V. SPURENSICHERUNG

Michael Sailer

Warum Forsmark immer wieder passieren kann – oder: Sind Atomreaktoren wirklich sicher?

Ende Juli 2006: Schlagzeilen in deutschen Medien wie „Schwerer Störfall im schwedischen Atomkraftwerk Forsmark". Massive Verwunderung bei vielen darüber, dass solche Dinge nicht nur in osteuropäischen AKW passieren können. Schweden galt bisher als ein Land der sicheren Reaktoren.

Wahrscheinlich war der Fall in Schweden doch nicht so schwer, wurde später vermutet. In den deutschen Medien wurde herausgestellt, dass in Schweden selbst die Sache gar nicht so ernst gesehen werde. Die Veröffentlichungen des Betreibers Vattenfall und der schwedischen Atomkontrollbehörde SKI aus dieser Zeit bekräftigten diesen Eindruck.

Einige Monate später: Ein Vattenfall-interner Kontrollbericht [1] von Ende Oktober 2006, am 19. Dezember 2006 an die SKI übergeben, wurde im Januar 2007 Medien zugespielt und führte zu neuen Schlagzeilen – und diesmal auch in Schweden. Der verantwortliche Kraftwerksleiter trat zurück, SKI hat bei der Staatsanwaltschaft strafrechtliche Schritte gegen die Verantwortlichen beim Betreiber einleiten lassen. Im Februar 2007 werden dann neue Unregelmäßigkeiten beim Umgang mit Undichtigkeiten im Reaktor bekannt. In der internationalen Nukleargemeinde wird das „Ereignis" vom Juli 2006 in Forsmark inzwischen als einer der 20 relevantesten Beinaheunfälle seit 1986 geführt.

Am Standort Forsmark befinden sich drei Siedewasserreaktoren schwedischer Bauart. Der am 10. Dezember 1980 in Betrieb gegangene Reaktor 1 war damals weltweit ein sicherheitstechnisches Vorbild. Hier wurden, anders als bei älteren Reaktorkonstruktionen, konsequent vierfache Sicherheitssysteme eingebaut. Jedes System

wurde von den anderen so gut getrennt, dass auch größere Brände nicht mehrere Sicherheitssysteme außer Kraft setzen konnten. Noch war den Konstrukteuren frisch in Erinnerung, dass 1975 im amerikanischen AKW Browns Ferry eine zur Dichtheitsprüfung eingesetzte Kerze ein Feuer entfachte, das fast alle mehrfach vorhandenen Sicherheitssysteme funktionsunfähig machte. Browns Ferry schlitterte damals knapp an der Katastrophe vorbei.

Was ist also eigentlich in Forsmark passiert? In dürrer technischer Sprache findet sich das in der GRS-Weiterleitungsnachricht [2]:

„Im schwedischen Kernkraftwerk Forsmark, Block 1, fiel am 25. Juli 2006 in Folge einer elektrischen Transiente, die in einer Freiluftschaltanlage außerhalb des Kraftwerkgeländes ausgelöst wurde, die gesicherte Wechselstromversorgung in zwei von vier Strängen aus. Dies führte im weiteren Ereignisablauf in den beiden betroffenen Strängen zur Unverfügbarkeit aller Wechselstromschienen der Notstromanlage."

Und später: „Nach Einschätzung der schwedischen Aufsichtsbehörde SKI handelt es sich um einen ‚Common cause failure', der, wenn auch die beiden anderen Stränge betroffen gewesen wären, zu einem Ausfall der Wechselstromversorgung in der gesamten Notstromanlage geführt hätte und damit zu einem Ereignis, das im Sicherheitsbericht der Anlage nicht unterstellt wurde."

Letzteres heißt in der lapidaren Sprache der Nuklearingenieure: ein Fall, dessen Beherrschung durch Sicherheitssysteme nicht gesichert ist. Also eine Störung in der Stromversorgung, die zu einem unbeherrschbaren Zustand im AKW führen kann.

