiber und der Aufsichtsbehörde SKI

3.1 Unmittelbare Massnahmen

Der Betreiber informierte die Aufsichtsbehörde SKI umgehend über die Reaktorschnellabschaltung und nach den ersten Analysen auch weitere KKW in Schweden und Finnland, dass erkannte Fehler grundsätzlicher Art sein könnten.

Am 28. Juli verlangte das SKI von allen Betreibern Informationen über das Verhalten ihrer Anlagen bei einem solchen Ereignis. In der Folge beschloss der Betreiber OKG, die Anlagen Oskarshamn 1 und 2 für weitere Analysen abzuschalten. Forsmark 1 war wegen des hier besprochenen Zwischenfalls ausser Betrieb und Forsmark 2 in Revision. Wie das SKI am 4. August aufgrund der eingeholten Informationen bekannt gab, waren keine weiteren Abschaltungen notwendig [7]. In den vier ähnlich konzipierten Anlagen Forsmark 1 und 2 sowie Oskarshamn 1 und 2 mussten Nachbesserungen an den Notstromversorgungen durchgeführt werden.

3.2 Betriebsfreigabe mit Bedingungen

Das SKI setzte für die Wiederinbetriebnahme von Forsmark 1 und 2 voraus, dass die erkannten technischen Mängel in verschiedenen Teilen der Stromversorgung behoben werden [8].

Die Freigabe für das Wiederanfahren erfolgte am 28. September und war mit einer Anzahl von Forderungen für weitere mittel- und langfristige Aktionen verbunden [9]: Umsetzungspläne für die Schichtausbildung hinsichtlich ausserordentlicher Situationen sowie für die Verbesserung des Änderungswesens und der Instandhaltung; Nachbesserung des Sicherheitsberichts bezüglich Störungen in der Stromversorgung; Offenlegung der Vorgaben auf Geschäftsleitungsebene bezüglich Sicherheitsfragen. Ausserdem wurden alle drei Blöcke des KKW Forsmark einem generell erhöhten Aufsichtsregime unterworfen.

3.3 Einstufung INES 2

Die internationale Ereignisskala für Kernanlagen (International Nuclear Event Scale, INES) bildet eine Grundlage für die Bewertung von Ereignissen nach einheitlichen Regeln. Sie wurde 1990 von IAEA und NEA eingeführt und umfasst die sieben Stufen von INES 1 ("Anomalie") bis INES 7 ("Katastrophaler Unfall"). Unterhalb der Skala wird für Abweichungen von geringer sicherheitstechnischer Wichtigkeit ("significance") auch die Einstufung INES 0 verwendet. Ereignisse ohne sicherheitstechnische Bedeutung ("relevance") fallen ausser Betracht ("out of scale").

Mit Datum 27. Juli 2006 hat das SKI das Ereignis von Forsmark 1 provisorisch als INES 2 ("Zwischenfall") klassiert und dies am 24. August 2006 mit der endgültigen Klassierung bestätigt [10]. Grundsätzlich sind Ereignisse der Stufe INES 2 gekennzeichnet durch bedeutendes Versagen von Sicherheitseinrichtungen, wobei aber noch genügend gestaffelte Massnahmen verbleiben, um zusätzliche Abweichungen bewältigen zu können.

Diese Einstufung wurde wie folgt begründet: Die Abschaltung des Reaktors und die Nachwärmeabfuhr als die wesentlichen Sicherheitsfunktionen waren nach Beurteilung des SKI mit genügenden Reserven gewährleistet. Anhand des INES-Handbuchs wurde für das Ereignis von Forsmark 1 eine Basiseinstufung INES 1 ("Anomalie") ermittelt. Bei der Einstufung INES 1 handelt es sich grundsätzlich um Ereignisse mit einer Bedeutung für die Sicherheit,

aber bedeutenden Reserven hinsichtlich gestaffelter Massnahmen. Diese Basiseinstufung ist aber wegen CCF-Aspekten (systematischer Mehrfachausfall) beim Ausfall von zwei gesicherten Wechselstromschienen (siehe Abschnitt 2.3.4, Unregelmässigkeit 5) um eine Stufe zu erhöhen. Massgebend dafür ist die Überlegung, dass der nicht ausschliessbare Ausfall der gesicherten Wechselstromschienen in den verbleibenden Strängen zu einer Konfiguration geführt hätte, die durch den Sicherheitsbericht von Forsmark 1 nicht abgedeckt ist.

3.4 Weitere Entwicklung

Aufgrund der publik gewordenen betriebsinternen Kritik bezüglich Sicherheitskultur trat im Februar 2007 der Chef der FKA zurück und darüber hinaus wurden weitere Umbesetzungen in der Führungsspitze des KKW Forsmark vorgenommen [11]. Bereits zuvor hatte die intensivierte Aufsicht u.a. zur Folge, dass Forsmark 2 im Oktober 2006 vorübergehend abgeschaltet werden musste, weil von der Aufsichtsbehörde verlangte Prüfdokumente für eine Schweißnaht am Containment² nicht gefunden wurden [12]. Am 3.2.2007 nahm der Betreiber die beiden Blöcke Forsmark 1 und 2 wegen einer Unregelmässigkeit mit einer Gummidichtung des Containments erneut ausser Betrieb [12]. Für die Gummidichtung war das Datum für den unbedenklichen Einsatz überschritten, aber weder ein Ersatz noch eine Tauglichkeitsprüfung für eine allfällige Weiterverwendung war vorgenommen worden.

Am 29.1.2007 erstattete das SKI Anzeige gegen den Betreiber von Forsmark 1, weil im unmittelbaren Nachgang zum Vorkommnis vom 25.7.2006 die Anlage erst verzögert in den Zustand "kalt abgestellt" abgefahren wurde [12]. Die Anlage war zunächst während etwa 18 Stunden im Zustand "heiss abgestellt" belassen worden (vgl. Abschnitt 2.3.9). Dieser Zustand gilt gemäss schwedischem Regelwerk nicht als "sicherer Zustand". Stand und damit auch das Ergebnis des Rechtsverfahrens sind der KSA z.Z. des Redaktionsschlusses für den vorliegenden Bericht nicht bekannt.

4 Massnahmen der schweizerischen Aufsichtsbehörde HSK

4.1 Untersuchungen

Mit Brief vom 14. August forderte die HSK die Betreiber der schweizerischen KKW auf, die Stromversorgung ihrer Anlagen (nach damaligem Kenntnisstand insbesondere den Überspannungsschutz) nochmals detailliert zu überprüfen, und verlangte in diesem Sinn kurzfristig per Mitte bzw. Ende August Antworten auf eine Reihe von Fragen [13]. Diese betrafen das Verhalten der Anlage bei externen elektrischen Ereignissen (z.B. Kurzschlüssen und Überspannungen im Übertragungsnetz), insbesondere die Sicherstellung der Funktionsfähigkeit bzw. die Konsequenzen eines Ausfalls von essenziellen Systemen: Sicherheitssysteme für die Störfallbeherrschung, Notstromversorgung (gesicherte Schienen, vgl. Abschnitt 2.1.2) sowie Mensch-Maschine-Schnittstelle (Anzeigen und Bedienelemente). Ein weiterer Themenkreis betraf die Frage, ob die massgebenden Elemente des Zwischenfalls von Forsmark am Anlagensimulator berücksichtigt werden können. Aufgrund der Antworten [14] und der Erkenntnisse aus der ersten Analyse konnte festgehalten werden, dass ein gleichartiges Versagen der Notstromversorgung ausgeschlossen werden könne und sich keine Sofortmassnahmen aufdrängten.

² Das Containment (Sicherheitsbehälter) ist im Fall eines schweren Unfalls die letzte Sicherheitsbarriere gegen die Freisetzung von Radioaktivität. Die Dichtheit ist für die Einschlussfunktion essenziell.

Die Untersuchungen und Massnahmen sowohl in den KKW wie bei der HSK waren damit aber noch nicht abgeschlossen. Im vierten Quartal 2006 verschaffte sich die HSK mit Inspektionen in allen KKW Gewissheit darüber, dass die notwendigen Lehren für die Ausbildung und das Simulatortraining gezogen und die Massnahmen umgesetzt werden.

4.2 Bericht und Empfehlungen der HSK

Im Februar veröffentlichte die HSK ihren Bericht [1] zum Zwischenfall von Forsmark und dessen Bedeutung bezüglich der schweizerischen KKW. Die HSK geht darin ausführlich auf die Konzeption der Eigenbedarfs- und Notstromversorgung der schweizerischen KKW, die vorhandenen Schutzeinrichtungen und die Erfahrungen aus relevanten Vorkommnissen im elektrotechnischen Bereich ein. Sie stellte fest, dass in den Bereichen, die in Forsmark 1 als Schwachstellen identifiziert worden waren und massgeblich zum komplexen Störfallablauf beigetragen hatten, keine Lücken in den technischen und organisatorischen Vorkehrungen der schweizerischen KKW vorhanden seien.

Aufgrund ihrer Untersuchungen gelangte die HSK trotz des insgesamt positiven Bildes zu folgender Empfehlung bzw. Forderung an die schweizerischen KKW:

- Simulatoreausbildung des Schichtpersonals: Die HSK empfiehlt, noch vermehrt den Umgang mit Ausfällen von Redundanzen der Sicherheitssysteme oder der Energieversorgung sowie den Umgang mit dem Ausfall von Informationssystemen und Anzeigen im Kommandoraum zu schulen.
- Auswertung von Vorkommnissen und Betriebserfahrungen in ausländischen Anlagen: Die HSK erwartet von den schweizerischen KKW, dass sie die dafür notwendigen Ressourcen bereitstellen.

5 Zu technischen Ursachen und Aspekten menschlichen Handelns

5.1 Anlageninterne Stromversorgung

5.1.1 Generelle Konzeption

Die Eigenbedarfs- und Notstromanlagen der schweizerischen KKW unterscheiden sich in ihrer Konzeption von derjenigen von Forsmark 1 (vgl. Abschnitt 2.1.2). Die HSK geht in ihrem Bericht [1] ausführlich darauf ein. Im vorliegenden Zusammenhang besonders wichtig ist, dass die leittechnischen Einrichtungen in den schweizerischen KKW mehrheitlich direkt von Batterien gespeist werden. Durch die direkte Batterieanspeisung wird die sicherheitstechnische Bedeutung der USV-Anlagen relativiert. Wie der HSK-Bericht zeigt, kann auch dann von einem unkritischen Verlauf ausgegangen werden, wenn bei den schweizerischen KKW die weiteren, nicht USV-bezogenen technischen Unregelmässigkeiten des Zwischenfalls von Forsmark unterstellt würden.

