Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Nuklearsicherheitsinspektorat ENSI
Inspection fédérale de la sécurité nucléaire IFSN
Ispettorato federale della sicurezza nucleare IFSN
Swiss Federal Nuclear Safety Inspectorate ENSI

Auslegungsgrundsätze für in Betrieb stehende Kernkraftwerke

Ausgabe August 2019 (Änderung vom 1. Oktober 2024)

Erläuterungsbericht zur Richtlinie ENSI-G02/d

Inhalt

1 Ausgangslage

Die Basis für die Auslegung von Kernkraftwerken mit Leichtwasserreaktoren bildeten in der Schweiz ursprünglich die Auslegungsanforderungen der Herstellerländer, konkret die Anforderungen in den USA und in Deutschland. Die Anforderungen in den beiden Ländern waren nicht gleichwertig. Die Anforderungen in Deutschland verlangten unter anderem eine konsequente Trennung der einzelnen Stränge von Sicherheitssystemen, einschliesslich der dafür notwendigen Unterstützungssysteme. Zudem wurde in Deutschland früh das sogenannte n-2-Prinzip eingeführt, das heisst das Einzelfehler- und Instandhaltungsprinzip.

Diese teilweise grundsätzlichen Unterschiede in den Anforderungen an die amerikanischen und an die deutschen Anlagen verlangten in der Schweiz nach einer Anpassung in der Auslegung der beiden Reaktorkonzepte. In Richtlinien wurden die in der Schweiz anzuwendenden Regelungen festgehalten. Solche Richtlinien wurden erstellt, wenn zwischen den amerikanischen und deutschen Regelungen eine Wahl zu treffen oder ein Kompromiss zu finden war sowie wenn sonst ein Bedürfnis nach einheitlicher Regelung bestand. Ziel war ein für alle schweizerischen Kernkraftwerke vergleichbarer und hoher Stand der Sicherheit.

In der im Mai 1987 veröffentlichten Richtlinie HSK-R-101 „Auslegungskriterien für Sicherheitssysteme von Kernkraftwerken mit Leichtwasser-Reaktoren“ wurden erstmals Grundsätze für die Auslegung von Sicherheitssystemen festgeschrieben. Eine Reihe weiterer system- und komponentenspezifischer Richtlinien wurde im Laufe der Jahre verfasst, wenn ein Regelungsbedarf vorlag. Ebenso wurden Richtlinien im Bereich der Störfall- und Notfallvorsorge erlassen. Detaillierte bauliche, technische, organisatorische, personelle und administrative Massnahmen zur Sicherung wurden und werden in klassierten Richtlinien festgelegt und sind nicht Teil der Richtlinie ENSI-G02.

Die übergeordneten Sicherheitskonzepte wie das Schutzzielkonzept, das Barrierenkonzept und das Konzept der gestaffelten Sicherheitsvorsorge werden im Kernenergiegesetz (KEG) und der Kernenergieverordnung (KEV) zwar angesprochen, doch fehlte bisher eine umfassendere Darlegung dieser Konzepte und der zu deren Umsetzung notwendigen Auslegungsvorgaben. Diese Lücke wird durch die ENSI-G02 geschlossen.

Zudem werden Auslegungsvorgaben, die bisher in älteren Richtlinien (HSK-R-16, HSK-R-40, HSK-R-101 und HSK-R-103) festgeschrieben waren, sowie einige Anforderungen aus anderen Richtlinien zwecks besserer Abgrenzung der Auslegungsthematik (z. B. Auslegungsvorgaben aus der Richtlinie ENSI-B12) nach deren Überprüfung auf Aktualität in die Richtlinie ENSI-G02 übernommen. Im Weiteren erfolgt eine Harmonisierung mit internationalen Auslegungsanforderungen.

2 Harmonisierung mit internationalen Anforderungen

2.1 IAEA

Der zentrale Standard für die Auslegung von Kernkraftwerken ist der IAEA Safety Standard SSR-2/1 „Safety of Nuclear Power Plants: Design“. Viele darin enthaltene Empfehlungen sind bereits in schweizerischen Gesetzen, Verordnungen oder Richtlinien festgeschrieben. In die Richtlinie ENSI-G02 werden eine Reihe der bisher noch nicht im schweizerischen Regelwerk festgeschriebenen Empfehlungen des IAEA Safety Standard SSR-2/1 übernommen.

2.2 WENRA

Die „Western European Nuclear Regulators‘ Association“ (WENRA) hat europaweit harmonisierte Sicherheitsanforderungen (sogenannte „Safety Reference Levels“, SRL) für Kernkraftwerke festgelegt. Das ENSI hat sich verpflichtet, die Anforderungen der WENRA umzusetzen. Der Detaillierungsgrad der WENRA-Anforderungen übersteigt meist diejenigen des KEG und der KEV, weshalb sich auch hier deren Umsetzung in ENSI-Richtlinie anbietet.

Insbesondere in den Issues E (Design Basis Envelope for Existing Reactors) und F (Design Extension of Existing Reactors) sind Anforderungen an die Auslegung für in Betrieb stehende Kernkraftwerke festgelegt. Die im September 2014 veröffentlichten SRLs berücksichtigen Erkenntnisse aus dem Unfall in Fukushima. Dabei wurden insbesondere für die Vorsorge auf der Sicherheitsebene 4 (Notfallmassnahmen) zusätzliche SRLs festgelegt.