Warum braucht das Atomkraftwerk eigentlich Strom?

Ein AKW kann man nicht einfach abschalten. Denn die Wärme im laufenden Reaktor stammt aus zwei physikalischen Prozessen, zu 93 % aus der Kernspaltung und zu 7 % aus dem radioaktiven Zerfall der entstandenen Spaltprodukte – der Nachzerfallswärme. Die Schnellabschaltung des Reaktors kann nur die Kernspaltung unterbrechen, der radioaktive Zerfall lässt sich nicht stoppen. Deshalb bleibt nur übrig, die weiterhin anfallende Nachzerfallswärme mit sehr zuverlässigen Kühlsystemen, den so genannten Not- und Nachkühlsystemen, abzuführen.

Die von den Notkühlsystemen zu beherrschende Nachzerfallswärme lässt sich veranschaulichen: 7 % der thermischen Leistung eines

Reaktors von der Größe Forsmark sind etwa 210 MW. Dies entspricht der Heizleistung von rund einhunderttausend Haushaltsheizlüftern der üblichen Größe. Diese Wärme wird konzentriert im Reaktorkern freigesetzt, dessen Rauminhalt gerade mal einem kleinen Zimmer entspricht. Auch wenn nach einer Stunde nach Abschalten des Reaktors die Nachzerfallswärme auf etwa 1% der ursprünglichen Reaktorleistung zurückgegangen ist, entspricht dies immer noch etwa dreizehntausend Heizlüftern.

Es wird deutlich: Wenn die Notkühlsysteme im Falle des Falles nicht zur Verfügung stehen, heizt sich der Reaktorkern so schnell auf, dass innerhalb weniger Dutzend Minuten die Kernschmelze eintritt. Diese führt zur massiven Freisetzung von großen Mengen radioaktiver Stoffe in die Umgebung.

Die Systeme, die die Nachwärmeabfuhr sicherstellen, benötigen für ihren Betrieb und ihre Steuerung Strom. Ohne Strom fällt die Nachwärmeabfuhr aus. Um zuverlässig Strom für die Sicherheitssysteme zu haben, wird die Stromversorgung in verschiedenen Ebenen und aus verschiedenen Quellen aufgebaut:

- Normalfall ist die Abzweigung eines Teils der eigenen Erzeugung des AKW, der so genannte Eigenbedarf. Dies funktioniert aber nur, solange Reaktor und Turbinenanlagen laufen.
- Das Kraftwerk kann auch aus dem Stromnetz versorgt werden, in das es normalerweise liefert.
- Außerdem gibt es einen Reservenetzanschluss.
- Teilweise gibt es schnell startende Gasturbinen, die Strom liefern können.
- Weil diese verschiedenen Möglichkeiten der externen Stromversorgung nicht ausreichend zuverlässig sind, hat jedes AKW besonders gesicherte Notstromdieselanlagen, entsprechend den Sicherheitssystemen ebenfalls vierfach und getrennt aufgebaut. Sie können innerhalb weniger Minuten starten und die volle Stromversorgung der Sicherheitssysteme übernehmen.
- Bestimmte Sicherheitssysteme können keine Unterbrechung der Stromversorgung vertragen. Für sie muss eine unterbrechungslose Stromversorgung vorhanden sein, die auf leistungsstarken Batterien aufbaut. Unterbrechungsfrei zu versorgende Systeme sind z.B. sicherheitstechnisch relevante Steuer- und Leittechnik, sicherheitsrelevante Anzeigen, aber auch die Start- und Zuschaltprozeduren für die Notstromdieselversorgung selbst.

