
RSK-Stellungnahme
(460. Sitzung der Reaktor-Sicherheitskommission am 29.08.2013)

(Veröffentlicht im Bundesanzeiger, Amtlicher Teil, am 05.12.2013, B4)

RSK-Verständnis der Sicherheitsphilosophie

Inhaltsverzeichnis

1	Einleitung.....	2
2	Grundlage der kerntechnischen Sicherheit.....	2
3	Grundsätzliche Anforderungen an Organisation und Personal.....	2
4	Sicherheitsgrundsätze für die technische Anlagenauslegung.....	3
4.1	Grundsätze	3
4.2	Barrierenkonzept.....	4
4.3	Konzept der Sicherheitsebenen	4
4.4	Schutzziele und Sicherheitsfunktionen	6

1 Einleitung

Gemäß § 1 Nr. 2 AtG sind Leben, Gesundheit und Sachgüter vor den Gefahren der Kernenergie und der schädlichen Wirkung ionisierender Strahlen zu schützen. Dies ist das oberste Sicherheitsziel. Um dieses Sicherheitsziel zu erreichen, muss insbesondere gewährleistet sein, dass die nach dem Stand von Wissenschaft und Technik erforderliche Vorsorge gegen Schäden durch die Errichtung und den Betrieb einer kerntechnischen Anlage getroffen ist. Die Anlage muss so beschaffen sein und betrieben werden, dass sie jederzeit im bestimmungsgemäßen Betrieb und bei Störfällen sicher abgeschaltet und in abgeschaltetem Zustand gehalten, die Nachwärme abgeführt und die Strahlenexposition des Personals und der Umgebung auch unterhalb derjenigen Dosisgrenzwerte so gering wie möglich gehalten werden kann, die durch die Vorschriften des Atomgesetzes und der auf Grund des Atomgesetzes erlassenen Rechtsverordnungen festgesetzt sind. Außerdem sind in angemessenem Umfang organisatorische und technische Maßnahmen zur Begrenzung der Auswirkungen von auslegungüberschreitenden Anlagenzuständen vorzusehen.

Die im Folgenden dargestellte Sicherheitsphilosophie soll eine konsistente Interpretation der in den „Sicherheitsanforderungen an Kernkraftwerke“ konkretisierten technischen und organisatorischen Anforderungen und eine schlüssige Einordnung zukünftiger neuer Anforderungen in das gestaffelte Sicherheitskonzept unterstützen.

2 Grundlage der kerntechnischen Sicherheit

Mensch, Technik und Organisation sind in einem ganzheitlichen Ansatz so aufeinander abzustimmen, dass das oberste Sicherheitsziel eingehalten ist und Gefahren für die Umgebung des Kernkraftwerks durch frühe oder große Freisetzungen¹ ausgeschlossen sind².

3 Grundsätzliche Anforderungen an Organisation und Personal

Der Genehmigungsinhaber hat sicherzustellen, dass

- (1) durch die Auslegung der Anlage die Sicherheitsanforderungen erfüllt werden und der erforderliche Qualitätszustand der Anlage über die gesamte Lebensdauer hinweg erhalten wird. Hierbei sind die Weiterentwicklung des Standes von Wissenschaft und Technik, die sicherheitsrelevanten Erfahrungen bei Bau und Betrieb in der eigenen Anlage und in fremden Anlagen sowie alle relevanten Alterungsphänomene zu berücksichtigen,

¹ **Frühe Freisetzung:** Freisetzungen radioaktiver Stoffe in die Umgebung der Anlage aufgrund eines frühzeitigen Versagens oder einer Umgehung des Sicherheitsbehälters, die Maßnahmen des anlagenexternen Notfallschutzes erfordern, für deren Umsetzung nicht ausreichend Zeit zur Verfügung steht.

Große Freisetzung: Freisetzungen radioaktiver Stoffe in die Umgebung der Anlage, die räumlich umfangreiche und zeitlich langandauernde Maßnahmen des anlagenexternen Notfallschutzes erfordern.

² **„ausgeschlossen“:** Das Eintreten eines Ereignisses oder Ereignisablaufs oder Zustands kann als ausgeschlossen angesehen werden, wenn das Eintreten physikalisch unmöglich ist oder wenn mit einem hohen Maß an Aussagesicherheit das Eintreten als extrem unwahrscheinlich angesehen werden kann. Dies gilt z. B. für die Überlagerung von zwei unabhängigen, jeweils für sich unwahrscheinlichen Ereignissen.

