

21. September 2007

Bundesamt für Energie  
Sektion Recht  
Mühlestrasse 4  
3063 Ittigen

**Stellungnahme zu:**

## **HSK-Richtlinie A01**

# **Anforderungen an die deterministische Störfallanalyse für Kernanlagen: Umfang, Methodik und Randbedingungen der technischen Störfallanalyse**

---

# 1 Zusammenfassung

Mit der neuen Atomgesetzgebung und der Neunummerierung der Richtlinien wird der Zusammenhang mit den bestehenden Richtlinien A01 „Anforderungen an die deterministische Störfallanalyse für Kernanlagen: Umfang, Methodik und Randbedingungen der technischen Störfallanalyse“ nicht klar. Die Richtlinie R-101 „Auslegungskriterien für Sicherheitssysteme von Kernkraftwerke mit Leichtwasser-Reaktoren“ wird nicht referenziert, ist aber (in ihrem eingeschränkten Zweck) näher am Stand von Wissenschaft und Technik als die A01, welche dies für sich in Anspruch nimmt.

Die Richtlinie nimmt zwar nicht mehr wie die früheren Bezug auf neue AKW, aber sie bringt auch keinen Gewinn zur Beurteilung der „Defizite“ älterer Anlagen. Es ist jedoch eine starke Tendenz auszumachen, die Anforderungen an die Sicherheit von AKW herunterzuschrauben. Dies ist am - gegenüber früher - aufgeweichten Konzept der Störfallhäufigkeit und an der Behandlung von Operateurhandlungen gut zu verfolgen.

Vor allem stossend ist die explizite Ausklammerung verschiedener Auslegungsstörfälle wie derjenige des Sicherheitserdbebens. Offensichtlich haben die Ergebnisse der PEGASOS-Studie die Behörden zu sehr erschreckt.

## 2 Allgemeines

### 2.1 Killerkriterien

Das Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK hat im Zusammenhang mit der neuen Atomgesetzgebung die „Verordnung des UVEK über die Methodik und die Randbedingungen zur Überprüfung der Kriterien für die vorläufige Ausserbetriebnahme von Kernkraftwerken“ zur Vernehmlassung herausgegeben. Diese Verordnung soll die Aufsichtspraxis und die Anwendung des Regelwerks bei laufenden AKW regeln.

Heute sind die fünf AKW der Schweiz zwischen 23 und 36 Jahre alt. Die Ausserbetriebnahmekriterien zu definieren – also Killerkriterien für den Betrieb von AKW -, sollte die vordringlichste Arbeit für die Aufsichtsbehörden sein. Sie werden abgeleitet aus den strengeren Richtlinien, welche den Stand von Wissenschaft und Technik betreffen.

Mit der A01 beansprucht die Hauptabteilung für die Sicherheit der Kernanlagen HSK, den Stand von Wissenschaft und Technik zu konkretisieren. Sie könne aber „Abweichungen im Einzelfall zulassen“.

*In der vorliegenden Stellungnahme messen wir unter Anderem die A01 an ausgewählten „Abweichungen“, heisst von der HSK tolerierten Gefahren, der Schweizer AKW vom Regelwerk.*

### 2.2 Unterlagen zu unserer Stellungnahme

Wir beziehen uns auf die Aufsichtspraxis der HSK bzw. die Bewilligungspraxis der Behörden.

Ihre Gutachten werden im Zeitrahmen von 1991 bis 2004 betrachtet. Wir zitieren vorwiegend Beurteilungen des AKW Mühleberg. Wichtig ist auch die jüngst herausgekommene Kurzfassung der PEGASOS-Studie. Wo nötig wurde die in Vernehmlassung stehende Richtlinie A05 „Anforderungen an die Qualität und den Umfang einer Probabilistischen Sicherheitsanalyse (PSA)“ zum Vergleich herangezogen. Auf sie gehen wir aber nicht näher ein.

### 3 Kritikpunkte

In diesem Kapitel werden grundsätzliche Einwände gegen die Richtlinie A01 vorgetragen. Sie beziehen sich lediglich auf Inkonsistenzen und Mängel in den Anforderungen an den Betrieb von AKW.