Für die KSA ist aufgrund der elektrotechnischen Analysen im Nachgang zum Zwischenfall von Forsmark die Feststellung zentral, dass sich eine Störung in der Eigenbedarfsversorgung gleichzeitig auf alle Redundanzen der Sicherheitssysteme negativ auswirken kann; siehe dazu Abschnitt 5.1.3.

5.1.2 Schulung hinsichtlich Systemausfällen

Die HSK gelangt zwar, wie oben erwähnt, zu einer günstigen Schlussfolgerung bezüglich technischer Konzeption der anlageninternen Stromversorgung in den schweizerischen KKW. Sie gibt aber im Sinn guter Vorsorge die Empfehlung ab, bei der Simulatorenausbildung des Schichtpersonals noch vermehrt den Umgang mit Ausfällen von Redundanzen der Sicherheitssysteme oder der Energieversorgung zu schulen. Die KSA unterstützt diese Empfehlung.

Im Rahmen der Umsetzung der HSK-Empfehlung soll auch überprüft werden, wie weit die Schulung alle denkbaren Störfälle in der anlageninternen Energieversorgung abdeckt.

Die Beübung des Schichtpersonals setzt voraus, dass auch entsprechende Simulationsmöglichkeiten bestehen. Nach Kenntnisstand der KSA ist der Bereich der Eigenbedarfsversorgung in den Simulatoren der schweizerischen KKW in unterschiedlicher Tiefe nachgebildet. Dabei ist aber sicherzustellen, dass die Simulatorenausrüstung für Schulungen hinsichtlich gestörter Energieversorgung hinreichend ist. Insbesondere sollen auch Störungen mit einer Spannungstransiente in der Schaltanlage simuliert werden können.

5.1.3 Spannungstransiente als mögliche Ursache für Common-cause-Fehler

Eine Spannungstransiente im Bereich des Netzanschlusses eines Kraftwerks wirkt sich auf die gesamte Eigenbedarfsanlage aus und ist somit eine mögliche Ursache für Common-cause-Fehler (CCF) bei Verbrauchern, die an die Eigenbedarfs- und Notstromanlage angeschlossen sind (vgl. Abschnitt 2.1.2).

Spannungstransienten können aus verschiedenen Gründen entstehen, u.a.:

- Kurzschlüsse und Erdschlüsse in der Hochspannungsanlage (längere Transienten im Zeitbereich von Sekunden);
- Blitzeinschlag und Schalthandlungen im Netz (kürzere Transienten);
- Lastabwurf auf Eigenbedarf; dies führt zu Überspannungen, d.h. Spannungen im Bereich von 120 bis 130% der Nominalspannung.

Auch Störungen oder Fehler in der Generatorerregung können Spannungstransienten zur Folge haben. Massgebend für die in diesem Fall auf das Kraftwerk einwirkende Spannungserhöhung ist der im Generatorschutz eingestellte Grenzwert, der die Öffnung des Generatorschalters auslöst.

Wie gross die Spannungstransienten ausfallen, ist abhängig von vielen Parametern wie Störungsort, Dämpfungsverhalten der Netzkomponenten, Art der Erregung, Schutzeinstellungen usw., ist somit für jede Anlage unterschiedlich und kann rechnerisch ermittelt werden.

Spannungstransienten können unerwartete Reaktionen zur Folge haben. Während Starkstromkomponenten in dieser Hinsicht relativ unempfindlich sind, ist bei Gleichrichtern, Wechselrichtern oder leitetechnischen Komponenten eher mit Folgen zu rechnen, weil bei diesen Komponenten Grenzwertüberwachungen zu Reaktionen führen können. Zu vermeiden sind Auslösungen, die nach Normalisierung der Situation zeitintensive lokale Handrückstellungen verlangen.

In den schweizerischen KKW sind schon mehrmals Ereignisse eingetreten, die Spannungstransienten zur Folge hatten. In ihrem Bericht [1] geht die HSK auf diejenigen Ereignisse ein, denen ein ähnliches auslösendes Ereignis zugrunde lag wie beim Zwischenfall von Forsmark, nämlich eine Störung im externen Netz. Laut HSK ist in keinem dieser Fälle die sogenannte gesicherte Stromversorgung (vgl. Abschnitt 2.1.2) eines schweizerischen KKW beeinträchtigt worden.

Der Zwischenfall von Forsmark zeigt aber, dass Transienten bzw. Überspannungen, die grösser ausfallen als bei der Auslegung der Kraftwerksanlage unterstellt, unerwartete Folgen haben können. In Forsmark 1 wirkte sich besonders negativ aus, dass einige an den gesicherten Schienen angeschlossene Verbraucher (Anzeigen im Kommandoraum, Drehzahlregelung der Notstromdiesel) beeinträchtigt waren. Um dies zu vermeiden ist sicherzustellen, dass sicherheitsrelevante Leittechnik und Informationssysteme sowie deren Anspeisung auch beim Erreichen des oberen Bandes der möglichen Spannungstransienten verfügbar bleiben.

5.1.4 Empfehlungen

- Die KSA unterstützt die Empfehlung der HSK, bei der Simulatorenausbildung des Schichtpersonals noch vermehrt den Umgang mit Ausfällen von Redundanzen der Sicherheitssysteme oder der Energieversorgung zu schulen. Dabei soll auch überprüft werden, wie weit die Schulung alle denkbaren Störfälle in der anlageninternen Energieversorgung abdeckt. Ausserdem soll sichergestellt werden, dass die Simulatoren der schweizerischen Kernkraftwerke für Schulungen hinsichtlich gestörter Energieversorgung, insbesondere auch Spannungstransienten in der Schaltanlage, hinreichend ausgerüstet sind.
- Mit Blick auf das Potenzial für Common-cause-Fehler, das von Störungen in der Eigenbedarfsversorgung ausgeht, empfiehlt die KSA zudem, die für Störungen in der Eigenbedarfsversorgung zu unterstellende maximale Spannungstransiente nach konservativen Grundsätzen neu zu überprüfen und allenfalls neu festzulegen. Im Fall einer Neufestlegung soll sichergestellt werden, dass die für die Sicherheit massgebenden elektrotechnischen und elektronischen Komponenten so ausgelegt sind, dass sie im Rahmen der zu unterstellenden Spannungstransiente korrekt funktionieren und bei deren Überschreiten sicherheitsgerichtete Systemreaktionen auslösen.

5.2 Funktionsprüfungen und unerkannte Fehler

5.2.1 Periodische Funktionsprüfungen in den schweizerischen Kernkraftwerken

Sicherheitssysteme werden auf Anforderung in Betrieb genommen; im Normalbetrieb eines KKW sind sie in Bereitschaft. Da allfällige Ausfälle bzw. Fehler im Bereitschaftsmodus nur bedingt erfasst werden können, sind periodische Funktionsprüfungen für Sicherheitssysteme notwendig.

Weltweit wird in den KKW die Funktionstüchtigkeit der Komponenten und Systeme mehrheitlich mit periodischen Funktionsprüfungen getestet. In den schweizerischen KKW sind die entsprechenden Testanforderungen sowohl für Sicherheitssysteme als auch für sicherheitsrelevante Systeme in den Technischen Spezifikationen festgelegt. Ähnliche Tests machen die Betreiber auch an Betriebssystemen, um die Verfügbarkeit der Kraftwerksanlage zu gewährleisten.

Die periodischen Funktionstests lassen sich grob in 5 Kategorien unterteilen:

- Plausibilitätsprüfung von Signalen durch Vergleich mit Referenzwerten (Kanalfunktions-Check)
- Prüfung von Signalen mittels Testsignal (Kanalfunktions-Test)
- Eichen von Signalkanälen (Kanalkalibrierung)
- Funktionstest aller Komponenten eines Teilsystems (System-Funktionstest)
- Test der gesamten Steuerungslogik eines Teilsystems (Systemlogik-Funktionstest)

Mit diesen verschiedenen Testarten werden Teilsysteme abschnittsweise, jedoch an den Abschnittsgrenzen überlappend geprüft, sodass gesamthaft eine durchgehende Prüfung aller Pfade eines Teilsystems ab Sensoren bis hin zu den aktiven Komponenten resultiert. In der angegebenen Reihenfolge der Testarten nimmt der Umfang der einbezogenen Teile in der Regel zu und die Wiederholungshäufigkeit ab. Mit zunehmender Komplexität der Tests wird deren Durchführung während des Betriebs schwierig oder ist gar nicht möglich. Deshalb werden die grossen, integralen Tests, mit denen das Zusammenwirken von verschiedenen Komponenten und Teilsystemen einer Systemgruppe geprüft wird, in den Revisionsstillstand verlegt.

Die verschiedenen Funktionsprüfungen haben verschiedene Testintervalle. Die Länge der Intervalle beruht zum grössten Teil auf Erfahrungswerten und auch auf probabilistischen Betrachtungen zu den Ausfallraten. Sie ist abhängig einerseits von der Wichtigkeit der zu prüfenden Systeme in Bezug auf die Sicherheit und andererseits von der gegebenen Situation bezüglich Prüfbarkeit der Komponenten und Systeme.

Der Nachweis der Funktionstüchtigkeit von Systemen und Komponenten mittels Funktionstests hat in den schweizerischen Kernanlagen einen ausgereiften Stand erreicht und kann mit dem gegebenen Anlagen-Design nicht mehr nachhaltig verbessert werden.

5.2.2 Grenzen von Funktionsprüfungen

Grosse, integrale Tests, wie beispielsweise die Prüfung des korrekten Verhaltens der Anlage bei einem Notstromfall (vollständiger Verlust der externen Stromversorgung), werden durch definierte Massnahmen eingeleitet, im genannten Fall durch das Öffnen der entsprechenden Leistungsschalter. Damit kann objektiv überprüft werden, ob die Anlage dem erwarteten Verhalten folgt. Mit diesem definierten Vorgehen können aber nicht alle elektrischen Transienten abgedeckt werden.

Im Gegensatz dazu hat ein Ausfall der externen Stromversorgung infolge einer Netzstörung, wie sie in Forsmark aufgetreten ist, einen weniger klar definierten Verlauf zur Folge. Die Auswirkungen von Netzstörungen und insbesondere Kurzschlüssen hängen von der Art des Kurzschlusses, vom Ort relativ zur Schaltanlage, der Netzbelastung und den Einstellungen der Schutzvorrichtungen der Schaltanlage ab. Streng genommen ist der Lastfall nach oben offen.