Die WENRA SRLs der Issues E und F wurden bei der Erstellung der Richtlinie ENSI-G02 berücksichtigt, sowie weitere SRLs, die Auslegungsvorgaben beinhalten. Die für die Richtlinie ENSI-G02 relevanten WENRA SRLs sind im Anhang 2 zusammen mit deren Abbildung im schweizerischen Regelwerk aufgeführt.

3 Aufbau der Richtlinie

Aufbau und Inhalt der Richtlinie ENSI-G02 orientieren sich am IAEA Safety Standard SSR-2/1 „Safety of Nuclear Power Plants: Design“:

Die ersten drei Kapitel bestehen aus der Einleitung, die für alle ENSI-Richtlinien einheitlich ist, aus den rechtlichen Grundlagen, auf die sich die Richtlinie ENSI-G02 abstützt sowie aus der Darlegung des Gegenstands und Geltungsbereichs sowie. Der Geltungsbereich der ENSI-G02 umfasst die in Betrieb stehenden Kernkraftwerke.

Kapitel 4 umfasst die grundlegenden Konzepte der nuklearen Sicherheit, nämlich das Schutzzielkonzept, das Barrierenkonzept und das Konzept der gestaffelten Sicherheitsvorsorge. Neu wird in der Richtlinie ENSI-G02 die Sicherheitsebene 4 (im Englischen als Design

Extension Conditions, DEC, bezeichnet) in zwei Unterebenen aufgeteilt, in eine Ebene 4a, auf der bestimmte auslegungsüberschreitende Störfälle beherrscht werden müssen, und in eine Ebene 4b, auf der die Auswirkungen von auslegungsüberschreitenden Störfällen mit Kernschmelzen begrenzt werden sollen. Das ENSI bezeichnet Störfälle, die auf der Sicherheitsebene 4 beherrscht oder deren Konsequenzen begrenzt werden, in Übereinstimmung mit der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen (SR 732.112.2) als auslegungsüberschreitende Störfälle.

Kapitel 5 legt konkrete Anforderungen an Schutzzielfunktionen fest.

Kapitel 6 umfasst Auslegungsanforderungen zum Schutz gegen ausgewählte Störfälle.

Kapitel 7 enthält zu den Bereichen Bautechnik, Systemtechnik und Elektrotechnik spezifische Auslegungsanforderungen. Auslegungsanforderungen im Bereich Strahlenschutz sind bereits in mehreren Verordnungen und Richtlinien festgelegt, weshalb darauf in der Richtlinie ENSI-G02 nicht zusätzlich eingegangen wird.

4 Grundsätzliche Erläuterungen

Zum Verständnis der Anforderungen in der Richtlinie ENSI-G02 ist es hilfreich, einige grundsätzliche Aspekte zu erläutern.

4.1 Zum Begriff Auslegung

Der Begriff „Auslegung“ wird in der Richtlinie ENSI-G02 umfassend verstanden. Ausgelegt wird jede SSK (Struktur, System und Komponente). Dies gilt für alle Sicherheitsebenen. Ohne Auslegungsvorgaben, die üblicherweise in Spezifikationen festgelegt sind, kann eine SSK nicht hergestellt werden. Während es auf den Sicherheitsebenen 1 bis 3 grundlegende Auslegungsvorgaben gibt (vgl. Kap. 4 und 5 der Richtlinie), die je nach Sicherheitsebene Redundanz, Diversität, Einzelfehlerauslegung und weitere Kriterien verlangen, gibt es für die Sicherheitsebene 4 diese übergreifenden Auslegungsvorgaben nur begrenzt. Die für die Sicherheitsebene 4 zur Störfallbeherrschung (SE4a) respektive zur Milderung der Störfallkonsequenzen (SE4b) vorgesehenen SSK sind gegen störfallspezifische Belastungen auszulegen. Die störfallspezifischen Belastungen müssen nicht abdeckend sein für alle denkbaren Störfallabläufe, sondern es werden spezifische Belastungen festgeschrieben, die als Auslegungsgrundlage für die SSK in entsprechenden Auslegungsspezifikation festgeschrieben werden. Das Spektrum der zu berücksichtigenden SE4a-Störfälle ist in der Richtlinie ENSI-A01 festgeschrieben.

Die spezifischen Anforderungen für die Sicherheitsebene 4a resultieren aus den in der Richtlinie ENSI-A01 festgelegten auslösenden Ereignissen. Diese Ereignisse umfassen zum einen den Ausfall aller Systeme auf der Sicherheitsebene 3 für eine spezifische Sicherheits-

funktion (z. B. Ausfall der gesamten Wechselstromversorgung, der Reaktorschnellabschaltung oder der sekundärseitigen Nachwärmeabfuhr). Grundsätzlich gilt gemäss Richtlinie ENSI-A01 für die Nachweisführung auf der Sicherheitsebene 4a, dass alle auf dem Anlagenareal noch verfügbaren SSK, eingeschlossen mobile Komponenten, berücksichtigt werden dürfen, wobei deren Verfügbarkeit und Funktionalität nachzuweisen ist.