#### 3.1 Rechtlicher Zusammenhang

Die vorliegende Richtlinie A01 konkretisiert die „Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen“, Art. 14, Abs. 2., sowie die Strahlenschutzverordnung StSV, Art. 94, Abs. 8. Was die radiologische Störfallanalyse betrifft, werden in der A01 die Richtlinien HSK-A08 und G-14 erwähnt. Zudem wird auf die Kernenergieverordnung SR 732.11 zurückgegriffen. Folgende bisherigen Richtlinien werden nicht zitiert:

R-100 „Nachweis ausreichender Vorsorge gegen Störfälle in Kernkraftwerken (Störfall-Richtlinie)“ und R-101 „Auslegungskriterien für Sicherheitssysteme von Kernkraftwerken mit Leichtwasser-Reaktoren“. Die Neu Nummerierung der in Vernehmlassung stehenden Richtlinien fördert den Verdacht, dass der Rückgriff auf die bestehenden Richtlinien aufgeweicht wird.

*Ohne explizite Voraussetzung beziehungsweise Integration v.a. der R-101 bedeutet die vorliegende Richtlinie einen unvermeidbaren Rückschritt gegenüber der bisher gültigen Regulierung. Deterministische Kriterien der Separation, Diversität, Prüfbarkeit, Automatisierung und Ergonomie etc. fehlen vollständig. Sie gehören bedingungslos zum Umfang einer Störfallanalyse.*

#### 3.2 Nichterreicherung des Standes der Wissenschaft und Technik

##### 3.2.1 Grundsätzliches zum Stand von Wissenschaft und Technik

Kapitel 1 der A01:

In der Einleitung der A01 wird angeführt: „Die HSK kann im Einzelfall Abweichungen zulassen, wenn die vorgeschlagene Lösung in Bezug auf die nukleare Sicherheit mindestens gleichwertig ist.“ Dieser Satz dürfte eine der interessantesten Stellen der ganzen Richtlinie sein. In den weiteren Kapiteln der A01 wird das Problem nicht mehr aufgegriffen.

*Dass der Umgang mit Abweichungen in der Einleitung nur nebenbei erwähnt und nicht in den Bestimmungen zur technischen Analyse von Auslegungsstörfällen selbst behandelt wird, macht die Verordnung über die Ausserbetriebnahmekriterien zur Makulatur.*

Das bedeutet: Nach wie vor sträuben sich die Behörden, konkrete Kriterien für gültige „Abweichungen“ und letztlich für die Ausserbetriebnahme von AKW zu formulieren. Nach wie vor bleiben die behördlichen Beurteilungen alter AKW im Bereich willkürlicher Substitution des Regelwerks.

### **3.2.2 Fehlendes Mass für „gleichwertige Sicherheit“**

Die älteren drei AKW der Schweiz haben insgesamt eine zehnmal höhere Kernschadenshäufigkeit als die neueren. Diese Differenz resultiert aus der Differenz der Auslegung. Mit den neuen Erkenntnissen aus den Erdbebenstudien hat sich überdies gezeigt, dass die Kernschadenshäufigkeit der Schweizer AKW nicht mehr wie früher angenommen eine Grössenordnung geringer ist als die Richtwerte der IAEA. Es fehlen durchwegs die Kriterien, an welchen „gleichwertige Sicherheit“ gemessen werden könnte. Darüber wird in der A01 nichts geschrieben.

*Die Vorgabe der HSK, dass die Kompensation eines Mangels an regelkonformer Auslegung gleichwertige Sicherheit biete (s.o.), ist in etlichen Fällen bei den Alt-AKW nicht haltbar (s. unten Kap. 4).*

## **3.3 Störfallhäufigkeit**

### **3.3.1 Einbezug des Einzelfehlers**

Kapitel 4.1.1 und Kapitel 4.1.3, c)

Entgegen den alten Richtlinien (vor Herausgabe der heutigen R-100 von 2004) wird bei der Einteilung der Störfallkategorien neu nicht nur mit dem auslösenden Ereignis, sondern auch mit einem Einzelfehler (vorgegebene Häufigkeit von 0.1/a) gerechnet. Zugleich wird aber verlangt: „Falls ein Störfall aufgrund der Unterstellung eines Einzelfehlers einer höheren (vermutlich = tieferen, d.Verf.) Störfallkategorie zugeordnet wird und damit andere Nachweiskriterien gelten, ist der Nachweis der Störfallbeherrschung auch ohne Einzelfehler zu erbringen.“

*Mit dieser Forderung ist allerdings der Sinn der Neudefinition der Störfallhäufigkeit undurchsichtig; denn der deterministische Nachweis für die radioaktive Freisetzung bleibt letztlich doch abhängig von der Häufigkeit des Auslösers. Dies gilt, solange keine weiteren Bedingungen – welche an sich erforderlich wären – an den relativen Schweregrad der Unfälle innerhalb einer Störfallkategorie gestellt werden.*

### **3.3.2 Berücksichtigung des Anlagezustands**

Kapitel 4.1.2

Es wird verlangt, dass die Anlagezustände analysiert werden müssen. Dabei wird der Zeitabschnitt berücksichtigt, während dem der Zustand gilt. Das Eintreten eines Einzelfehlers pro Jahr wird entsprechend kleiner.