Die auftretenden Belastungsspitzen einer realen betrieblichen Transiente können in ungünstigen Fällen den wirksamen Bereich der Schutzeinrichtungen übersteigen. Daraus ergibt sich, dass Funktionsprüfungen für extreme Lastzustände nicht durchgeführt werden können: Die dafür erforderliche Ausrüstung der Anlage mit entsprechenden Testeinrichtungen, der mit der Funktionsprüfung verbundene Verschleiss oder das Schadenspotenzial an der Anlage wären unverhältnismässig.

Gewisse Prüfungen, die komplex sind, einen unverhältnismässigen Vorbereitungsaufwand bedingen oder ein gewisses Schadenspotenzial beinhalten, können faktisch nur während der Bau- und Inbetriebnahmephase durchgeführt werden. Ein wesentlicher Gesichtspunkt für diese Einschränkung ist der Verlust an Verfügbarkeit der Anlage. Diesbezüglich sind die Voraussetzungen für anspruchsvolle Funktionsprüfungen während einer Bau- und Inbetriebnahmephase in der Regel wesentlich günstiger. Gründe dafür sind u.a. bessere Zugänglichkeit, isolierte Teilsysteme und deshalb besser kontrollierbare Konsequenzen sowie verfügbare Fachspezialisten. Diese Möglichkeit gilt es nicht nur bei allfälligen Neubauten, sondern auch bei Anlagenerneuerungen und Nachrüstungen konsequent zu nutzen.

5.2.3 Massnahmen gegen unerkannte funktionale Fehler in Anlagen

Beim Zwischenfall von Forsmark spielte eine Reihe von Auslegungsfehlern und Ausführungsmängeln eine Rolle. Diese hatten sich im Zuge von Anlagenänderungen eingeschlichen und waren weder bei der Inbetriebsetzung der entsprechenden Systeme noch bei den periodischen Funktionsprüfungen entdeckt worden. Wie im vorangehenden Abschnitt erwähnt, können gewisse Überprüfungen an Komponenten und Systemen nur im Zug der Inbetriebsetzung durchgeführt werden. Unterlassungen können demzufolge u.U. für die gesamte Systemlebensdauer nicht mehr nachgeholt werden. Die Durchführung eines umfassenden Prüfprogramms, auch mit "scharfen" und allenfalls für die Systeme anspruchsvollen Tests, ist deshalb im Rahmen der Bau- und Inbetriebnahmephase von neuen Komponenten und Systemen sicherzustellen.

Weitere Überprüfungsmöglichkeiten ergeben auch betriebliche Transienten, die sich auf neu eingebaute Komponenten oder auf kürzlich geänderte Systeme auswirken. Solche Transienten sind Folge von unerwarteten auslösenden Ereignissen oder sie werden von Hand ausgelöst, um das dynamische Verhalten der Gesamtanlage zu testen, z.B. ein Lastabwurf. Die sorgfältige Analyse des Verhaltens von neuen oder geänderten Komponenten oder Systemen in solchen Transienten kann Abweichungen gegenüber dem Sollverhalten aufdecken und somit auf Schwächen oder Fehler hinweisen.

Die Inbetriebnahmetests und die Analyse von Transienten dienen vor allem dazu, allfällige Mängel in der Auslegung oder Ausführung von Komponenten oder Systemen zu erkennen und zu eliminieren. Speziell in den ersten Betriebsjahren können auch die periodischen Funktionstests gemäss Abschnitt 5.2.1 entsprechende Mängel aufdecken helfen. Vor allem aber wird mit den periodischen Funktionstests vermieden, dass im Laufe der Betriebszeit bzw. Bereitschaftszeit entstehende Fehler in einzelnen Komponenten unentdeckt bleiben.

Weitere Hinweise auf Schwächen einer Anlage können Ereignisse und Betriebserfahrungen von andern, insbesondere auch ausländischen Anlagen liefern. Allerdings ist die Flut von verfügbarer Information gross, was einer oberflächlichen Prüfung Vorschub leisten kann; vgl. dazu Abschnitt 6.2.1.

5.2.4 Empfehlungen

- Den Prüfmöglichkeiten ist bei der Systemkonzeption grosse Beachtung zu schenken. Im Zug der Baufreigaben soll sichergestellt werden, dass alle Einrichtungen im Systemkonzept enthalten sind, damit die erforderlichen periodischen Funktionsprüfungen vorgenommen werden können. Insbesondere sollen auch die entsprechenden Vorgaben im Regelwerk überprüft werden.
- Im Zug der Bau- und Inbetriebnahmephase von neuen Komponenten oder Systemen ist ein umfassendes Prüfprogramm durchzuführen. Damit soll insbesondere auch die funktional korrekte Montage sichergestellt werden; auch Prüfungen mit hoher Systembeanspruchung sind notwendig.
- Das Verhalten bei Transienten von sicherheitsrelevanten Systemen und Komponenten, die geändert oder erneuert worden sind, soll systematisch ausgewertet werden.

5.3 Informationen für das Schichtpersonal im Kommandoraum

5.3.1 Allgemeine Erfordernisse

Die Abarbeitung der ereignis- bzw. symptomorientierten Störfallvorschriften basiert auf Anzeigen sicherheitsrelevanter Anlagenparameter und dem Zustand wichtiger Komponenten. Deshalb ist es wichtig, dass die Informationen, die für die Störungserkennung und die Bestimmung einzuleitender Massnahmen erforderlich sind, dem Schichtpersonal im Kommandoraum jederzeit zur Verfügung stehen. Neben den aktuellen Messwerten und Zustandsmeldungen ist für die Lagebeurteilung und Trendverfolgung auch die Registrierung wichtiger Anlagenparameter unerlässlich. Wichtig sind ebenfalls funktionstüchtige Kommunikationsmittel. Vorteilhaft sind durch Informationstechnik gestützte Systeme, die Alarme und Meldungen nach Dringlichkeit und Vorrang selektionieren, mittels ergonomisch günstiger Darstellungen sicherheitsrelevanter Systeme und Parameter die Diagnose erleichtern und Anweisungen für die zu ergreifenden Massnahmen geben.

Die Anlagen sind sowohl in Schweden wie in der Schweiz so ausgelegt, dass zur Beherrschung eines Störfalles in den ersten 30 Minuten keine Operateureingriffe erforderlich sind. Das bedeutet aber nicht, dass dem Schichtpersonal die erforderlichen Informationen für die Lageanalyse nicht zur Verfügung stehen müssen und dass keine Schalthandlungen vorgenommen werden dürfen. Erfahrungsgemäss können frühe Schalthandlungen der Operateure den Ablauf eines Störfalles günstig beeinflussen. Geeignete Schalthandlungen setzen eine korrekte Beurteilung der Situation voraus, und dies wiederum setzt abgesehen von Schulung und Übung voraus, dass die obgenannten Mittel im Kommandoraum verfügbar sind und jederzeit ein richtiges Bild des Anlagenzustandes liefern.

5.3.2 Informationen im Kommandoraum in den schweizerischen Kernkraftwerken

Wie der Zwischenfall von Forsmark gezeigt hat, können Ausfälle in der unterbrechungslosen Notstromversorgung zu Ausfällen von Anzeigen, Registriereinrichtungen und Kommunikationsmitteln im Kommandoraum und damit zu Problemen bei der Beurteilung des Anlagenzustandes führen.

Anzeige- und Registriergeräte benötigen für ihre Verfügbarkeit eine durchgehende Stromversorgung auf dem vollständigen Signalpfad, d.h. vom Messwertgeber via Signalverarbeitung bis zur Anzeige auf einem Instrument oder einem Bildschirm bzw. Aufzeichnungsgerät. Wichtig für die Beurteilung sind ebenfalls Rückmeldungen von Komponentenzuständen sowie Alarmmeldungen, die ebenfalls auf eine entsprechende Anspeisung angewiesen sind. Gemäss Abklärungen im Nachgang zum Zwischenfall von Forsmark [1] erfüllen die in den schweizerischen KKW installierten Systeme zur sicheren Stromversorgung sicherheitstechnisch wichtiger Systeme ihre Funktion auch beim Auftreten störungsbedingter Spannungstransienten zuverlässig. Dies wird durch die Erfahrung aus den bisher aufgetretenen Störungen in der externen Stromversorgung bestätigt.

Auch in schweizerischen KKW steht bei Verlust der externen Spannung nicht mehr die ganze Instrumentierung im Kommandoraum zur Verfügung. Die zur Beurteilung des Anlagenzustands notwendige Information steht aber dem Schichtpersonal jederzeit zur Verfügung. Durch den Teilverlust von Information entsteht jedoch für das Schichtpersonal eine ungewohnte Situation, die sich belastend auswirken und ein entsprechendes Potenzial für ungünstiges Verhalten oder sogar fehlerhafte Massnahmen schaffen kann. Um dies zu vermeiden, muss geschult werden, wie allenfalls fehlende Informationen zur Bestimmung von geeigneten Massnahmen aufgrund von alternativen, noch vorhandenen Messwerten, Anzeigen oder Indikatoren abgeleitet werden können oder wie unsicher erscheinende Informationen auf ihre Verlässlichkeit hin überprüft werden können. Zudem ist sicher-

zustellen, dass die Stör- und Notfallanweisungen die entsprechenden Vorgehensweisen unterstützen. Sodann muss der Umgang mit dem Verlust von Informationen im Rahmen des Simulatortrainings angemessen geübt werden.

Gleichzeitig weist die KSA aber darauf hin, dass die Schulung im Hinblick auf Informationsverlust zwar eine sinnvolle sicherheitsgerichtete Massnahme ist, der jedoch eine bestmöglich robuste Gestaltung der Anlage vorangehen muss. Denn anlagentechnische Massnahmen sind sicherheitstechnisch grundsätzlich administrativen Massnahmen (z.B. Schulung) überlegen.

Die HSK hat in ihrem Bericht [1] eine Empfehlung betreffend Simulatorschulung abgegeben. Sie hat sich bei Inspektionen in den einzelnen Werken davon überzeugt, dass Störfälle mit Ausfall von Informationssystemen und Anzeigen im Rahmen der Simulatorschulung geübt werden und das Betriebspersonal auf solche aussergewöhnlichen Situationen vorbereitet ist. Die KSA unterstützt diese Empfehlung der HSK.