4.2 Auslegung vs. Nachweis

Für das Verständnis der Anforderungen in der Richtlinie ENSI-G02 ist es entscheidend, zwischen Auslegungsvorgaben und Nachweisvorgaben zu unterscheiden. Die Richtlinie ENSI-G02 ist eine Auslegungsrichtlinie und legt die Anforderungen an Anlageänderungen fest. Diese können sich nur am zum Zeitpunkt der Anlageänderung gültigen Regelwerk (Gesetze, Verordnungen, Richtlinien, Verfügungen) orientieren. Deshalb wird in der Richtlinie ENSI-G02 an mehreren Stellen darauf hingewiesen, dass das zum Zeitpunkt der Errichtung gültige Regelwerk zu berücksichtigen ist. Konkret bezieht sich dies oft auf die zu berücksichtigende Gefährdung durch externe Einwirkungen.

Ändern sich im Laufe der Betriebszeit eines Kernkraftwerks die Gefährdungsannahmen oder das Regelwerk, ist zu überprüfen, ob das Kernkraftwerk auch die geänderten Anforderungen erfüllt. Im Rahmen dieser Überprüfung müssen die zum Zeitpunkt der Überprüfung gültigen Nachweisvorgaben des Regelwerks, namentlich die Richtlinien ENSI-A01, ENSI-A05, ENSI-A06, ENSI-A08 und ENSI-G14 berücksichtigt werden.

Falls die Überprüfung zeigt, dass der Nachweis mit den geänderten Nachweisvorgaben nicht erbracht werden kann, muss das Kernkraftwerk grundsätzlich nachgerüstet werden. Falls ein Kriterium zur Ausserbetriebnahme eines Kernkraftwerks vorliegt, muss das Kernkraftwerk vorläufig ausser Betrieb genommen werden, bis die Nachrüstungen umgesetzt sind (Verordnung des UVEK über die Methodik und die Randbedingungen zur Überprüfung der Kriterien für die vorläufige Ausserbetriebnahme von Kernkraftwerken, SR 732.114.5).

Zum Umfang der Nachrüstungen gemäss Art. 82 KEV für in Betrieb stehende Anlagen wird im erläuternden Bericht zur KEV ausgeführt: „Bezüglich der Nachrüstung bestehender Kernkraftwerke ist auf Art. 22 Abs. 2 Bst. g KEG hinzuweisen, wonach eine bestehende Anlage in dem Umfang nachzurüsten ist, dass sie möglichst weitgehend an den Stand von Wissenschaft und Technik angenähert wird, zumindest soweit, als dies nach der Erfahrung und dem Stand der Nachrüstungstechnik notwendig ist und darüber hinaus, soweit dies zu einer weiteren Verminderung der Gefährdung beiträgt und angemessen ist.“

4.3 Auslegungsgrundsätze und Angemessenheit

Die Grundsätze für die nukleare Sicherheit sind im Kernenergiegesetz im 2. Kapitel (Art. 4 und 5 KEG) übergeordnet festgelegt. Insbesondere wird dabei festgehalten, dass bei der

Auslegung, beim Bau und beim Betrieb Schutzmassnahmen nach international anerkannten Grundsätzen zu treffen sind.

Die Kernenergieverordnung (KEV) führt diese Auslegungsgrundsätze in Art. 7 bis 12 weiter aus, wobei für Anlageänderungen in Kernkraftwerken die Art. 7 bis 10 zentral sind. Art. 10 führt eine Reihe von Auslegungsgrundsätzen auf, die auf internationalen Grundsätzen beruhen. Dazu gehören das Einzelfehlerkriterium (Bst. a), Redundanz und Diversität von Sicherheitsfunktionen (Bst. b), räumliche Trennung von redundanten Strängen von Sicherheitsfunktionen (Bst. d), das 30-Minuten-Kriterium für Eingriffe des Personal (Bst. f). In der KEV wird die Umsetzung dieser Auslegungsgrundsätze selbst für neu zu errichtende Kernkraftwerke nicht absolut gefordert, sondern oftmals nur „soweit möglich“. Damit hat der Verordnungsgeber das Prinzip der Angemessenheit berücksichtigt. In Art. 10 Abs. 2 KEV ist vorgesehen, dass das ENSI spezifische Auslegungsgrundsätze für Leichtwasserreaktoren in Richtlinien zu regeln hat. Damit hat der Gesetzgeber klargestellt, dass zur Umsetzung der Auslegungsgrundsätze gemäss Art. 10 KEV für in Betrieb stehende Kernkraftwerke weitere Ausführungen unter Berücksichtigung der Angemessenheit gemäss Art. 82 KEV notwendig sind. Es ist wichtig zu verstehen, dass die Angemessenheit sich nicht auf die grundlegenden Auslegungsgrundsätze beziehen, sondern auf deren Umsetzung durch technische und organisatorische Massnahmen.

Das ENSI berücksichtigt in der ENSI-G02 drei Stufen der Angemessenheit:

- Stufe 1: Ein Auslegungsgrundsatz muss in jedem Fall umgesetzt werden.
- Stufe 2: Ein Auslegungsgrundsatz ist in der Regel umzusetzen. Abweichungen sind zu begründen und sicherheitstechnisch zu bewerten.
- Stufe 3: Ein Auslegungsgrundsatz ist soweit möglich und angemessen umzusetzen.

Der Antragssteller muss somit Anforderungen gemäss Stufe 1 in jedem Fall umsetzen. Auf Stufe 2 muss er begründen, dass die Sicherheit seiner Anlage auch bei einer Abweichung vom Auslegungsgrundsatz gewährleistet bleibt. Abweichungen kann das ENSI zulassen, wenn die vorgeschlagene Lösung in Bezug auf die nukleare Sicherheit und Sicherung gleichwertig ist. Auf Stufe 3 muss der Antragsteller die Anforderungen umsetzen, es sei denn er kann zeigen, dass der Grundsatz nur mit unverhältnismässig grossem Aufwand umzusetzen wäre und sicherheitstechnisch wenig Gewinn bringen würde.