Nicht geregelt ist aber:

Wie bestimmen sich die Störfallkategorien pro Anlagezustand? Mit den Festlegungen in Kapitel 4.1.2 kann ein an sich heftiger Fehler während eines speziellen Zustands - welcher nur in diesem Zustand auftreten kann - zu einem geringen (weil übers Reaktorjahr gemittelten) „Ereignis“ werden. Es ist aber für die Bestimmung der Dringlichkeit von Vorsorgemassnahmen zentral, Unfälle auf ein „Zustandsjahr“ (also z.B. pro Jahr des Anlagestillstands) zu beziehen.

*Das Störfallkonzept ist zu wenig durchdacht. Es ist richtig, Anlagezustände in der Analyse zu differenzieren. Aber die Auswirkungen während des Zustands dürfen nicht mit rechnerischen Tricks tiefer bewertet werden.*

### **3.3.3 Ausserachtlassung der Diversität**

Während in den PSA (s. A05) die Analyse der Common Cause Failures CCF zwingend analysiert werden müssen, spielen sie in der A01 keine Rolle. Hier zeigt sich auch der mangelnde Rückgriff auf die R-101.

*Die HSK macht es sich zu leicht, ausdrücklich nur vom Versagen einer technischen Komponente, eines Teilsystems oder einem Operateurfehler auszugehen.*

Bedingungen, wann die CCF in der Analyse nicht berücksichtigt werden müssen, sind ausdrücklich aufzuführen und zu begründen.

## **3.4 Handlungen des Betriebspersonals**

Handlungen des Betriebspersonals werden von der HSK seit bald 20 Jahren bei der Störfallbeherrschung in Betracht gezogen. Es liegt auf der Hand, dass dies dem ursprünglichen Konzept der Reaktortechnik widerspricht (30-Minuten-Regel). Der Einbezug von Handeingriffen bei den Störfallanalysen offensichtlich wichtig, weil anders der Nachweis für die Einhaltung der Strahlenschutzverordnung nicht hätte erbracht werden können.

Operateurhandlungen werden in der A01 an verschiedenen Orten erwähnt: im Zusammenhang mit dem Einzelfehler und als eigenes Unterkapitel.

### Kapitel 4.4.4

Unterstellt man Erfolg versprechende Operateurhandlungen innerhalb der ersten 30 Minuten, so sind jene sehr spezielle „Sicherheits“systeme, für welches auch spezielle zusätzliche deterministische Annahmen zu treffen sind. Gerade durch das Fehlen der technisch erforderlichen Sicherheitskomponenten erhalten menschliche Eingriffe eine hohe Importanz, was sich in strengeren Anforderungen widerspiegeln muss.

*Die HSK ordnet den Operateurhandlungen nicht die nötige Gefährlichkeit zu und definiert demzufolge keine speziellen deterministischen Anforderungen. In den zusätzlichen Ausfallausnahmen (Kap. 4.4.3) müssen solche Handlungen (zumindest mit Berücksichtigung von Zeitverzögerungen) einbezogen werden.*

Wie unsystematisch die HSK mit Operateurhandlungen umgeht, zeigt sich im Quervergleich mit der A05 (dort wird in den grundsätzlichen Punkten zwar auch nur die „Bewertung der sicherheitstechnischen Bedeutung (Importanz) von Komponenten“, ohne Handeingriffe, erwähnt): In der A05 werden drei Typen von Operateurhandlungen (A, B, C) eingeführt. Die A01 scheint von solchen Erkenntnissen unberührt.

## **3.5 Wegfall von Unfallszenarien**

### Anhang 3:

Bei der Störfallanalyse werden entgegen aller bisherigen, auch internationalen, Praxis verschiedene Unfallarten ausgeschlossen. Dazu gehören als auffälligste das

Sicherheitserdbeben und der Flugzeugabsturz. Es ist nicht klar, wie diese Unfälle für die Aufsichts- und die Bewilligungspraxis behandelt werden sollen.

Es ist klar, dass kein Schweizer AKW nach den neuesten Erkenntnissen über die Erdbebengefährdung mehr betrieben werden darf. Das ist der wirtschaftliche und psychologische Grund für die Streichung des Sicherheitserdbebens aus der Störfallanalyse.