5.3.3 Rechnergestützte Systeme

Die Anzeigen für sicherheitsrelevante Grössen im Kommandoraum der schweizerischen KKW sind, dem Stand der Technik bei deren Projektierung entsprechend, in der Regel dezentral ausgeführt, d.h. sie werden über den gesamten Signalpfad mit direkt zugehörigen (dedizierten) Ketten von Elektronikkomponenten verarbeitet. Diese Komponenten werden redundant von Batterien angespeist und sind somit von Netz und Notstromdieseln unabhängig.

Bei Ersatzbedarf und aufgrund der allgemeinen Entwicklung in der Mess-, Steuer- und Regeltechnik werden die bisherigen dezentralen Anzeigen zunehmend durch rechnergestützte Informationssysteme mit Bildschirmanzeigen ersetzt. Dabei werden Rechner eingesetzt, die beim heutigen Stand der Digitaltechnik im Prinzip je einzeln eine Grosszahl von Signalen in Quasi-Echtzeit verarbeiten können und die resultierenden Grössen über flexibel einsetzbare Bildschirme ausgeben. Für derartige Systeme sind üblicherweise Wechselstrom-Anspeisungen erforderlich. Diese eignen sich weniger gut für eine redundante Ausführung als Gleichstrom-Komponenten. Ausserdem ist die bei Bildschirmen übliche Steckerverbindung für die Stromversorgung leicht versetzbar, was zu Abweichungen vom vorgesehenen Versorgungspfad führen kann.

Für diese Anwendungen sind ausfallsichere Anspeisungen wichtig. Mit der absehbaren zunehmenden Verbreitung derartiger Informationssysteme ist in Zukunft noch vermehrt auf die Sicherstellung von deren Anspeisungen, auch bei Redundanzverlust, zu achten.

Abgesehen von ausgefallenen Anzeigen ergaben sich beim Zwischenfall von Forsmark für die Schichtmannschaft Schwierigkeiten aus nicht korrekt angezeigten Informationen. Dies kann bei Auswahlhaltungen von mehreren Messwerten der gleichen Prozessgrösse oder bei berechneten Werten, die von mehreren Eingangssignalen abhängig sind, eine Folge davon sein, dass die Anzeigewerte bei Ausfall von einzelnen Messgrössen nicht korrekt ermittelt werden. Kann ein Anzeigewert nicht zuverlässig ermittelt werden, muss der Ausfall klar erkennbar sein. Dieser Problematik ist besonders bei der Programmierung von rechnergestützten Systemen gebührend Beachtung zu schenken.

5.4 Rückwirkungen aus dem Netz und liberalisierter Strommarkt

Ein KKW ist für die Einspeisung seiner Stromproduktion an das Übertragungsnetz (höchste Spannungsebene, 400 kV oder 220 kV) angeschlossen und verfügt über mindestens eine weitere Einspeisung aus einem zweiten Netz (mittlere bis hohe Spannungsebene, Bereich

50 kV bis 220 kV), hier als Fremdnetz bezeichnet; vgl. dazu Abschnitt 2.1.2 und Abbildung 1 sowie Beilagen 1 bis 4 in [1]. Das Fremdnetz stellt in erster Linie die Eigenbedarfsversorgung bei Revisionsarbeiten an Anlagenteilen der höchsten Spannungsebene sicher; es kann auch als redundante Versorgung bei Störungen dienen. Die Verfügbarkeit dieser Netze hat Einfluss auf die Sicherheit des Kraftwerks.

Der Auslöser für den Zwischenfall von Forsmark war eine Fehlhandlung während Instandhaltungsarbeiten in der 400-kV-Schaltanlage. Kurzschlüsse und weitere Störungen können in Schaltanlagen und Netzen auch spontan durch technische Defekte auftreten. Deren Störungspotenzial nimmt in der Regel zu, je näher beim Kraftwerk sie stattfinden. Mit derartigen Störungen können grosse Energieströme (Leistung) verbunden sein und auf das Kraftwerk einwirken. Um die beteiligte Energie und somit das Schadenspotenzial möglichst zu beschränken, werden schnelle Schutzrichtungen vorgesehen. Solche Schutzrichtungen sind im Übertragungsnetz Stand der Technik; ausgereift ist auch die Prüfung von deren Wirksamkeit durch wiederkehrende Tests. Wichtig ist, dass sowohl die Einstellung der Schutzrichtungen wie die Arbeiten im Bereich Schaltanlage und Zuleitungen zwischen Netz- und Kraftwerksbetreiber koordiniert werden.

In der Schweiz war bisher die Schaltanlage für den Anschluss des Kraftwerkes an das Übertragungsnetz in der Regel unter Kontrolle des Kraftwerksbetreibers. Die Zugehörigkeit von Netz und KKW zur gleichen Organisation haben bislang im Allgemeinen eine gute Koordinationsgrundlage gebildet, die erhalten bleiben muss.

Mit der Neuorganisation des Strommarktes, insbesondere dem Stromversorgungsgesetz [15] (Teil-Inkraftsetzung am 15. Juli 2007, weitere Teile und zugehörige Verordnungen voraussichtlich 2008) und der Trennung von Produktion und Netz ergeben sich neue Aspekte. Die Verantwortung für das Übertragungsnetz liegt in der Schweiz neu bei der Netzgesellschaft Swissgrid. Sie hat für den sicheren, zuverlässigen und wirtschaftlichen Betrieb des Übertragungsnetzes zu sorgen. Eine wesentliche Stütze für hohe Verfügbarkeit und stabilen Betrieb ist der europäische Netzverbund im Rahmen der Union for the Co-ordination of Transmission of Electricity (UCTE). Der Netzverbund verlangt aber auch die Einhaltung von entsprechenden Betriebsvorschriften [16]. Aus physikalischen Gründen muss das gesamte europäische Verbundnetz stets im Gleichgewicht von Produktion und Verbrauch betrieben werden. Andernfalls kommt es zu Instabilitäten und schliesslich zum Netzzusammenbruch. Entsprechend sehen die UCTE-Vorschriften z.B. vor, dass bei zu hohem Verbrauch, was sich in sinkender Netzfrequenz äussert, Verbraucher abgeschaltet werden. Die Zuverlässigkeit der Stromversorgung ist eine europaweite Angelegenheit, die gegebenenfalls die Opferung von regionalen Stromversorgungen verlangt.

In analoger Weise können im Fall einer Überproduktion im Interesse des Netzbetriebs auch Kraftwerke vom Netz getrennt werden. Da im neu organisierten Strommarkt Produktion und Übertragungsnetz organisatorisch getrennt sind, werden gemäss gültigen Regelungen entsprechende Entscheide aus der Perspektive des Netzbetreibers gefällt. Dabei können berechnete erhöhte Ansprüche bestimmter Teilnehmer übersehen werden, namentlich die mit dem Netzanschluss eines KKW verbundenen Sicherheitsaspekte.

Im Zuge der Verselbständigung des Übertragungsnetzes sind deshalb Massnahmen zu treffen, damit die Netzanschlüsse von KKW weiterhin primär nach Anforderungen der Anlagensicherheit betrieben werden: Abgesehen von Schutzabschaltungen sind Versorgungsunterbrüche möglichst zu vermeiden. Die Aufnahme entsprechender Regelungen in die Stromversorgungsgesetzgebung ist zu prüfen.

Unabhängig davon bleibt selbstverständlich im Sinn einer robusten Anlagenkonzeption die Anforderung bestehen, dass Netzstörungen und somit auch Netzabschaltungen von einem KKW jederzeit sicher beherrscht werden.

Empfehlungen 5.4

Im Zusammenhang mit der Verselbständigung des Übertragungsnetzes ist sicherzustellen, dass

- Betrieb und Unterhalt der Schaltanlage zwischen Kernkraftwerk und Netzbetreiber sicherheitsgerichtet koordiniert sind;
- der Netzbetreiber die speziellen Anforderungen der nuklearen Anlagensicherheit beim Betrieb der Netzanschlüsse der Kernkraftwerke mit Priorität berücksichtigt.

5.5 Verfügbarkeit von Notstromanlagen

Beim Zwischenfall von Forsmark konnten zwei der vier Notstrom-Dieselmotoren (hier: Notstromdiesel) nicht aufgeschaltet werden, weil der für die Drehzahlregelung erforderliche Strom von der zugeordneten gesicherten Wechselstromschiene nicht zur Verfügung stand (vgl. Abschnitt 2.3.4, Unregelmässigkeit 5). Welchem System die Fehlerursache zugeordnet wird, ist im vorliegenden Fall diskutierbar; aber im Ergebnis lag eine Nichtverfügbarkeit von Notstromdieseln vor.

Auch aus den schweizerischen Kernanlagen wurden und werden Funktionsstörungen an Notstromdieseln gemeldet, die bei den regelmässigen Funktionsprüfungen auftreten und als Nichtverfügbarkeit im Anforderungsfall zu bewerten sind. Aufgrund der Anzahl Vorkommnisse ist die Nichtverfügbarkeit von Notstromdieseln in der KSA schon früher thematisiert worden. Die Häufigkeit derartiger Störungen ist laut früheren Aussagen der HSK im internationalen Vergleich nicht auffällig und wird damit begründet, dass das Gesamtsystem eines Notstromdiesels wegen der zahlreichen Nebensysteme recht komplex ist ("ein Kraftwerk im Kleinen"); wie beim Zwischenfall von Forsmark rührt ein erheblicher Teil der Nichtverfügbarkeiten von Nebensystemen der Notstromdieselanlagen her. Ausserdem ist der Bereitschaftsmodus mit seinen langen Stillstandszeiten insofern anspruchsvoll, als graduelle Abweichungen vom Sollzustand als Vorläufer für mögliche Störungen weniger gut erkennbar sind als bei regelmässigem Leistungsbetrieb.

Aufgrund der Beobachtung, dass Notstromdieselanlagen von KKW relativ hohe Nichtverfügbarkeiten aufweisen, regt die KSA an, die Konzeption der Notstromversorgung von KKW grundsätzlich zu hinterfragen. Aufgrund der im obigen Absatz angegebenen Begründung für Nichtverfügbarkeiten müsste in erster Linie ein Abbau von Komplexität gesucht werden (z.B. einfachere Prozessführung unter Inkaufnahme schlechterer Wirkungsgrade). Eine entsprechende Analyse soll aber nicht eng auf die bisherigen Konzepte mit einzelnen grossen Dieselmotoren beschränkt bleiben, sondern auch andere und neuartige Lösungsansätze einbeziehen. Insbesondere für allfällige neue KKW müssten auch möglichst geringe Systemanforderungen hinsichtlich Notstromversorgung (z.B. bezüglich Leistung, Schnellstart) angestrebt werden.