-
- (2) durch ein wirksames Managementsystem die technischen, organisatorischen und administrativen Voraussetzungen zur Gewährleistung der Anlagensicherheit jederzeit gegeben sind und durch kontinuierliche Verbesserungen weiterentwickelt werden,
 - (3) eine ausgeprägte Sicherheitskultur in der Organisation entwickelt ist und insbesondere durch die Führungspersonen in der gesamten Unternehmens- und Anlagenhierarchie vorgelebt und bestärkt wird,
 - (4) die Zuverlässigkeit und Fachkunde des Anlagenpersonals gewährleistet sind,
 - (5) durch eindeutige Festlegungen Aufgaben- und Verantwortungsbereiche in der Organisation einander zugeordnet sind,
 - (6) die erforderlichen Prozeduren zum Erhalt eines sicheren Anlagenzustands, zum sicheren Betrieb, zur Beherrschung von Ereignissen sowie zur Begrenzung von Auswirkungen vorhanden und wirksam sind,
 - (7) identifizierte sicherheitstechnische Verbesserungspotentiale, soweit angemessen, umgesetzt werden,
 - (8) die personellen und finanziellen Ressourcen zur Gewährleistung der Anlagensicherheit bereitgestellt werden.

4 Sicherheitsgrundsätze für die technische Anlagenauslegung

4.1 Grundsätze

- (1) Zur Einhaltung des obersten Sicherheitsziels sind die im Kernkraftwerk vorhandenen radioaktiven Stoffe durch technische Barrieren und Rückhaltefunktionen mehrfach einzuschließen und ihre Strahlung ist ausreichend abzuschirmen. Die Wirksamkeit der Barrieren und Rückhaltefunktionen ist durch die Erfüllung der Schutzziele
 - Kontrolle der Reaktivität,
 - Kühlung der Brennelemente und
 - Einschluss der radioaktiven Stoffe

abzusichern.

Es ist ein gestaffeltes Sicherheitskonzept zu realisieren, mit dem gewährleistet wird, dass bei allen zu betrachtenden Ereignissen, die unter Berücksichtigung ihrer Eintrittshäufigkeit gestaffelten Sicherheitsebenen zugeordnet sind, die Schutzziele erfüllt werden und die Barrieren und Rückhaltefunktionen im erforderlichen Umfang erhalten bleiben.

Ziel einer Staffelung ist es, eventuelle Fehler und Ausfälle durch weitere Maßnahmen und Einrichtungen kompensieren zu können.

(2) Durch die Umsetzung des gestaffelten Sicherheitskonzeptes sind unzulässige radiologische Auswirkungen infolge

- zu unterstellender technisch oder menschlich bedingter anlageninterner Versagensereignisse oder
- eines Ereignisses mit anlagenexternem natur- oder zivilisationsbedingtem Ursprung

zu verhindern. Das heißt, die Eintrittshäufigkeit für Ereignisabläufe, die zu radiologischen Auswirkungen oberhalb der Dosiswerte der §§ 46 und 47 bzw. des § 49 der Strahlenschutzverordnung führen können, ist jeweils ausreichend gering zu halten. Ereignisabläufe mit frühen oder großen Freisetzungen radioaktiver Stoffe sind auszuschließen.

(3) Im Rahmen des gestaffelten Sicherheitskonzeptes sind gestaffelte, wirksame und zuverlässige Maßnahmen und Einrichtungen einerseits zum Vermeiden von Störungen und Verhindern von Störfällen, andererseits zum Beherrschen dennoch unterstellter Störungen und Störfälle sowie Maßnahmen und Einrichtungen zum Begrenzen der Auswirkungen von auslegungsüberschreitenden Anlagenzuständen und zum Ausschluss von Ereignisabläufen mit frühen oder großen Freisetzungen vorzusehen.

4.2 Barrierenkonzept

(1) Das Barrierenkonzept umfasst gestaffelte Barrieren und Rückhaltefunktionen zum Einschluss der radioaktiven Stoffe.

(2) Die erforderliche Anzahl und Auslegung der gestaffelten Barrieren sowie Rückhaltefunktionen soll sich orientieren an

- der radiologischen Bedeutung des einzuschließenden Aktivitätsinventars,
- den potenziellen Freisetzungsmechanismen,
- der erreichbaren Wirksamkeit und Zuverlässigkeit der zum Einschließen eingesetzten Maßnahmen und Einrichtungen sowie
- der Häufigkeit von gefährdenden Einwirkungen auf die Barrieren und Rückhaltefunktionen.