*Es geht nicht an, dass bisher elementare Auslegungsstörfälle gestrichen werden. Zudem ist es ein Skandal, dass sich die HSK nicht einmal die Mühe nimmt, wie sie Ergebnisse aus der Analyse der Erdbebengefahren berücksichtigen wird. Dies gilt allgemein für alle Unfälle, welche im Anhang 3 aufgeführt werden.*

## **4 Fehlende Anforderungen an Begründungen in der bisherigen Praxis**

In diesem Kapitel werden die vorliegenden Richtlinien mit einigen Beispielen der bisherigen Aufsichts- und Bewilligungspraxis der HSK verglichen. Es wird gezeigt, dass die schweizerischen Richtlinien für die strenge Beurteilung der Schweizer AKW noch immer keine Rechtssicherheit bieten.

### **4.1 Einbezug von Betriebssystemen**

In der A01 wird festgelegt (Kapitel 4.4.2 a, b.) dass nur Sicherheitssysteme in der Analyse der Auslegungsstörfälle betrachtet, Betriebssysteme aber im Falle möglicher nachteiliger Beeinflussung des Störfalls berücksichtigt werden sollen.

Im Gutachten zum Gesuch um unbefristete Bewilligung und Leistungserhöhung für das Kernkraftwerk Mühleberg (HSK, 1991) argumentiert die HSK auf S.8-40: „Bei vollständiger Torusentleerung würden alle Pumpen auf -11m überflutet und auch alle Lochrohrdüsen aus dem Wasser austauschen. In diesem Fall wäre man ausschliesslich auf Betriebssysteme (Speisewasser- und Kondensatsystem) zur Kernkühlung und Nachwärmeabfuhr angewiesen.“

*Wie beim Bewilligungsverfahren seinerzeit vorgetragen, muss das AKW Mühleberg schon deswegen stillgelegt werden, weil Betriebssysteme als Notsysteme gerechnet werden.*

Nach wie vor bleibt die HSK die Antwort schuldig, weshalb – deterministisch - Betriebssysteme unter ungünstigen Umständen als Sicherheitssysteme gelten können.

### **4.2 Automatisierung**

Die Berücksichtigung von Operateurhandlungen ist problematisch und von uns immer kritisiert worden. Wie komplex solche Handlungen werden können, zeigt sich auch im Gutachten der HSK im Bewilligungsverfahren des AKW Beznau II:

„Die dominante Bedeutung der Operateurhandlungen zur Einleitung einer alternativen Kühlung nach Ausfall des Restwärmesystems ist darauf zurückzuführen, dass aufgrund der Anlagenauslegung eine Vielzahl von Optionen für den Einsatz der erforderlichen Systeme bestehen, die alle manuell eingeleitet werden.“ (KKW Beznau II: Gutachten zum Gesuch der NOK um Aufhebung der Befristung der Betriebsbewilligung; HSK, 2004; S.8-81).

Technische Defizite, welche nachträglich durch Handeingriffe kompensiert werden sollen, tragen immer das Risiko von Fehlüberlegungen in sich. Dies zeigte sich während dem Bewilligungsverfahren zum AKW Mühleberg: Beim ATWS-Unfall sollten Operateure das Wasserniveau im RDB auf die Kernoberkante absenken; dem stand aber – von den Autoren

unbemerkt – die Tatsache gegenüber, dass die Automatik dies eben gerade verhindern würde. Die Lösung solcher Probleme mit weiteren Betriebsvorschriften, Umgehungsmöglichkeiten der einmal eingerichteten Automatik und mit neuen Alarmierungshilfen verlagert einfach die Schwierigkeiten.

*Der Komplexitätsgrad von Operateurhandlungen an Stelle technischer Automatik ist zu gross. Unter diesen Umständen - wie oben geschildert - darf ein AKW nicht mehr betrieben werden.*

Eine „Entschuldigung“ für diese Auslegungs-Missstände in den alten Schweizer AKW legt die A01 nicht auf den Tisch.

### **4.3 Separation**

Im AKW Mühleberg wurde schon lang festgestellt, dass im Torusbereich auf -11m, aber nicht nur dort, eine dem Stand der Technik entsprechende Separation nicht zu erreichen ist. Dies wurde 1991 von der HSK explizit bestätigt.

Damals argumentierte die HSK damit, dass diese Nachrüstungen „nicht mit vertretbarem Aufwand voll realisiert werden können.“ Aus technischer Sicht ist eine solche Argumentation skandalös. Eine Aufsichtsbehörde hat lediglich festzuhalten, auf welchem Unsicherheitsniveau sich der AKW-Betrieb bewegen darf.

*Separation als Kriterium ist in einer Richtlinie zur Störfallanalyse aufzuführen. Vor allem sind Angaben zu machen, wie weit und weshalb der reale Stand der Schweizer AKW vom Soll abweichen darf.*

Die A01 erhellt die Argumentation von damals in keiner Weise.