Empfehlung 5.5

Möglichkeiten zur deutlichen Senkung der Anzahl Nichtverfügbarkeiten von Notstromanlagen sollen in grundsätzlicher Art untersucht werden.

5.6 Probabilistische Sicherheitsanalysen vs. Zwischenfall von Forsmark

Mit Probabilistischen Sicherheitsanalysen (PSA) der Stufe 1 kann ermittelt werden, mit welcher Häufigkeit statistisch mit Kernschmelzen (d.h. mit einem schweren Unfall) zu rechnen ist. Zu diesem Zweck wird das KKW mit geeigneten logischen Strukturen und statistischen Werten für die Versagenswahrscheinlichkeit der verschiedenen Komponenten,

Systeme und Operateurhandlungen modelliert. Auf dieser Basis kann für ein umfassendes Spektrum von auslösenden Ereignissen, deren Häufigkeit aus der internationalen und anlagenspezifischen Betriebserfahrung abgeleitet wird, die Kernschadenshäufigkeit ermittelt werden. Aufgrund der erwähnten Struktur der PSA sind auch detailliertere Aussagen zum Einfluss der verschiedenen auslösenden Ereignisse oder einzelner Komponenten, Systeme oder Operateurhandlungen möglich, so dass insgesamt ein Bild über sicherheitstechnische Stärken und Schwächen eines KKW gewonnen werden kann.

Die Versagenhäufigkeiten werden aus der Betriebserfahrung abgeleitet und beschränken sich in der Regel auf statistische Werte für Komponenten- bzw. Systemversagen oder Fehlhandlungen. Bislang nicht bekannte Schwächen in der Auslegung oder nicht-statistische Fehler werden somit in der Regel in der PSA nicht berücksichtigt. Aufgrund der PSA-Methode wäre das zwar möglich; die Modellierung geht aber grundsätzlich davon aus, dass sich die Anlage so verhält, wie für die Auslegung unterstellt. Also gehen ungünstige oder fehlerhafte Systemkonzepte sowie Abweichungen von den Vorgaben der Auslegung infolge rechnerischer, methodischer oder logischer Fehler in der Regel nicht in die PSA ein. Naturgemäß enthalten auch Common-cause-Fehler (CCF) derartige Elemente und sind somit in einer PSA schwierig zu erfassen.

Mehrere Unregelmässigkeiten im Ablauf des Zwischenfalls von Forsmark fallen in die oben erwähnten Kategorien von Ausfällen, die in einer PSA nicht oder nur schwierig erfassbar sind. Folgende Beispiele seien erwähnt:

- Beim Verdrahtungsfehler in der Frequenzüberwachung (vgl. Abschnitt 2.3.4, Unregelmässigkeit 4) handelt es sich um einen Montagefehler.
- Beim Ausfall der USV (vgl. Abschnitt 2.3.4, Unregelmässigkeit 5) handelt es sich um eine Schwäche der Auslegung, die zudem ein erhebliches CCF-Potenzial zur Folge hat.

Derartige Fehler und Schwächen können in der PSA nicht angemessen berücksichtigt werden; somit kann die PSA auch keine verlässliche quantitative Aussage über Störfallabläufe liefern, die von den betreffenden Systemteilen mitbestimmt sind. Es ist davon auszugehen, dass die PSA für den Störfallablauf, wie er im Zwischenfall von Forsmark aufgetreten ist, eine wesentlich geringere Häufigkeit ausweisen würde, als tatsächlich zu erwarten ist.

Mit diesen Aussagen weist die KSA auf gewisse Grenzen der Aussagekraft von PSA hin. Die PSA ist zwar ein sehr wertvolles Mittel zur sicherheitstechnischen Beurteilung von Systemen. Letztlich massgebend sind aber nicht statistische Grössen, sondern reale Gegebenheiten und Handlungen. Aus diesem Grund weist die KSA auf die nach wie vor grosse Bedeutung einer konservativen Auslegung der Kernanlagen und eines hohen Standards beim Faktor Mensch hin.

6 Zu Aspekten der Sicherheitskultur im Allgemeinen

6.1 Bericht des Betreibers des KKW Forsmark zur Sicherheitskultur

Der Ereignisbericht [5] des Betreibers des KKW Forsmark zum Zwischenfall vom 25.07.2006 geht hauptsächlich auf die technischen Störungen und das technische Verhalten der Anlage sowie auf das Handeln des Schichtpersonals während und nach dem Zwischenfall ein. Mit Datum 23.10.2006 wurde in der Betreiberorganisation der Hintergrundbericht mit dem Titel (übersetzt) "Analyse des laufenden Betriebs, des Qualitätsmanagements und der Leitungsprozesse innerhalb des FKA" verfasst [6]; vgl. auch Abschnitt 2.4. Dieser Bericht behandelt Aspekte der Sicherheitskultur und des menschlichen Verhaltens während des Zwischenfalls, aber vor allem während der Jahre vor dem Zwischenfall.

Der Bericht hält folgende Schlussfolgerungen fest (Zitate aus Übersetzung [6] *kursiv*):

- Der Zwischenfall vom 25.07.2006 muss *als Höhepunkt im Verfall der Sicherheitskultur des Unternehmens betrachtet werden*. Ursache dafür sind wahrscheinlich zu einem grossen Teil die in letzter Zeit erfolgte Fokussierung auf Produktionssteigerung und eine allzu schnelle Erneuerung der Anlage.
- Der Ereignisbericht [5] zum Zwischenfall ist zu eng auf technische Mängel eingegrenzt. Das Verhalten des Schichtpersonals, welches den Schweregrad der Situation unterschätzt hat und teilweise von Weisungen abgewichen ist, wird nicht erwähnt. Dadurch werden Grundursachen nicht ermittelt. Die zu enge Betrachtungsweise führte dazu, dass mehrere Faktoren, die für die Gestaltung von korrigierenden und vorbeugenden Massnahmen von Bedeutung sind, ausser Acht gelassen wurden.
- Etwa die Hälfte der Störungsberichte, die im Jahre 2005 in Forsmark 1 verfasst wurden, weist auf Mängel und Fehler hin, die beitragende Faktoren im Zwischenfall vom 25. Juli 2006 waren. Wären aus den damaligen Ereignisberichten die erforderlichen Massnahmen abgeleitet sowie rechtzeitig und konsequent umgesetzt worden, so hätte der Zwischenfall vom 25.07.2006 verhindert werden können oder er hätte einen weniger problematischen Verlauf genommen.
- In Forsmark 1 fehlt eine etablierte Vorgehensweise, um Erkenntnisse aus Störungen zu analysieren, daraus Massnahmen abzuleiten, diese umzusetzen und deren Wirksamkeit zu überprüfen.
- Dass das Problem bei der generellen Einstellung der Führung und des Personals zur Sicherheit liegt, es also um Sicherheitskultur geht, zeigt folgende Aussage im Bericht: Zum Zeitpunkt des Zwischenfalls in Forsmark 1 fand auch die Revision in Forsmark 2 statt. *Vor dem Hintergrund, dass das Interesse der Öffentlichkeit für Forsmark stark zugenommen hatte, hätten Sicherheitsfragen sowie der Wille, es "richtig zu machen", über das normale Mass hinaus für Arbeiten während der Forsmark-2-Revision wegweisend sein müssen. Stattdessen müssen leider in der internen Berichterstattung unakzeptabel viele und ernsthafte Defizite in der Sicherheitskultur sowie Risiken in der Arbeitsumwelt festgestellt werden... – Dies beruht vermutlich darauf, dass das höchste Prinzip für den Betrieb nach wie vor darin besteht, Zeitpläne einzuhalten und dadurch beizutragen, die von der FKA aufgestellten Produktionsziele, "Rekorde aufzustellen", zu erfüllen.*

6.2 Zu Aspekten der Sicherheitskultur in den schweizerischen Kernkraftwerken

Die HSK stellt in ihrem Aufsichtsbericht 2006 [17] zusammenfassend fest, dass im Berichtsjahr die nukleare Sicherheit aller schweizerischen KKW in Bezug auf die Auslegung und das Betriebsgeschehen gut war und die Betriebsbedingungen eingehalten wurden.

Trotzdem scheinen der KSA gewisse im Hintergrundbericht [6] von FKA erwähnten Aspekte auch in Bezug auf die schweizerischen KKW beachtenswert.

6.2.1 Auswertung von Ereignissen in anderen Kernanlagen

Die HSK beurteilt in ihrem Bericht [1] die von den schweizerischen KKW vorgenommene Auswertung externer Betriebserfahrung und den Erfahrungsaustausch mit andern KKW überwiegend positiv, hat aber in einzelnen Anlagen auch Ressourcen-Engpässe festgestellt. Sie erwartet, dass alle Betreiber die dafür notwendigen Ressourcen bereitstellen, und wird entsprechende Massnahmen ergreifen. Die KSA begrüsst diese Forderung der HSK.

Die KSA behandelt im Rahmen ihres Auftrags "Beobachtung des Betriebs von Kernanlagen" [18] ausgewählte Ereignisse. Sie hat dabei festgestellt, dass die Auswertung von Ereignissen in der eigenen und in anderen Anlagen nicht selten in enger Weise auf technische Ursachen und Aspekte fokussiert ist. So werden die organisatorischen und menschlichen Aspekte nicht immer hinreichend einbezogen und beurteilt. Ausserdem werden Ereignisse in Drittanlagen häufig als irrelevant betrachtet, weil das dort betroffene System in der eigenen Anlage nicht oder nicht in genau gleicher Form vorhanden ist. Aufgrund eines derartigen Beurteilungsmusters können neben technischen insbesondere auch wichtige Aspekte im Bereich Sicherheitskultur und menschliche Faktoren übersehen werden.

Die KSA erachtet es deshalb als wichtig, dass die Betreiber Ereignisse in der eigenen und in fremden Anlagen sowie Betriebserfahrungen von anderen Anlagen umfassend analysieren, insbesondere auch bezüglich Aspekten der Sicherheitskultur und des menschlichen Verhaltens.

6.2.2 Umsetzung von Empfehlungen aus Expertenüberprüfungen

Im Jahr 2004 hat in Forsmark 1 ein WANO Peer Review stattgefunden. Dieses führte zu einer Reihe von kritischen Anmerkungen in mehreren Bereichen, die aber nicht beachtet wurden [6].