Auf den ersten Blick gibt es breit gefächerte und voneinander unabhängige Möglichkeiten, den funktionsnotwendigen Strom im AKW

bereitzustellen. Schwierigkeiten ergeben sich aber durch die unvermeidlichen Verknüpfungen der beschriebenen Systeme:

- Grundsätzlich kann eine Versorgungsschiene zur gleichen Zeit nur aus einer Stromquelle versorgt werden. Deshalb braucht es komplizierte steuer- und leittechnische Systeme, die beim Ausfall der aktuell versorgenden Stromquelle den Ausfall erkennen, die bisherige Stromquelle abtrennen und die neue Stromquelle auf die Versorgungsschiene schalten.
- Bei Störungen müssen auch nacheinander geschaltete Versorgungsschienen sich voneinander trennen, um eine Übertragung des Fehlers auf die nächste Ebene zu verhindern.
- Wenn eine Notstromschiene ihre normale Stromversorgungsquelle verliert, muss der Notstromdieselgenerator zunächst gestartet und dann synchronisiert werden, bevor er die Schiene versorgen kann.
- Die Batterien liefern Gleichstrom, die meisten Systeme benötigen aber Wechselstrom. Deswegen sind Gleichrichter erforderlich, um die Batterien im Normalbetrieb laufend nachzuladen, und Wechselrichter, um im Ernstfall den Gleichstrom aus den Batterien in den benötigten Wechselstrom umzuwandeln.

Diese Kürzesteinführung in Elektrotechnik erleichtert die Einordnung der technischen Vorgänge beim Störfall in Forsmark.

Das Ereignis am 25. Juli 2006

In der Netzschaltanlage, in die Forsmark 1 seinen Strom liefert, waren Reparaturarbeiten im Gange. Durch Fehler wurde ein Kurzschluss erzeugt. Die automatischen Schaltungen hätten das AKW innerhalb von 100 Millisekunden vom Netz trennen müssen. Tatsächlich wurde erst nach 300 Millisekunden getrennt. Dieser so klein erscheinende zeitliche Unterschied reichte aus, dass der ins Kraftwerk eingetragene elektrische Impuls verschiedene unerwünschte Folgeeffekte auslöste:

- Beide Turbinen des Reaktors schalteten sich aufgrund von bisher nicht erkannten Fehlern in der Ölversorgung ab; damit war auch die Eigenbedarfsversorgung ausgefallen.
- Das Hauptnetz war schon durch den Kurzschluss ausgefallen.
- Die Umschaltung auf das Reservenetz war nicht erfolgreich, weil aufgrund eines falsch angeschlossenen Schalterbauteils die Notstromschienen sich schon abgekoppelt hatten.
- Die Gasturbinenanlage war ebenfalls nicht startfähig, eine Überprüfung hatte seit dem Bau der Anlage nicht mehr stattgefunden.

Weil alle vorgelagerten Ebenen versagten, blieben nur noch die vier Notstromdieselanlagen. Der 200 Millisekunden zu lange anstehende Impuls aus der Netzschaltanlage hatte hier aber schon einen fatalen Fehler erzeugt: Über ihren Aggregateschutz wurden zwei der Wechselrichter abgeschaltet. Die entsprechenden Notstromdiesel konnten wegen der fehlenden Stromversorgung aus diesen Wechselrichtern nicht synchronisiert werden und deshalb auch die zugehörigen Sicherheitssysteme nicht mit Strom versorgen. Glücklicherweise schaltete der Spannungsimpuls nur zwei der vier gleich aufgebauten Wechselrichter ab.

Damit war unmittelbar die Hälfte der Sicherheitssysteme im Kraftwerk stromlos und so funktionsunfähig. Auch fiel damit ein größerer Teil der Anzeigen in der Warte aus, sodass sich die Betriebsmannschaft nun im teilweisen Blindflug befand. Es war nicht einmal klar, ob der Reaktor abgeschaltet war, denn Stellungsmeldungen der Steuerstäbe gehörten auch zu den ausgefallenen Anzeigen.

Nach 22 Minuten konnte die Betriebsmannschaft die beiden ausgefallenen Notstromanlagen von Hand in Betrieb setzen. Erst damit waren die Anzeigen und die Sicherheitssysteme wieder voll funktionsfähig. Der schon abgefallene Wasserstand im Reaktor konnte jetzt wieder auf den Sollwert hochgefahren werden. Der Reaktor wurde dann weiter heruntergekühlt und in den Zustand „Hot Stand-by" gefahren. Ein Abfahren in den kalten abgeschalteten Zustand wurde erst am nächsten Tag veranlasst.