In jedem Fall muss der Antragsteller dem ENSI aufzeigen, weshalb er eine bestimmte Lösung gewählt hat. Das ENSI wird die vorgeschlagene Lösung eingehend prüfen und bei Bedarf Nachbesserungen verlangen. Der Massstab der Beurteilung durch das ENSI ist dabei Art. 82 KEV.

4.4 Beherrschung von Auslegungsstörfällen

Gemäss Kap. 5.2.2 Bst. e der Richtlinie ENSI-G02 sind Strukturen, Systeme und Komponenten (SSK) für SE3-Funktionen so auszulegen, dass zur Beherrschung von Auslegungsstörfällen in den ersten 10 Stunden grundsätzlich nur SE3-Systemen notwendig sind. Der Einsatz von anderen für die Beherrschung von Auslegungsstörfällen qualifizierter SSK in den ersten 10 Stunden ist zu begründen. Nach 10 Stunden können alle auf der Anlage vorhandenen Mittel zur Störfallbeherrschung benutzt werden. Nach 72 Stunden können auch extern gelagerte Mittel verwendet werden (vgl. Richtlinie ENSI-A01).

Für die langfristige Beherrschung eines Auslegungsstörfalls, insbesondere zum langfristigen Halten der Anlage in einem sicheren Zustand, sind somit auch der Einsatz von SSK, welche nicht zu den Sicherheits- oder Notstandsystemen zählen, oder sicherheitsrelevante Handlungen des Betriebspersonals unter Zuhilfenahme von mobilen Mitteln zulässig, vorausgesetzt die Verfügbarkeit oder Funktionalität der kreditierten SSK ist nachgewiesen und die Handlungen sind in Vorschriften geregelt.

Die Zeitspanne von 10 Stunden stimmt mit der Anforderung überein, dass durch Notstandsysteme ausgeführte SE3-Funktionen mindestens während 10 Stunden autark funktionieren müssen.

Diese Grundsätze zur Beherrschung von Auslegungsstörfällen finden sich auch im IAEA Safety Standard SSR-2/1, Revision 1 (2016) „Safety of Nuclear Power Plants: Design“ wieder:

> *5.11. Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.*
>
> *5.12. Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.*
>
> *5.13. The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.*

5.14. The design shall specify the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control.

5.15. Any equipment that is necessary for actions to be taken in manual response and recovery process shall be placed at the most suitable location to ensure its availability at the time of need and to allow safe access to it under the environmental conditions anticipated.

Gemäss Ziff. 5.12 von SSR-2/1 werden neben der Aktivierung von SE3-Funktionen („manual initiation of systems“) auch andere Betriebshandlungen („other operator actions“) zur Beherrschung von Störfällen für zulässig erklärt, wenn keine unverzügliche und zuverlässige Reaktion („prompt action“) auf das auslösende Störfallereignis gefordert ist und die Zuverlässigkeit der vorbereiteten Handlungen des Betriebspersonals sichergestellt („adequate procedures ensure the performance of such actions“) ist. Ziff. 5.15 enthält präzisierende Vorgaben zur Bereitstellung und Zugänglichkeit der Ausrüstung für manuelle Handlungen im Anforderungsfall und lässt dabei Raum für die Verwendung von mobilen Ausrüstungen zur Störfallbeherrschung.

Die Zulassung von manuellen Handlungen und der Einsatz von mobilen Ausrüstungen zur Beherrschung von Auslegungsstörfällen sind auch mit den WENRA-SRLs vereinbar. Im Vorwort zur SRL-Revision von 2014 wird festgehalten, dass die Referenzniveaus in einer Gesamtschau zu betrachten seien:

> *There are significant interactions between some of the issues and hence each issue should not necessarily be considered self-standing and the RLs need to be considered as a whole set.*

Diese Aussage zur Gesamtschau der WENRA-SRL ist insbesondere wichtig, wenn die Anforderung von E8.3 betrachtet wird. Diese besagt:

> *Only systems that are suitably safety classified can be credited to carry out a safety function. Non safety classified systems shall be assumed to operate only if they aggravate the effect of the initiating event.*

Anderseits enthält der Issue T (Natural Hazards) eine Reihe von Anforderungen zu Beherrschung oder Milderung der Konsequenzen von Naturereignissen. Kapitel 5 von Issue T enthält Auslegungsvorgaben insbesondere im Hinblick auf die Beherrschung der 10 000-jährlichen Ereignisse:

5.1. Protection shall be provided for design basis events. A protection concept shall be established to provide a basis for the design of suitable protection measures.

5.2. The protection concept shall be of sufficient reliability that the fundamental safety functions are conservatively ensured for any direct and credible indirect effects of the design basis event.

5.3. The protection concept shall:

(a) apply reasonable conservatism providing safety margins in the design;

(b) rely primarily on passive measures as far as reasonable practicable;

(c) ensure that measures to cope with a design basis accident remain effective during and following a design basis event;

(d) take into account the predictability and development of the event over the time;

(e) ensure that procedures and means are available to verify the plant condition during and following design basis events;

(f) consider that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and countermeasures;

(g) ensure that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;

(h) not adversely affect the protection against other design basis events (not originating from natural hazards).