(3) Die jeweils erforderliche Wirksamkeit und Zuverlässigkeit der Barrieren und Rückhaltefunktionen ist durch entsprechende Qualität bei Auslegung und Fertigung sowie Überwachung und Instandhaltung im Betrieb zu gewährleisten.

4.3 Konzept der Sicherheitsebenen

(1) Für Ereignisse, die die Wirksamkeit von Barrieren und Rückhaltefunktionen oder die Einhaltung der Schutzziele direkt oder indirekt beeinträchtigen können, sind Maßnahmen und Einrichtungen zum Vermeiden und Beherrschen derartiger Ereignisse im erforderlichen Umfang vorzusehen. Dabei ist das „je-desto-Prinzip“ zu beachten, d. h. je häufiger ein Ereignis zu erwarten ist, desto geringer soll die dadurch mögliche radiologische Auswirkung sein bzw. je schwerer die Folgen eines Ereignisses sein können, desto geringer soll seine Eintrittshäufigkeit sein. Dabei sind

- ein möglichst störungsfreier Betrieb durch zuverlässigkeitsfördernde Auslegungs-, Fertigungs- und Betriebsgrundsätze zu gewährleisten sowie Abweichungen vom Normalzustand frühzeitig zu erkennen und weitgehend zu begrenzen, so dass Betriebsstörungen vorgebeugt wird,
 - dennoch auftretende Störungen möglichst zu beherrschen und damit das Auftreten von Störfällen zu vermeiden,
 - die zuverlässige Beherrschung von dennoch postulierten Störfällen sicherzustellen und damit die Ausweitung eines Störfalles zu einem auslegungsüberschreitenden Anlagenzustand zu verhindern sowie,
 - für den Fall eines dennoch eintretenden auslegungsüberschreitenden Anlagenzustands (Unfall) die Auswirkungen zu begrenzen sowie Ereignisabläufe mit frühen oder großen Freisetzung radioaktiver Stoffe auszuschließen.
- (2) Eine übergeordnete sicherheitstechnische Zielsetzung des Konzepts der gestaffelten Sicherheitsebenen ist es, die auf einer Sicherheitsebene evtl. nicht beherrschten Ereignisabläufe auf der nächsten Sicherheitsebene aufzufangen.
- (3) Die Ereignisse und Anlagenzustände, die zu sicherheitstechnisch relevanten Abweichungen vom Normalbetrieb führen können, sind Ereignisklassen und Sicherheitsebenen mit jeweils zu berücksichtigenden Anfangs- und Randbedingungen, Postulaten sowie einzuhaltenden Nachweiszielen zuzuordnen. Es sind folgende Ereignisklassen und zugeordnete Sicherheitsebenen zu unterscheiden, wobei deren jeweils angegebenen Eintrittshäufigkeiten als Orientierungswerte zu verstehen sind:
- Normalbetrieb (Sicherheitsebene 1)
 - Betriebsstörungen (Sicherheitsebene 2) größer ca. $10^{-2}/a$
 - Auslegungsstörfälle (Sicherheitsebene 3) kleiner ca. $10^{-2}/a$ bis größer ca. $10^{-5}/a$
 - auslegungsüberschreitende Anlagenzustände (Sicherheitsebene 4) kleiner ca. $10^{-5}/a$

Für Einwirkungen von Innen und Außen, die in den „Sicherheitsanforderungen an Kernkraftwerke“ nicht einer Sicherheitsebene zugeordnet sind, gelten Anforderungen entsprechend einer anlagen- und standortspezifischen Zuordnung der Bemessungsgrößen zu den Sicherheitsebenen unter Verwendung der Orientierungswerte.

Bei wetterbedingten Einwirkungen von außen ist eine Zuordnung der Anforderungen zur Sicherheitsebene 3 bis zu einer Eintrittshäufigkeit von $10^{-4}/a$ ausreichend, da bei noch niedrigeren Eintrittshäufigkeiten und damit tendenziell höheren Einwirkungen diese entweder frühzeitig erkennbar sind und damit auch frühzeitig Maßnahmen auf der Sicherheitsebene 4 eingeleitet werden können oder das Schadenspotential eingegrenzt ist.