Schon aus technischer Sicht beunruhigend

Die Analyse des Ereignisses ergibt schon aus technischer Sicht beunruhigende Ergebnisse:

- Auswirkungen von Fehlern außerhalb des AKW (in der Netzschaltanlage) konnten durch die existierenden Sicherheitseinrichtungen nicht rechtzeitig abgeschirmt werden. Die immer postulierte Trennung zwischen nichtnuklearen Einrichtungen und dem nuklearen Sicherheitssystem hatte versagt.
- Grundsätzlich hat das Prinzip der hintereinander gestuften Verteidigungsebenen versagt, denn der Impuls aus dem Kurzschluss in der Netzschaltanlage hat sich bis auf die letzte Verteidigungsebene ausgewirkt.
- Das Prinzip der vierfach getrennten Systeme hat im konkreten Fall wenig genutzt, denn der gleiche Effekt hat mehrere der parallelen

Systeme gleichzeitig außer Kraft gesetzt (der gefürchtete „Common Cause Failure“).
- Bis heute gibt es keine belastbare Erklärung dafür, dass der Impuls lediglich zwei der vier Wechselrichter abgeschaltet hat. Weil alle vier Systeme gleich aufgebaut sind, hätten genauso gut alle vier ausfallen können. Die Konsequenz beim Abschalten aller vier Wechselrichter wäre einerseits gewesen, dass der Betriebsmannschaft wegen der ausgefallenen Stromversorgung alle Informationsmöglichkeiten gefehlt hätten. Unter solchen Umständen wären Versuche von manuellen Wiederinstandsetzungen oder Notmaßnahmen sehr erschwert oder gar unmöglich gewesen. Andererseits wären alle Sicherheitssysteme ohne Stromversorgung und damit funktionsunfähig gewesen. Die Weiterentwicklung zur katastrophalen Kernschmelze wäre nur schwer aufzuhalten gewesen.

In der Debatte über die technischen Stärken und Schwächen der Sicherheit von Atomkraftwerken werden die komplexen Zusammenhänge oft übersehen. Die typische Betrachtungsweise sieht Sicherheitssysteme als getrennte stabilisierte Inseln in einem technischen System und schreibt ihnen hohe Wirksamkeiten zu. Letztere bestehen unbestritten, aber sie sind nicht absolut.

Die Sicherheitssysteme sind in der Realität verwoben mit der umgebenden Systemtechnik. Wenn die Annahme besteht, dass ein störender Impuls aus der Netzschaltanlage nach 100 Millisekunden abgeschirmt wird, dann waren die Sicherheitssysteme nicht gegen alle denkbaren elektrischen Impulse ausgelegt, sondern nur gegen den unterstellten. Genauso stecken Annahmen in der Stabilität von Baukonstruktionen oder in der Funktionsfähigkeit von elektrischen Bauteilen und elektronischen Schaltungen, auf denen Sicherheitssysteme im AKW basieren. Auch die Reichweite von erfolgreicher Qualitätssicherung bei der Herstellung und beim Einbau ist ein solcher Punkt.

Viele Fachdiskussionen zeigen, dass keine praktikablen Methoden zur Verfügung stehen, systematisch und vollständig Fehlerquellen in diesen Bereichen zu erfassen. Die Inseln der Sicherheitssysteme sind nicht wirklich abzutrennen und auch nicht vollständig zu stabilisieren. Dies gelingt weder in Forsmark, wie das Ereignis gezeigt hat, noch in anderen AKW, wie viele hier aus Platzgründen nicht weiter diskutierbare Ereignisse der letzten Jahre zeigen.