5.4. For design basis events, SSCs identified as part of the protection concept with respect to natural hazards shall be considered as important to safety.

5.5. Monitoring and alert processes shall be available to support the protection concept. Where appropriate, thresholds (intervention values) shall be defined to facilitate the timely initiation of protection measures. In addition, thresholds shall be identified to allow the execution of pre-planned post event actions (e.g. inspections).

Im Zentrum dieser Auslegungsvorgaben stehen begrifflich nicht Sicherheits- respektive SE3-Systeme („safety systems“), sondern ein Schutzkonzept („protection concept“). Das Schutzkonzept soll in erster Linie auf passiven Schutzmassnahmen beruhen, soweit dies verhältnismässig ist („reasonable practicable“; vgl. SRL T5.3 Bst. b).

Im Guidance Document zu Issue T (vgl. WENRA, Guidance Document Issue T, Natural Hazards, Head Document, April 2015) wird SRL T5.3 Bst. d wie folgt erläutert:

> *Some, but certainly not all, natural hazards are predictable and may even evolve gradually (e.g., some meteorological hazards). For such hazards, due credit may also be taken from monitoring and alert processes and from additional temporary measures and equipment.*

Das bedeutet, dass nach Ansicht der WENRA bei Naturgefahren, die sich in vorhersehbarer Weise graduell entwickeln, Überwachungs- und Warnprozesse für die Störfallbeherrschung kreditiert werden dürfen. Dasselbe gilt gemäss WENRA für zusätzliche temporäre Mass-

nahmen und Ausrüstungen, die im Anforderungsfall zum Einsatz gelangen. Diese Aussagen im Guidance Document bestätigen den Querbezug zwischen der Berücksichtigung des angenommenen Störfallverlaufs und der Kreditierung von alternativen Schutzmassnahmen anstelle von Sicherheitssystemen zur Störfallbeherrschung. Das ENSI verlangt zudem, dass mobile Komponenten nur dann verwendet werden dürfen, falls diese auf dem Anlagenareal vorhanden sind und an einem geschützten Ort gelagert werden, sodass diese vom spezifischen Naturereignis nicht betroffen werden und somit zur Störfallbeherrschung zur Verfügung stehen. Der Einsatz mobiler Ausrüstungen muss zudem in Störfallvorschriften geregelt sein und es muss ausreichend Zeit für Diagnose und Ausführung der konkreten Massnahme zur Verfügung stehen (Richtlinie ENSI-A01).

Langfristig lässt sich ein Kernkraftwerk, das bei einem Auslegungsstörfall erfolgreich abgeschaltet wurde, nicht über einen unbegrenzten Zeitraum allein mit SE3-Systemen in einem sicheren Zustand halten. Da die externe Stromversorgung nicht sicherheitsklassiert ist, wird sie beim Störfall als ausgefallen unterstellt. Deshalb ist der Betrieb von Notstromgeneratoren für die Störfallbeherrschung erforderlich. Anlageinterne Notstromaggregate gelten bei adäquater Ausgestaltung als Sicherheitssystem. Deren Einsatzdauer ist jedoch abhängig von den vorhandenen Reserven an Kraftstoff (Diesel), mit dem sie betrieben werden. Der Kraftstoff ist nach verhältnismässig kurzer Zeit verbraucht. Spätestens dann ist ein manueller Einsatz (mit mobilem Equipment) erforderlich, um die Kraftstoffbehälter der Notstromaggregate neu zu befüllen. Neben technischen sind somit ebenso organisatorische Schutzmassnahmen zur wirksamen Umsetzung des Konzepts der gestaffelten Sicherheitsvorsorge erforderlich.

Der Einsatz von SSK, welche nicht zu den Sicherheits- oder Notstandsystemen zählen, oder sicherheitsrelevante Handlungen des Betriebspersonals sind somit längerfristig in jedem Fall notwendig. Deren Einsatz 10 Stunden nach Störfalleintritt steht im Einklang mit internationalen Vorgaben. Ein begründeter Einsatz dieser Systeme vor 10 Stunden ist zulässig. Beispiele dafür sind Brandschutzmassnahmen.

Nach 72 Stunden kann zudem externe Unterstützung, insbesondere extern gelagerte Komponenten, berücksichtigt werden, um das Kernkraftwerk langfristig in einem sicheren Zustand zu halten.

5 Erläuterungen zu den einzelnen Kapiteln

5.1 Kapitel 2 „Rechtliche Grundlagen“

Artikel 10 Absatz 2 der Kernenergieverordnung (KEV, SR 732.11) verlangt explizit, dass das ENSI spezifische Auslegungsgrundsätze für Leichtwasserreaktoren in Richtlinien regelt.