Den Umgang mit den Ergebnissen derartiger Expertenüberprüfungen hat die KSA bereits in ihrem Bericht KSA-Report 07-01 [19] angesprochen. Sie ist der Ansicht, dass der Charakter der WANO Peer Review als eigenverantwortliche Aktion der Betreiber ohne Einbezug der Aufsichtsbehörde respektiert werden soll. Denn es kann davon ausgegangen werden, dass der Diskurs über Sicherheitsfragen und -praktiken im Kreis der Betreiber kritischer geführt wird als in Gegenwart von Dritten bzw. von Aufsichtsbehörden. Zudem sieht der WANO-Prozess selber eine Überprüfung der Umsetzung der Massnahmen im Rahmen einer Folge-mission vor. Damit jedoch Empfehlungen zur Verbesserung der Sicherheit möglichst breit greifen, empfiehlt die KSA im erwähnten Bericht, dass die Betreiber der Aufsichtsbehörde nach einem Review mitteilen, welche Erkenntnisse zur Verbesserung der Sicherheit resultiert haben.

Aufgrund der Berichte zum Zwischenfall von Forsmark präzisiert die KSA diese Empfehlung.

Empfehlung 6.2.2

Die Betreiber sollen der Aufsichtsbehörde sämtliche Massnahmen zur Verbesserung der Sicherheit mitteilen, die aus Expertenüberprüfungen durch Betreiberorganisationen resultieren. Hingegen soll die Aufsichtsbehörde die Betreiberinitiative respektieren und nicht direkt in den Prozess einwirken oder in Dokumente Einblick nehmen.

6.2.3 Gesetzliche Vorgaben im Bereich Sicherheitskultur

Im Bericht KSA-Report No. 07-01 [19] hat die KSA festgehalten, dass bei mehreren Vorkommnissen der Stufen INES 1 bis INES 3, die sich weltweit ereignet haben, die Aufsichtsbehörden die vorgängig bereits manifesten Unzulänglichkeiten im Bereich der Sicherheitskultur nicht erkannt und/oder keine geeigneten Massnahmen gefordert haben. Wie im vorangehenden Abschnitt erwähnt, unterblieben in Forsmark 1 Massnahmen, die aufgrund von Hinweisen aus der WANO Peer Review notwendig gewesen wären.

Die schweizerische Kernenergiegesetzgebung ([20][21] und zugehörige Erlasse) enthält u.a. folgende Bestimmungen mit Relevanz für die Sicherheitskultur:

- Art. 30 Abs. 3 KEV [21]: *Er [Der Bewilligungsinhaber] hat ein Gremium einzusetzen, das Ereignisse und Befunde mit Ursache im Bereich menschliche Faktoren analysiert, Massnahmen vorschlägt und deren Umsetzung überwacht.*
- Anhang 3 KEV [21]: *Das Kraftwerksreglement bzw. das Betriebsreglement dokumentiert die organisatorischen und personellen Voraussetzungen für einen sicheren Betrieb einschliesslich der organisatorischen Abschaltkriterien.*

Soweit die KSA die Umsetzung dieser Vorschriften beobachtet hat, ist sie unterschiedlichen Ansätzen und unterschiedlichem, teilweise auch ungenügendem Umsetzungsgrad begegnet. Mit Hinweis auf die Schwierigkeit einer Korrektur und die möglicherweise schwerwiegenden Folgen einer negativen Entwicklung bei der Sicherheitskultur empfiehlt die KSA der Aufsichtsbehörde, die Umsetzung, Anwendung und Wirksamkeit der gesetzlichen Vorgaben in diesem Bereich zu überprüfen.

Wie oben erwähnt hat die KSA bei der Erarbeitung ihres Berichtes KSA-Report No. 07-01 [19] festgestellt, dass bei mehreren Ereignissen, die auf der INES-Skala den Stufen 1 bis 3 zugeteilt wurden, die Aufsichtsbehörden, trotz teilweise sehr intensiver Aufsichtstätigkeit, die Mängel in der Organisation, der Einstellung der Führung und des Personals sowie der Sicherheitskultur nicht erkannt bzw. keine Forderungen zur Verbesserung der Situation gestellt haben. Die KSA hat einerseits den Aufsichtsbehörden empfohlen zu überlegen, wie sie Mängel in der Unternehmenskultur besser erfassen und geeignet darauf reagieren können. Andererseits plant sie, einen Bericht zur Aufsichtstätigkeit der Behörde in den Bereichen Organisation und menschliches Verhalten zu erarbeiten.³

7 Zusammenfassung und Schlussfolgerungen

Der Zwischenfall vom 25. Juli im schwedischen Kernkraftwerk (KKW) Forsmark 1 hat in Schweden selber und international grosse Aufmerksamkeit seitens der Betreiber, Behörden und Öffentlichkeit erweckt. Auch die schweizerische Aufsichtsbehörde, die Hauptabteilung für die Sicherheit der Kernanlagen (HSK), hat nach dem Zwischenfall von den Betreibern der schweizerischen KKW umgehend Abklärungen eingefordert, die Situation analysiert und in einem Bericht [1] ihre Erkenntnisse und Empfehlungen dargelegt. In der KSA wurde der Zwischenfall ebenfalls thematisiert; mit Brief vom 23. August 2006 [3] erhielt die KSA vom Bundesamt für Energie (BFE) formell den Auftrag, den Zwischenfall vertieft zu erörtern und mit dem vorliegenden Bericht ihre Erkenntnisse zuhanden der Behörden festzuhalten.

Der Zwischenfall von Forsmark wurde durch eine Fehlmanipulation in der Schaltanlage, also kraftwerksextern, ausgelöst. Der Verlauf war geprägt durch eine Reihe von Unregelmässigkeiten:

- Ein Netztrenner zwischen Schaltanlage und Übertragungsnetz wurde unter Last geöffnet. (kraftwerksextern)
- Der Sammelschienenschutz sprach nicht an. (kraftwerksextern)
- Der Übergang auf die Eigenbedarfsversorgung misslang.
- Der Generatorschalter öffnete beim ersten Grenzwert für Unterfrequenz nicht.

³ Die Fertigstellung des angekündigten Berichts ist nicht sichergestellt: Aufgrund des Bundesgesetzes über das Eidgenössische Nuklear-Sicherheitsinspektorat (ENSIG) vom 22. Juni 2007 wird die KSA aufgelöst und die Eidgenössische Kommission für nukleare Sicherheit (KNS) neu gebildet. Die Ablösung ist vorgesehen per 1.1.2008.

- Die unterbrechungsfreien Stromversorgungen (USV) von zwei (von vier) Strängen wurden durch Geräteschutz abgeschaltet. Dies hatte u.a. zur Folge, dass die Notstromdiesel in den beiden beeinträchtigten Strängen nicht aufgeschaltet werden konnten.
- Die als Redundanz für das Fremdnetz kraftwerksextern vorhandene Gasturbine startete nicht. (Dieser Ausfall hatte keine konkrete Konsequenz für den Zwischenfall.)

Insbesondere der Ausfall der Notstromversorgung in zwei von vier Strängen führte zu einer kritischen Situation im Kommandoraum, weil dadurch gewisse Informations- und Kommunikationssysteme beeinträchtigt waren. Die Schichtmannschaft hatte dadurch während rund 20 Minuten nicht die vollständige Kontrolle über den Anlagenzustand. Mit den noch verfügbaren und automatisch tätigen Sicherheitssystemen wurde der Zwischenfall aber beherrscht. Alle grundlegenden Schutzziele blieben erfüllt, doch insbesondere bezüglich des Schutzzieles "Kühlung der Brennelemente" war ein Teil der vorgesehenen gestaffelten Massnahmen ausgefallen und somit die verbleibende Marge wesentlich geschmälert. Endgültig normalisiert werden konnte die Situation, nachdem etwa 22 Minuten nach Beginn des Ereignisses das Fremdnetz, das eigentlich stets verfügbar gewesen wäre, manuell zugeschaltet wurde.

Das Ereignis wurde von der schwedischen Aufsichtsbehörde SKI nach der internationalen Ereignisskala für Kernanlagen (International Nuclear Event Scale, INES) der Stufe INES 2, Zwischenfall, zugeordnet.

Aus technischer Sicht ist die Serie von ursächlich unabhängigen Fehlfunktionen bemerkenswert. Besonders schwerwiegend ist der Ausfall der USV in zwei Strängen. Dieser Ausfall weist Merkmale eines Common-cause-Fehlers auf. Bezüglich technischer Befunde verweist die KSA auf die Analysen der HSK [1] und der GRS [2].

Die direkten Ursachen für die eingetretene Sequenz von Fehlfunktionen liegen zu wesentlichen Teilen in Ausführungsmängeln und konzeptionellen Schwächen. Diese stehen in mehreren Fällen im Zusammenhang mit vorgenommenen Anlagenänderungen, womit Schwächen im Änderungswesen und damit im organisatorischen Bereich angesprochen sind.

Die HSK geht in ihrem Bericht [1] speziell ausführlich auf die Gestaltung der Eigenbedarfs- und Notstromanlagen in Forsmark 1 einerseits und in den schweizerischen KKW andererseits ein. Sie kommt zum Schluss, dass aufgrund der unterschiedlichen Konzeption der schweizerischen Anlagen im Bereich der Stromversorgung keine Massnahmen erforderlich sind. Auch andere technische Massnahmen sind gemäss Beurteilung der HSK nicht erforderlich. Sie formuliert jedoch zwei Empfehlungen bezüglich Simulatorausbildung des Schichtpersonals sowie Auswertung von Vorkommissen und Betriebserfahrungen in ausländischen Anlagen. Die KSA unterstützt diese Empfehlungen.

Die KSA hat den Zwischenfall von Forsmark ebenfalls ausführlich behandelt. Die Grundursachen für den Zwischenfall liegen vor allem im Bereich der Sicherheitskultur; im Sinn einer allgemeinen zentralen Folgerung ergibt sich daraus, dass zum Erhalt einer hohen Sicherheitskultur (Menschliches Handeln, Organisation, Prozesse) konstant hohe Anstrengungen erforderlich sind. Lehren für die schweizerischen KKW lassen sich jedoch auch für die technische Ausrüstung und deren Prüfung sowie für die Ereignisbewältigung ziehen. Zudem spricht die KSA in ihren Empfehlungen energiewirtschaftliche Rahmenbedingungen an, welche die Sicherheit der KKW beeinträchtigen können.