Der Einfluss des menschlichen Faktors

Neben diesen stark technikbezogenen Aspekten zeigt der im Januar 2007 publik gewordene Bericht des Betreibers von Forsmark [1] eine weitere Facette der kerntechnischen Sicherheit auf. Er bringt viele konkrete Beispiele für Sicherheitsdefizite aufgrund von menschlichem Verhalten und organisatorischen Mängeln. In der Zusammenfassung heißt es:

„Die aufgetretene Störung muss leider aus der Perspektive eines Höhepunktes im Verfall der Sicherheitskultur des Unternehmens betrachtet werden. Dies ist wahrscheinlich zu einem großen Teil der in letzter Zeit erfolgten Konzentration auf Produktionssteigerung und vielleicht einer allzu schnellen Erneuerung der Anlagen geschuldet. Um die grundlegenden Ursachen für die große Störung zu beleuchten (jedoch noch nicht abschließend zu analysieren), wurden eine Reihe von Bedingungen in der ‚F1-Transiente', jedoch auch Ereignisse in anderen Teilen des Unternehmens in der Zeit unmittelbar vor der Transiente sowie in deren Vorgeschichte untersucht.

Die aufgezeigten Beispiele weisen nach, dass die in Zusammenhang mit der F1-Transiente durchgeführte Störfallanalyse zu eng auf technische Mängel, durch die die Störung am 25.7.2006 verursacht wurde, begrenzt ist. Dadurch werden die grundlegenden Ursachen nicht ermittelt. Es ist auch zweifelhaft, ob der Betrieb die geltenden Bestimmungen erfüllt.

Die Fähigkeit des Unternehmens, sowohl kurz- als auch langfristig als lernende Organisation zu fungieren, wird anhand einiger Beispiele beleuchtet. Es treten viele nicht akzeptable Qualitätsmängel auf, obwohl die Möglichkeit bestand, aus der Vergangenheit zu lernen. Auch wird keine unmittelbare Verbesserung in der Zeit direkt nach der F1-Transiente sichtbar, obwohl es dazu hätte kommen sollen.

Vieles deutet darauf hin, dass die grundlegenden Ursachen für das Ereignis am 25.7.2006 in Mängeln im Qualitätsmanagementsystem zu finden sind, das nicht die Anforderungen der Umwelt erfüllt. Es sieht auch so aus, dass sich die Möglichkeiten und sogar der Wille, Anweisungen und Verordnungen zu befolgen, verschlechtert haben. Wir erfüllen oft deren Buchstaben, aber nicht deren wahren Sinn. In bestimmten Fällen sind leider auch eindeutige Verstöße festzustellen.

Der Mangel an Zeit scheint zu rechtfertigen, dass oftmals verstärkt Risiken auf allen Ebenen des Unternehmens eingegangen werden und die Bestimmungen für Reaktorsicherheit und Arbeitsschutz eine immer breitere Auslegung erfahren."

Ein konkretes Beispiel für in diesem Bericht aufgeführte Unterlassungen ist, dass die Betriebsmannschaft das zweite System zur Abschaltung des Reaktors nicht aktiviert hat, obwohl 22 Minuten lang die Anzeige für die Position von Steuerstäben, die das erste Abschaltsystem bilden, nicht funktionierte und somit nicht klar war, ob die Kernspaltung im Reaktor wirklich gestoppt war.

Eine zweite monierte Unterlassung ist, dass der Reaktor nach der Wiederherstellung der Stromversorgung im Zustand „Hot Stand-by" gelassen wurde, anstatt sofort in den ungefährlicheren kalten Zustand gefahren zu werden. Diese Unterlassung war übrigens der Grund, warum die Atomaufsichtsbehörde den Staatsanwalt einschaltete.