Wichtige gesetzliche Grundlagen, auf die sich die Richtlinie ENSI-G02 abstützt, sind:

- Art. 4 und 5 des Kernenergiegesetzes (KEG, SR 732.1) legen die übergeordnete Auslegungsgrundsätze zur nuklearen Sicherheit fest.
- Art. 22 Abs. 2 Bst. g KEG fordert, dass Anlagen soweit nachzurüsten sind, als dies nach der Erfahrung und dem Stand der Nachrüstungstechnik notwendig ist und darüber hinaus, soweit dies zu einer weiteren Verminderung der Gefährdung beiträgt und angemessen ist.
- Art. 7, 8 und 10 der Kernenergieverordnung beinhalten Anforderungen an die nukleare Sicherheit und den Schutz gegen Störfälle sowie Grundsätze für die Auslegung von Kernkraftwerken.
- Art. 82 KEV verlangt, dass der Umfang von Nachrüstungen in Kernkraftwerken, die vor Inkraftsetzung des KEG in Betrieb waren, die Anforderungen gemäss Art. 7 bis 12 KEV nach Massgabe von Art. 22 Abs. 2 Bst. g KEG erfüllen.
- Die Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen (SR 732.112.2) enthält eine Reihe von Gefährdungsannahmen, gegen die Vorsorgemassnahmen zu ergreifen sind. Die Richtlinie ENSI-G02 konkretisiert diese Vorsorgemassnahmen für ausgewählte Störfälle.
- Die Verordnung über sicherheitstechnisch klassierte Behälter und Rohrleitungen in Kernanlagen (VBRK, SR 732.13) regelt die Planung, Herstellung, Montage, Inbetriebsetzung sowie den Betrieb von sicherheitstechnisch klassierten Behältern und Rohrleitungen, deren Abstützungen und druckhaltenden Ausrüstungsteilen für die Verwendung in Kernanlagen.

5.2 Kapitel 3 „Gegenstand und Geltungsbereich“

Die Richtlinie ENSI-G02 ist eine Auslegungsrichtlinie für in Betrieb stehende Kernkraftwerke und legt die bei freigabepflichtigen Anlageänderungen und Sicherheitsüberprüfungen zu berücksichtigenden Auslegungsanforderungen fest. Bei Sicherheitsüberprüfungen ist entsprechend den Vorgaben der Richtlinie ENSI-A03 das übergeordnete Auslegungskonzept der Anlage anhand aller in der Richtlinie ENSI-G02 definierten Auslegungsanforderungen zu bewerten. Bei freigabepflichtigen Anlageänderungen kann in begründeten Fällen auf einen Vergleich mit den in der Richtlinie ENSI-G02 festgelegten Auslegungsanforderungen verzichtet werden.

Beispiele dafür sind im Bereich Elektrotechnik Instandhaltungsmassnahmen, die unter die Richtlinie ENSI-B14 fallen. Im Bereich Maschinentechnik betrifft dies Instandhaltungsmassnahmen, falls die nach ASME-Code BPVC III Appendix T maximal zulässigen Abweichungen zwischen „as built“ und „as analyzed“ gemäss Paragraph T-1210 eingehalten bleiben. In diesem Fall kann der vorhandene Nachweis mit den zum Zeitpunkt der Herstellung von der Auf-

sichtsbehörde akzeptierten Belastungsangaben weiter verwendet werden. Eine Neubewertung mit aktuellen Belastungen ist erforderlich, sobald zulässige „as built“-Abweichungen überschritten sind. Bei Nachweisen, die nicht auf ASME-Code III NB/NC/ND-3600 basieren, kann Paragraph T-1210 sinngemäss angewendet werden.

In Kap. 4.2 wurde dargelegt, dass zwischen Auslegung und Nachweis unterschieden werden muss. Diese Unterscheidung spiegelt sich auch in der vorliegenden Richtlinien mit Ausnahme des Bereichs Bautechnik wider. Jede Baustruktur in einem Kernkraftwerk stellt eine anlagespezifische Lösung dar. Es ist deshalb sinnvoll und notwendig, die sicherheitstechnische Nachweisführung als integraler Bestandteil der Auslegung zu betrachten. Aus diesem Grunde sind in der ENSI-G02 auch entsprechende Anforderungen an die Nachweismethoden eingeflossen.

5.3 Kapitel 4 „Grundlegende Konzepte der nuklearen Sicherheit“

5.3.1 Kapitel 4.1 „Schutzzielkonzept“

Das Ziel der nuklearen Sicherheit ist der Schutz des Menschen und der Umgebung vor den Gefahren radioaktiver Strahlung. Dieser Grundsatz ist in Art. 4 KEG festgehalten. In den IAEA Safety Fundamentals (SF-1, 2006) wird dieser als „fundamental safety objective“ bezeichnet, der bei der Auslegung und beim Betrieb einer Kernanlage als oberster Grundsatz zu beachten ist. Dieses „fundamental safety objective“ entspricht dem übergeordneten Schutzziel S4 „Begrenzung der Strahlenexposition“ gemäss Art. 1 Bst. d der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen (SR 732.112.2).

Bei der Auslegung eines Kernkraftwerks sind die folgenden grundlegenden Schutzziele zu beachten (vgl. auch Requirement 4 des IAEA Safety Standard SSR 2/1):

- S1: Kontrolle der Reaktivität
- S2: Kühlung der Brennelemente
- S3: Einschluss radioaktiver Stoffe

Das Schutzziel S2 umfasst auch die Kühlung der Brennelemente in Lagerbecken.

Bei allen Betriebszuständen und für alle Auslegungsstörfälle sind die Schutzziele S1 bis S4 einzuhalten. Kurzfristige Verletzungen einzelner der grundlegenden Schutzziele sind zulässig, sofern dies nicht zu einer Verletzung des Schutzzieles S4 führt.