Zusammenstellung der Empfehlungen

Empfehlungen 5.1.4

- Die KSA unterstützt die Empfehlung der HSK, bei der Simulatorenausbildung des Schichtpersonals noch vermehrt den Umgang mit Ausfällen von Redundanzen der Sicherheitssysteme oder der Energieversorgung zu schulen. Dabei soll auch überprüft werden, wie weit die Schulung alle denkbaren Störfälle in der anlageninternen Energieversorgung abdeckt. Ausserdem soll sichergestellt werden, dass die Simulatoren der schweizerischen Kernkraftwerke für Schulungen hinsichtlich gestörter Energieversorgung, insbesondere auch Spannungstransienten in der Schaltanlage, hinreichend ausgerüstet sind.
- Mit Blick auf das Potenzial für Common-cause-Fehler, das von Störungen in der Eigenbedarfsversorgung ausgeht, empfiehlt die KSA zudem, die für Störungen in der Eigenbedarfsversorgung zu unterstellende maximale Spannungstransiente nach konservativen Grundsätzen neu zu überprüfen und allenfalls neu festzulegen. Im Fall einer Neufestlegung soll sichergestellt werden, dass die für die Sicherheit massgebenden elektrotechnischen und elektronischen Komponenten so ausgelegt sind, dass sie im Rahmen der zu unterstellenden Spannungstransiente korrekt funktionieren und bei deren Überschreiten sicherheitsgerichtete Systemreaktionen auslösen.

Empfehlungen 5.2.4

- Den Prüfmöglichkeiten ist bei der Systemkonzeption grosse Beachtung zu schenken. Im Zug der Baufreigaben soll sichergestellt werden, dass alle Einrichtungen im Systemkonzept enthalten sind, damit die erforderlichen periodischen Funktionsprüfungen vorgenommen werden können. Insbesondere sollen auch die entsprechenden Vorgaben im Regelwerk überprüft werden.
- Im Zug der Bau- und Inbetriebnahmephase von neuen Komponenten oder Systemen ist ein umfassendes Prüfprogramm durchzuführen. Damit soll insbesondere auch die funktional korrekte Montage sichergestellt werden; auch Prüfungen mit hoher Systembeanspruchung sind notwendig.
- Das Verhalten bei Transienten von sicherheitsrelevanten Systemen und Komponenten, die geändert oder erneuert worden sind, soll systematisch ausgewertet werden.

Empfehlungen 5.4

Im Zusammenhang mit der Verselbständigung des Übertragungsnetzes ist sicherzustellen, dass

- Betrieb und Unterhalt der Schaltanlage zwischen Kernkraftwerk und Netzbetreiber sicherheitsgerichtet koordiniert sind;
- der Netzbetreiber die speziellen Anforderungen der nuklearen Anlagensicherheit beim Betrieb der Netzanschlüsse der Kernkraftwerke mit Priorität berücksichtigt.

Empfehlung 5.5

Möglichkeiten zur deutlichen Senkung der Anzahl Nichtverfügbarkeiten von Notstromanlagen sollen in grundsätzlicher Art untersucht werden.

Empfehlung 6.2.2

Die Betreiber sollen der Aufsichtsbehörde sämtliche Massnahmen zur Verbesserung der Sicherheit mitteilen, die aus Expertenüberprüfungen durch Betreiberorganisationen resultieren. Hingegen soll die Aufsichtsbehörde die Betreiberinitiative respektieren und nicht direkt in den Prozess einwirken oder in Dokumente Einblick nehmen.

Dieser Bericht wurde an der 460. KSA-Sitzung vom 14. September behandelt, anschliessend bereinigt und auf dem Korrespondenzweg verabschiedet.

Würenlingen, 2. Oktober 2007

EIDG. KOMMISSION FÜR DIE
SICHERHEIT VON KERNANLAGEN

Der Präsident



Prof. W. Wildi

Geht an: Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK)
Bundesamt für Energie (BFE)
Hauptabteilung für die Sicherheit der Kernanlagen (HSK)

Referenzen

- [1] Der Störfall vom 25. Juli 2006 im schwedischen Kernkraftwerk Forsmark1 und die Auswirkungen auf die Kernkraftwerke in der Schweiz; HSK-AN-6132; HSK, Februar 2007 (KSA-AN-2312) www.hsk.ch → Infos → Weitere Publikationen → 12.02.2007
- [2] Ereignis im schwedischen Kernkraftwerk Forsmark, Block 1 am 25.07.2006: "Nichtzuschalten von zwei Notstromdieseln nach Ausfall der 400-kV-Netzanbindung"; Weiterleitungsnachricht WLN 2006/07; GRS, Köln, 14.11.2006 (KSA-AN-2293.7) www.bmu.de → Atomenergie → AKW im Ausland → Forsmark
- [3] Forsmark und KSA – Rolle der KSA bei aktuellen Ereignissen in Kernanlagen; Brief von BFE an Prof. Dr. W. Wildi [Präsident der KSA]; Bern, 23. August 2006 (KSA-AN-2298)
- [4] Loss of 400 kV and Subsequent Failure to Start Emergency Diesel Generators Sub A and Sub B; main report No. 7788; "restricted"; International Incident Reporting System (IRS); 2006-09-28 (KSA-AN-2293.5)
- [5] Forsmark 1 - Störungsanalys - Bortfall 400kV samt utebliven dieselstart i A- och B-sub; Forsmarks Kraftgrupp; Rapport F1-2006-0699 Rev 6
- [6] Analyse des laufenden Betriebs, des Qualitätsmanagements und der Leitungsprozesse innerhalb des FKA; Bericht FM-2006-0968; "unternehmensinternes Dokument"; Vattenfall, 23.10.2006; *ins Deutsche übersetzt* (KSA-AN-2293.8)
- [7] Review of the licensee's account due to the electrical disturbance at Forsmark 1 on July 25, 2006; Review Report SKI 2006/779; SKI, 2006-08-03 (KSA-AN-2293.1) www.ski.se → English → current information (as of 2006-08-04)
- [8] Necessary measures in Forsmark 1 and 2 for future operations of the plant; press release; SKI, 2006-09-14; *zusammen mit*: Order on measures to be taken regarding the Forsmark NPP units 1 and 2; Decision SKI 2006/779; SKI, 14 september 2006 (KSA-AN-2293.4) www.ski.se → English → current information (as of 2006-09-14)
- [9] SKI permits the restart of the reactors at Forsmark and intensifies its supervision of the plant; press release; SKI, 2006-09-28 (KSA-AN-2293.6) www.ski.se → English → current information (as of 2006-09-28)
- [10] www-news.iaea.org/news → Events → 2006-07-25 [nicht mehr aufgeschaltet] → View event rating forms
- [11] Schweden: Regierung begrüsst "kraftvolle Massnahmen für Forsmark-Reaktor"; Deutsche Presse-Agentur, 9.02.2007
- [12] www.ski.se → English → current information (as of 2006-10-17 / 2007-02-03)
- [13] Störfall im schwedischen Kernkraftwerk Forsmark I: Anfrage betreffend Ausfall von Sicherheitskomponenten nach einem externen Spannungsausfall; Brief von HSK an alle schweizerischen KKW; Villigen, 14. August 2006 (*in KSA-AN-2293.2 Rev. 1*)
- [14] Antworten der schweizerischen KKW auf die HSK-Anfrage [13] (*in KSA-AN-2293.2 Rev. 1*)
- [15] Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz, StromVG) vom 23. März 2007; SR 734.7

- [16] www.ucte.org → Operation Handbook
- [17] Aufsichtsbericht 2006 zur nuklearen Sicherheit in den schweizerischen Kernanlagen; HSK-AN-6161; HSK (*KSA-AN-2317*)
- [18] Verordnung über die Eidgenössische Kommission für die Sicherheit von Kernanlagen vom 14. März 1983; SR 732.21
- [19] Methodik der Aufsicht über Kernanlagen; Teil 2: Beurteilung von Aspekten der Organisation und des menschlichen Verhaltens; Ableiten von Verbesserungsmassnahmen; KSA-Report No. 07-01; KSA, März 2007
- [20] Kernenergiegesetz (KEG) vom 21. März 2003; SR 732.1
- [21] Kernenergieverordnung (KEV) vom 10. Dezember 2004; SR 732.11