- (4) Es ist zudem zu zeigen, dass für die Summe der auslegungsüberschreitenden Anlagenzustände in allen Betriebsphasen des Leistungs- und Nichtleistungsbetriebs der Erwartungswert für die Kern-

schadenshäufigkeit (Ereignisse im Lagerbecken sind mit zu berücksichtigen) nicht mehr als 10^{-5} /a je Anlage beträgt.

- (5) „Orientierungswert“ in (3) bedeutet, dass Ereignisse, einschließlich der Kombination von Ereignissen untereinander und der Kombination von Ereignissen mit Betriebszuständen, den Sicherheitsebenen nicht alleine im Hinblick auf die genannten Häufigkeitsbereiche zugeordnet werden sollen.

In jedem Fall sind bei der Zuordnung die Unsicherheiten in den Ermittlungen der Eintrittshäufigkeiten und in den Ereignisablaufanalysen sowie die dazu jeweils vorliegende Aussagesicherheit ebenfalls zu berücksichtigen (Unsicherheiten sind bedingt u. a. durch die Komplexität der für den Ereignisablauf relevanten Zusammenhänge, Vollständigkeit der Kenntnisse zu relevanten Phänomenen, Belastbarkeit der Datenbasis.).

Ferner ist zu berücksichtigen, dass es zur Dimensionierung von Sicherheits- oder Systemfunktionen sinnvoll sein kann, Szenarien in Form von abdeckenden Ereignissen zu postulieren (wie z. B. das postulierte 2 F-Leck der Hauptkühlmittelleitung eines DWR für die Einspeisekapazität des Not- und Nachkühlsystems), die unabhängig von ihrer Eintrittshäufigkeit Sicherheitsebenen zugeordnet sind.

- (6) Mit der Zuordnung eines Ereignisses zu einer bestimmten Sicherheitsebene ist für die Nachweisführung in den „Sicherheitsanforderungen an Kernkraftwerke“ festgelegt, welche Postulate in der Ereignisanalyse zu berücksichtigen und welche Nachweiskriterien einzuhalten sind.

Für Kombinationen von auslösenden Ereignissen mit Ausfallannahmen, die über die in den „Sicherheitsanforderungen an Kernkraftwerke“ genannten hinausgehen (z. B. über das Einzelfehlerkonzept hinausgehende Ausfallannahmen), oder mit kurzzeitigen Betriebszuständen kann unter Berücksichtigung von (3) und (5) die Zuordnung dieses Ereignisablaufs zu einer Sicherheitsebene im Vergleich zum auslösenden Ereignis verändert werden.

Sonstige Anfangs- und Randbedingungen können im Rahmen von Unsicherheitsanalysen gemäß den „Sicherheitsanforderungen an Kernkraftwerke“ berücksichtigt werden, soweit nicht einzelne Parameterwerte explizit auch für Unsicherheitsanalysen „gesetzt“ sind, um in den Ereignisanalysen Sicherheitsmargen zu gewährleisten. Unwahrscheinliche Parameterwerte bzw. Kombinationen von Parameterwerten sind in der Unsicherheitsanalyse erfasst und ändern die Zuordnung des Ereignisses zu den Sicherheitsebenen nicht.

4.4 Schutzziele und Sicherheitsfunktionen

- (1) Die Einhaltung der Schutzziele (Kontrolle der Reaktivität, Kühlung der Brennelemente, Einschluss der radioaktiven Stoffe) ist durch entsprechende Sicherheitsfunktionen ggf. in Verbindung mit Vorsorgemaßnahmen zu gewährleisten¹. Die Sicherheitsfunktionen sollen gewährleistet werden durch

¹ Der Einschluss der radioaktiven Stoffe umfasst hier diejenigen Funktionen, die erforderlichenfalls Durchführungen durch die Barrieren verschließen oder Druckstaffelungen herstellen, um Aktivitätsfreisetzungen zu minimieren.