Für auslegungsüberschreitende Störfälle, die auf der Sicherheitsebene 4a beherrscht werden und somit nicht zu einem schweren Kernschaden führen, sind die grundlegenden Schutzziele S1 bis S3 einzuhalten, wobei kurzfristige Verletzungen dieser Schutzziele zulässig sind. Solange die Kernkühlung (Schutzziel S2) gewährleistet ist, kann es nicht zu einer

grösseren Freisetzung radioaktiver Stoffe kommen. Da es sich aber um keine Auslegungsstörfälle handelt, ist kein Nachweis der Einhaltung der Störfalldosen gemäss Art. 123 StSV zu erbringen.

Das ENSI legt in der Richtlinie ENSI-A01 fest, welche Störfälle auf der Sicherheitsebene 4a zu beherrschen sind.

5.3.2 Kapitel 4.2 „Barrierenkonzept“

Das Barrierenkonzept ist bereits bei der Auslegung der ersten Kernkraftwerke umgesetzt worden. Es ist 1996 von der International Nuclear Safety Advisory Group der IAEA zusammenfassend beschrieben worden.[1] Das Barrierenkonzept ist ein wichtiges Element zur Einhaltung des Schutzziels „Einschluss radioaktiver Stoffe“. Es ist somit kein von den Schutzzielen unabhängiges Sicherheitskonzept. Das Primärcontainment bekommt insbesondere bei schweren Störfällen eine zentrale Bedeutung als letzte Barriere zur Rückhaltung radioaktiver Stoffe. Bei Undichtheiten des Primärcontainments kann das Sekundärcontainment die Freisetzung radioaktiver Stoffe durch deren teilweise Rückhaltung deutlich reduzieren. Aus diesen Gründen wird das Containment als dritte Barriere bezeichnet.

Das Barrierenkonzept unterscheidet die Barrieren Brennelemente, Primärkreis und Containment. Der mit Abstand grösste Teil radioaktiver Stoffe eines Kernkraftwerks ist im Brennstoff lokalisiert, weshalb die Brennstoffmatrix oftmals auch als erste Barriere gezählt wird (vgl. den oben erwähnten INSAG-Bericht). Für die radioaktiven Edelgase bildet die Brennstoffmatrix allerdings keine Barriere, weshalb sie heute meist nicht als Barriere gezählt wird. Das Barrierenkonzept bildet für diese radioaktiven Stoffe eine gestaffelte Reihe von Barrieren. Es ist das Ziel und die Aufgabe der Reaktorauslegung und des Reaktorbetriebs, durch passive und aktive Massnahmen im Rahmen des Konzepts der gestaffelten Sicherheitsvorsorge die Integrität dieser Barrieren zu gewährleisten.

Im Nicht-Leistungsbetrieb können einzelne Barrieren aufgehoben werden oder nicht zur Verfügung stehen. In diesen Fällen soll durch geeignete Massnahmen, wie beispielsweise die Aufrechterhaltung der Druckstaffelung auch bei offenem Primärcontainment, die Rückhaltung radioaktiver Stoffe gewährleistet werden.

5.3.3 Kapitel 4.3 „Das Konzept der gestaffelten Sicherheitsvorsorge“

Seit der Formulierung des Konzepts der gestaffelten Sicherheitsvorsorge (Defence in Depth) durch die International Nuclear Safety Advisory Group der IAEA[2] hat sich international eingebürgert, die Sicherheitsvorsorge fünf Sicherheitsebenen zuzuordnen. Jede Sicherheitsebene umfasst auf spezifische Anlagezustände ausgerichtete Sicherheitsvorkehrungen mit spezifischen Zielen (vgl. Anhang 2 der Richtlinie ENSI-G02). Das Konzept der gestaffelten Sicherheitsvorsorge besteht somit aus mehreren hintereinander gestaffelten Ebenen von

[1] Defence in Depth in Nuclear Safety, INSAG-10
[2] Defence in Depth in Nuclear Safety, INSAG-10, sowie IAEA Safety Standard SSR-2/1 (Rev. 1)

Vorkehrungen, von denen jeweils die nächste dazu dient, ein Versagen der Vorkehrungen auf der davor liegenden Ebene aufzufangen oder die Konsequenzen des Versagens zu lindern. Die Sicherheitsebenen 1 bis 4 bilden die anlageninterne Sicherheitsvorsorge, die Ebene 5 die anlagenexterne Sicherheitsvorsorge.

Die Unterteilung der Sicherheitsebene 4 in die Sicherheitsebene 4a (auslegungsüberschreitende Störfälle ohne schwere Kernschäden) und die Sicherheitsebene 4b (auslegungsüberschreitende Störfälle mit schwerem Kernschaden) ist als Auslegungsvorgabe neu ins Regelwerk aufgenommen worden. Bereits in der Richtlinie ENSI-A01 wurde eine Auswahl von auslegungsüberschreitenden Störfällen festgelegt. Dabei handelt es sich um Störfälle, die erst auf der Sicherheitsebene 4a abgefangen werden und die ohne schweren Kernschaden zu beherrschen sind. Als solche gelten beispielsweise bestimmte Ereignisse mit Mehrfachfehlern in Sicherheits- oder Notstandsystemen. Als Konsequenz aus dem Unfall in Fukushima wurden in der Richtlinie ENSI-G02 insbesondere die Anforderungen an die Beherrschung externer Ereignisse sowie auslegungsüberschreitender Störfälle präzisiert und verschärft (vgl. Kap. 5.2.3 und 6.3 der Richtlinie ENSI-G02). Die Wirksamkeit der Vorsorgemassnahmen ist durch Störfallanalysen unter den in der Richtlinie ENSI-A01 festgelegten Randbedingungen nachzuweisen.