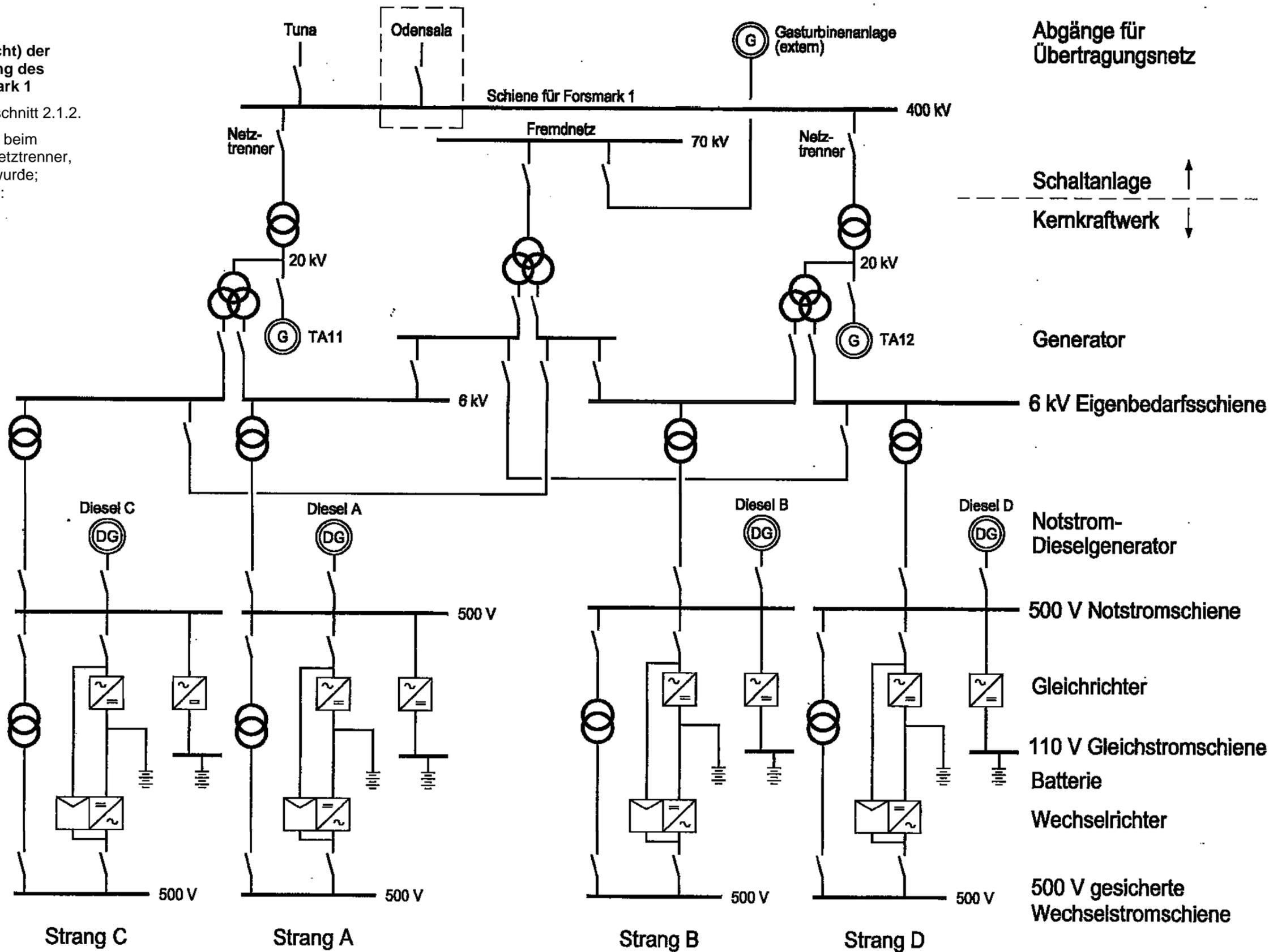
Abkürzungen und Begriffe

BFE	Bundesamt für Energie
CCF	Common Cause Failure (vgl. Abschnitt 2.2) (Systematischer Mehrfachausfall)
FKA	Forsmarks Kraftgrupp AB
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
HSK	Hauptabteilung für die Sicherheit der Kernanlagen
IRS	Incident Reporting System (IAEA/NEA) (Meldesystem von IAEA/NEA für Ereignisse)
IAEA	International Atomic Energy Agency
IAEO	Internationale Atomenergie-Organisation
INES	International Nuclear Event Scale (IAEA/NEA) (Internationale Bewertungsskala von IAEA/NEA für Ereignisse)
KEG	Kernenergiegesetz (SR 732.1) [20]
KEV	Kernenergieverordnung (SR 732.11) [21]
KKW	Kernkraftwerk(e)
KSA	Eidgenössische Kommission für die Sicherheit von Kernanlagen
NEA	Nuclear Energy Agency (OECD)
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
OKG	OKG AB [ursprünglich: Oskarshamns Kraftgrupp] (Eigentümer und Betreiber der drei KKW-Blöcke im schwedischen Oskarshamn)
PSA	Probabilistische Sicherheitsanalyse
SKI	Statens Kärnkraftinspektion (schwedische KKW-Aufsichtsbehörde, etwa: Staatliches Kernkraftinspektorat)
sub	Kurzform für "subdivision" (deutsch: Strang, vgl. Abschnitt 2.1.1)
SvK	Svenska Kraftnät (Eigentümer- / Betreibergesellschaft des schwedischen Übertragungsnetzes)
StromVG	Stromversorgungsgesetz (SR 734.7) [15]
TA11	Turbosatz 1 von Forsmark 1
TA12	Turbosatz 2 von Forsmark 1
Turbosatz	Maschineneinheit bestehend aus Turbine und Generator
UCTE	Union for the Co-ordination of Transmission of Electricity (Europäischer Netzverbund)
UPS	Uninterruptible Power Supply (Unit)
USV	Unterbrechungsfreie Stromversorgung (auch für Geräteeinheit verwendet)
WANO	World Association of Nuclear Operators (Weltorganisation der Betreiber von Nuklearanlagen)

Abbildung 1
Schaltchema (Übersicht) der elektrischen Versorgung des Kernkraftwerks Forsmark 1

Erläuterungen siehe Abschnitt 2.1.2.

Ganz oben (eingerahmt) beim Abgang Odensala der Netztrenner, der unter Last geöffnet wurde; vgl. dazu Abschnitt 2.3.1: Auslösendes Ereignis.



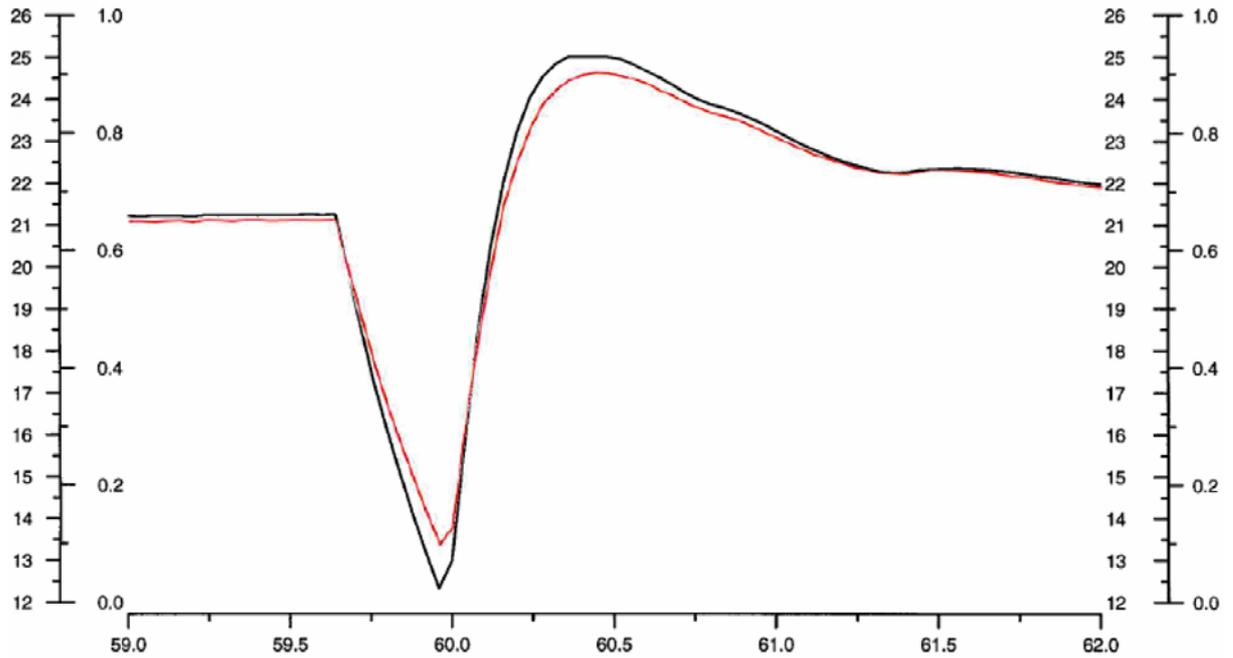


Abbildung 2 Spannungstransiente an den Generatorklemmen [5]
von Generator TA11 (schwarz) und TA12 (rot);
horizontal: Zeit in Sekunden; vertikal: Spannung in Kilovolt (je linke Skala).

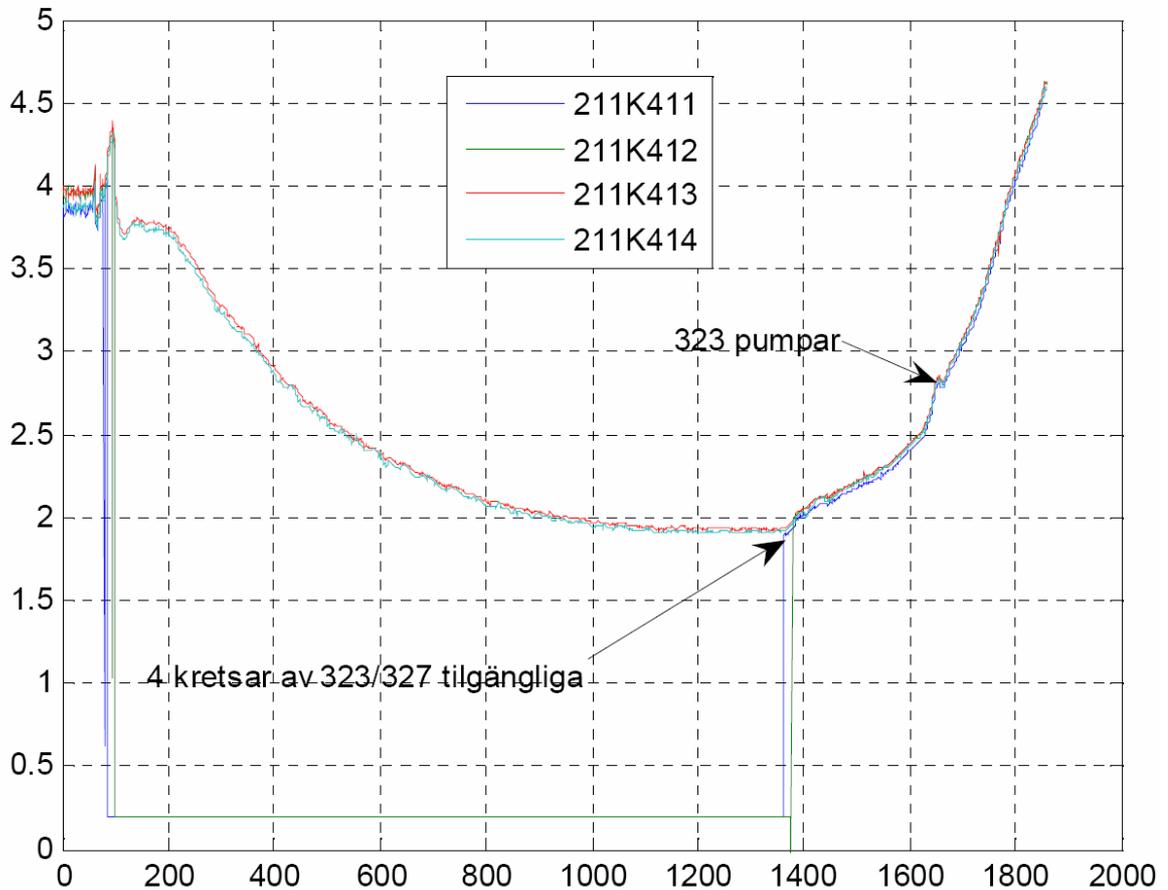


Abbildung 3 Füllstand im Reaktordruckbehälter [5];
horizontal: Zeit in Sekunden;
vertikal: Füllstand in Meter über Kernoberkante.

Eidgenössische Kommission für
die Sicherheit von Kernanlagen (KSA)
Sekretariat
CH-5232 Villigen PSI

Telefon: +41 (0)56 310 3968 / 3811
Telefax: +41 (0)56 310 3855
ksa@hsk.ch
www.ksa.admin.ch