-
- Maßnahmen und Einrichtungen, die Zustände, die zur Gefährdung von Schutzzielen führen können, vermeiden, verhindern oder ausschließen,
 - Maßnahmen und Einrichtungen, die bei nicht auszuschließender Verletzung der Nachweiskriterien für die Schutzziele auf einer Sicherheitsebene die Auswirkungen auf der nachfolgenden Sicherheitsebene beherrschen oder begrenzen.
- (2) Die Sicherheitsfunktionen sind durch hinreichend wirksame und zuverlässige (dazu in erforderlichem Umfang gestaffelte) Maßnahmen und Einrichtungen sicherzustellen.
 - (3) Die erforderliche Zuverlässigkeit der Sicherheitsfunktionen ist an den Anforderungen der jeweils zugeordneten Sicherheitsebene sowie an den möglichen Folgen und der Beherrschbarkeit bei unterstellter Unwirksamkeit der Maßnahmen und Einrichtungen zu bemessen. Dabei sollen Maßnahmen und Einrichtungen zum Vermeiden, Verhindern oder Ausschließen soweit technisch vertretbar realisiert werden, auch wenn auf einer der nachfolgenden Ebene Maßnahmen und Einrichtungen zum Beherrschen vorhanden sind.
 - (4) Die erforderliche Wirksamkeit und Zuverlässigkeit der Sicherheitsfunktionen zum Beherrschen von Ereignissen sind so zu bemessen, dass die den Sicherheitsebenen zugeordneten Nachweisziele für ein hinsichtlich Auswirkungen und Eintrittshäufigkeiten der Ereignisklassen abdeckendes Spektrum von Ereignissen und Anlagenzuständen eingehalten werden und damit eine Ausweitung in die jeweils nächste Sicherheitsebene vermieden bzw. verhindert wird.
 - (5) Sicherheitsfunktionen zur Beherrschung eines Ereignisses mit sicherheitstechnisch potenziell bedeutsamen Auswirkungen sind im Einzelfall dann nicht erforderlich, wenn die Vorkehrungen (Vorsorgemaßnahmen) gegen das Eintreten des Ereignisses so zuverlässig gestaltet sind, dass dieses als ausgeschlossen bewertet werden kann.
 - (6) Für ein lückenloses Zusammenwirken von einerseits „Ausschließen“, „Verhindern“ oder „Vermeiden“ und andererseits „Beherrschen“ von Ereignissen ist es zudem erforderlich, dass die dafür im Rahmen des realisierten Sicherheitskonzepts kreditierten Maßnahmen und Einrichtungen mit ihren Voraussetzungen und ihren Anforderungen zum Erhalt der Wirksamkeit während der Betriebsdauer überwacht und unzulässige Abweichungen beseitigt werden.
 - (7) Die Sicherheitsfunktionen auf den Sicherheitsebenen 1 und 2 sollen grundsätzlich durch betriebliche Maßnahmen und Einrichtungen erfüllt werden, wobei entsprechend der Bedeutung für das Beherrschen von Abweichungen („Störungen“) und damit das Vermeiden eines Störfalls erforderlichenfalls darüber hinausgehende Anforderungen festzulegen sind (z. B. Reserven, Redundanz in aktiven Komponenten, Automatisierung, Notstromversorgung).

Die Beherrschung der der Sicherheitsebene 3 zugeordneten Ereignisse („Störfallbeherrschung“) ist durch Maßnahmen und Sicherheitseinrichtungen unter Berücksichtigung besonderer Auslegungsgrundsätze (z. B. Schutz gegen übergreifende Ausfälle infolge Einwirkungen von innen oder außen, Redundanz, ggf. Diversität, Automatisierung, fail safe) wirksam und zuverlässig zu gewährleisten.

Für Einrichtungen und Maßnahmen, die für Aufgabenstellungen auf der Sicherheitsebene 4 kreditiert werden, ist zu zeigen, dass sie unter den Randbedingungen der jeweiligen auslegungsüberschreitenden Anlagenzustände wirksam und mit hinreichender Zuverlässigkeit durchführbar sind.

- (8) Sofern von Einrichtungen Aufgaben für mehr als eine Sicherheitsebene erfüllt werden müssen, sind für die Auslegung dieser Einrichtungen die einhüllenden Anforderungen bezüglich Wirksamkeit und Zuverlässigkeit zu berücksichtigen. Weiterhin ist sicherzustellen, dass mit der vorhandenen Staffelung von Einrichtungen (Systemfunktionen) die Zuverlässigkeit der betroffenen Sicherheitsfunktion insgesamt so hoch ist, dass nicht nur die Zuverlässigkeitsanforderungen der Sicherheitsebenen 1 bis 3 erfüllt werden, sondern auch die Voraussetzungen zum Ausschluss früher oder erheblicher Freisetzen gegeben sind.