Ereignisse kehren wieder

Im internationalen Rahmen wird in den letzten Jahren immer intensiver darüber diskutiert, dass der Informationsaustausch über die so genannten Ereignisse offensichtlich weit weniger nutzt, als man nach den schweren „Ereignissen" in Harrisburg (1979) und Tschernobyl (1986) erhofft hatte. In einem 2006 veröffentlichten Bericht [3] der Nuclear Energy Agency (NEA) der OECD, die zusammen mit der Internationalen Atomenergieagentur (IAEA) das wesentliche staatenübergreifende Informationsaustauschsystem betreibt, wird für den Zeitraum 2002 bis 2005 festgestellt:

„Rund 200 Ereignisse wurden von den teilnehmenden Ländern in dieser Periode berichtet … Praktisch alle der während dieser Periode berichteten Ereignisse haben sich schon früher in der einen oder anderen Form ereignet. Das zeigt, dass Gegenmaßnahmen, die im Prinzip gut bekannt sind, trotz der bestehenden Austauschsysteme auf nationaler wie internationaler Ebene möglicherweise nicht alle Endnutzer erreichen oder nicht immer stringent oder rechtzeitig angewandt werden."

Offensichtlich hat die Hoffnung, dass die Kerntechnik für ihre Sicherheit aus vergangenen Ereignissen deutlich lernen kann, wenig Grundlage. Eine ausführliche Analyse der Gründe hierfür wäre spannend, liegt aber bisher nicht vor.

Ein wichtiger Aspekt ist sicherlich, dass die Auswertung der Ereignisse von einer ganz anderen Personengruppe durchgeführt wird als jener, die im täglichen Betrieb eines AKW oder in der Ausarbeitung von Maßnahmen an der vordersten Front steht. Dieser Widerspruch lässt sich kaum auflösen, da für die eine Tätigkeit ganz andere Quali-

fikationen und Profile der ausführenden Personen gebraucht werden als für die andere.

Ein weiterer Effekt ist die verbreitete Abwehrhaltung der Praktiker gegen die von den Sicherheitstheoretikern ausgearbeiteten Analysen – und die daraus zu ziehenden Schlussfolgerungen. Gerade die in Deutschland seit einiger Zeit geforderte Einführung eines Sicherheitsmanagements zeigt dies. Die bestehende behördliche Forderung ist bisher wenig konkretisiert worden. Die einzelnen Betreiber führen solche Systeme ein. Aber gerade im innerbetrieblichen Umsetzen zeigen sich die Schwierigkeiten. Es bleibt für jeden Praktiker eine Gratwanderung, ob Fehler dargestellt werden sollen. Denn dies kann leicht zu Eingeständnissen und persönlichen Schwierigkeiten führen, wenn sich das Management nicht bewusst solche Konsequenzen verbietet. Andererseits ist es in der täglichen Praxis nur schwer möglich, die vielen theoretischen Forderungen, die sich aus dem Sicherheitsmanagement ergeben, wirklich vollständig einzuhalten.

Heute ist unter kerntechnischen Fachleuten – unabhängig von ihrer Einstellung zur Kernenergienutzung – unbestritten, dass bei den bestehenden Reaktoren schwere Reaktorunfälle mit Kernschmelzen und massiven Radioaktivitätsfreisetzungen physikalisch und technisch möglich sind – wenn zu viele der Sicherheitssysteme versagen. Im Lichte der diskutierten Schwachstellen sind solche Unfälle auch in Zukunft nicht auszuschließen.

Anmerkungen

[1] *Vattenfall, Kraftwerkgruppe Forsmark (FKA):* Analyse des laufenden Betriebs, des Qualitätsmanagements und der Leitungsprozesse innerhalb des FKA, Stockholm, 23.10.2006, Nummer des Dokuments FM-206-0968, unautorisierte Übersetzung aus dem Schwedischen.

[2] *GRS:* Ereignis im schwedischen Kernkraftwerk Forsmark, Block 1 am 25.7.2006: „Nichtzuschalten von zwei Notstromdieseln beim Ausfall der 400-kV-Netzanbindung", Köln 14.11.2006, WLN 2006/07. Internet: http://www.bmu.de/files/download/application/pdf/forsmark_oeko_institut_grs.pdf

[3] *OECD:* Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System, Paris 2006, NEA No. 6150. Internet: http://www.nea.fr/html/nsd/reports/2006/nea6150-irs.pdf