### **4.4 Erdbeben**

Die HSK listet in der PSÜ Mühleberg 2002 und im Gutachten zu Beznau II im Bewilligungsverfahren 2004 eine ganze Reihe von Sicherheitssystemen und –Komponenten auf, welche nicht für das Sicherheitserdbeben SSE ausgelegt sind. Seither hat sich die Lage verschlimmert: 2004 wurde die PEGASOS-Studie zur Erdbebengefährdung an den AKW-Standorten der Schweiz fertig gestellt und intern zu Stellungnahmen und weiteren Analysen weiter gegeben. Die zu erwartenden Kräfte sind in den bisherigen Auslegungsbereichen (Unfallhäufigkeiten) mehr als doppelt so gross als bisher angenommen. Deshalb ist, wie den letzten Aufsichtsberichten der HSK zu entnehmen ist, eine Kampagne für Risikoanalysen und für Verbesserungen gestartet worden.

*Schon nach früheren Erkenntnissen, spätestens aber seit der PEGASOS-Studie, müssen die Schweizer AKW ausser Betrieb genommen und nachgerüstet werden. Dies ist vor allem für die alten drei AKW von grosser Dringlichkeit.*

### **4.5 Risiko-Kriterien**

Seit etwa 1990 betont die HSK in den Publikationen und Gutachten im Rahmen von Bewilligungsverfahren, wie wichtig probabilistische Untersuchungen bei der Beurteilung von AKW seien. Das ist sicher richtig, wenn es darum geht, in Fehlerbäumen Schwachstellen zu identifizieren.

Leider ist aber die Argumentation in die Richtung gegangen, dass gewisse Ausfälle bei Auslegungsstörfällen als „sehr unwahrscheinlich“, „nach menschlichem Ermessen auszuschliessen“ und Dergleichen mehr abgetan wurden – womit der Unfall als beherrscht

„nachgewiesen“ war. Das motivierte die HSK auch, Betriebssystemen in Mühleberg den Status eines Notsystems zuzuschreiben (s.o.). Die Philosophie in der Kerntechnik wurde somit langsam verändert, ohne dass für die neuen Instrumentarien verbindliche Regelungen erstellt wurden. Gemeint sind hier nicht die A05 oder die früheren Leitfäden für die Erstellung von PSA. Vergeblich sucht man im schweizerischen Regelwerk, wie die Resultate einer PSA zu beurteilen sind, welche Konsequenzen beispielsweise aus einer Risikodominanz zu ziehen sind. (Angemerkt sei hier, dass Risiko nicht nur die Eintretenshäufigkeit, sondern auch das Schadensausmass beinhaltet).

*Im Sinne von Ausserbetriebnahmekriterien soll endlich der Stellenwert der Resultate probabilistischer Studien festgelegt werden, was aus Behördensicht tolerierbar ist und was nicht.*

## 5 Forderungen

- Die Abgrenzung der A01 gegenüber anderen Richtlinien und rechtlichen Grundlagen muss explizit getroffen werden.
- Bisher in den schweizerischen Richtlinien aufgeführte Auslegungsstörfälle müssen weiterhin in der Störfallanalyse bearbeitet und dürfen nicht davon ausgeschlossen werden. Dies gilt in spezieller Weise für das Erdbeben und den Flugzeugabsturz.
- Störfallhäufigkeiten sollen nicht mit verschiedenen Tricks heruntergerechnet werden.
- Innerhalb der Störfallkategorien sind Differenzierungen in konservativer Richtung vorzunehmen.
- Für Operateurhandlungen sind zusätzliche deterministische Kriterien, zumindest bezüglich der zeitlichen Verzögerung, zu berücksichtigen.
- Wichtige deterministische Anforderungen müssen zum Umfang einer deterministischen Störfallanalyse gehören. Dies betrifft insbesondere Separation und Common Cause Failures.
- Für Abweichungen der AKW-Auslegung vom Regelwerk müssen systematisch Kriterien aufgestellt werden.
- Es muss erklärt werden, wie eine PSA und deren Resultate zu gewichten sind.

Aufgrund der vorgelegten Richtlinien sind Mühleberg und Beznau I und II ausser Betrieb zu nehmen. Die Erdbebengefahr ist zu berücksichtigen, weswegen bis zur Einrichtung geeigneter Schutzvorkehrungen alle Schweizer AKW temporär stillgelegt werden müssen.

Bern, 21. September 2007

Jürg Aerni

Jürg Joss

Geht an: Bundesamt für Energie BfE  
Hauptabteilung für die Sicherheit der Kernanlagen HSK