Auslegungsüberschreitende Störfälle, die zu schweren Kernschäden führen, werden der Sicherheitsebene 4b zugeordnet. Bei diesen Ereignissen ist es das Ziel, die radiologischen Konsequenzen für das Personal und für die Umgebung möglichst gering zu halten. Da die Integrität der ersten beiden Barrieren (Brennelemente und Primärkreis) in der Regel nicht mehr gegeben ist, kommt der Integrität des Containments als letzter Barriere eine zentrale Bedeutung zu.

Das Konzept der gestaffelten Sicherheitsvorsorge ist auch im Nicht-Leistungsbetrieb soweit möglich und angemessen umzusetzen. Im Nicht-Leistungsbetrieb gehören zur Sicherheitsebene 1 beispielsweise die für die Arbeiten im Revisionsstillstand vorgesehenen Systeme und Ausrüstungen. Auch diese sind mit Alarmeinrichtungen ausgerüstet, die rechtzeitig auf ein Abweichen vom Normalbetrieb hinweisen. Die Gegenmassnahmen werden dann mehrheitlich durch Operateureingriffe initiiert und seltener durch Begrenzungssysteme. Auf der Sicherheitsebene 3 wirken die Sicherheits- und Notstandsysteme wie im Leistungsbetrieb, wobei einige Systeme wegen Instandhaltung ausser Betrieb sein können. Das Einzelfehlerkriterium ist auch im Nicht-Leistungsbetrieb einzuhalten.

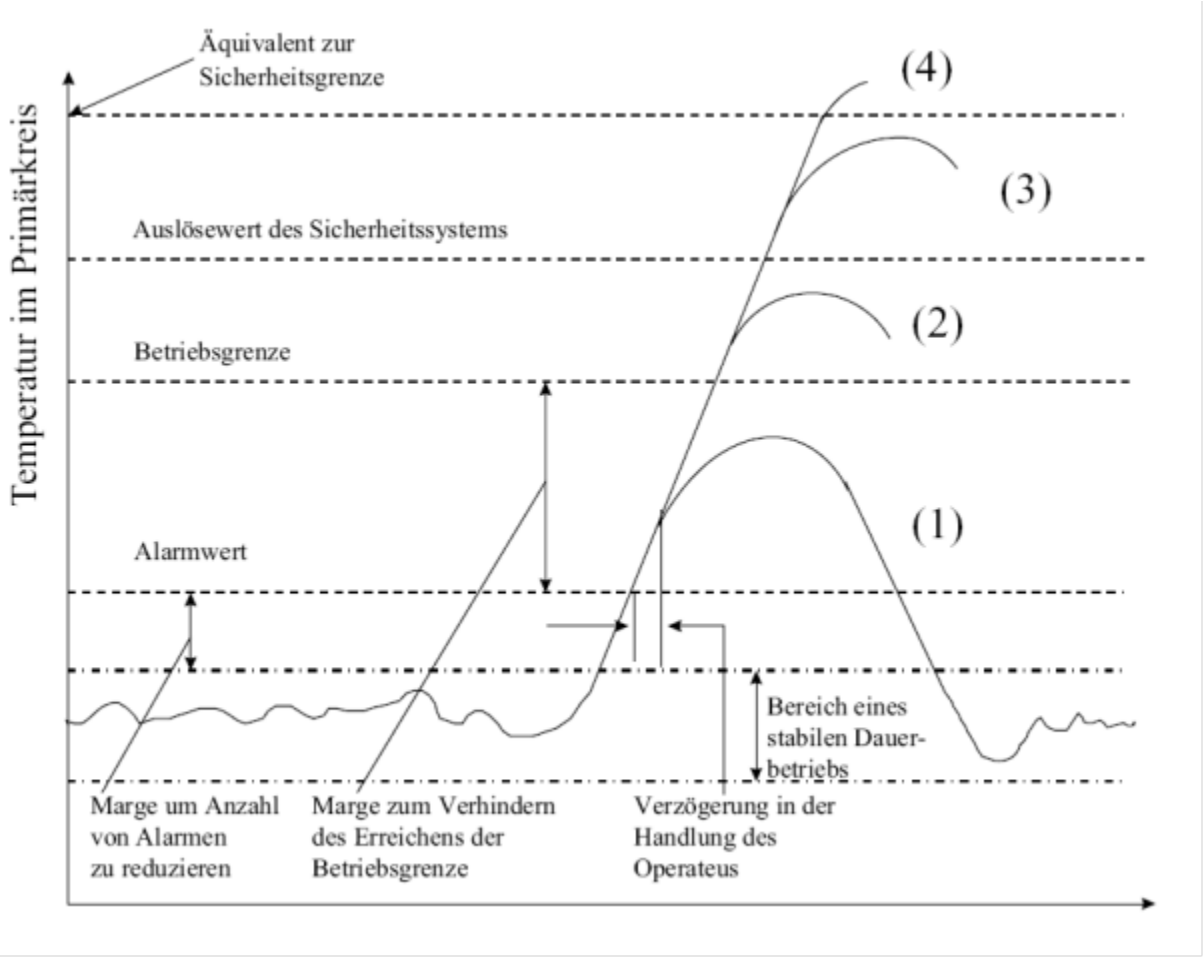
Die Gewährleistung einer guten Sicherheitskultur ist ein wichtiges schutzzielübergreifendes Element der gestaffelten Sicherheitsvorsorge. Das ENSI hat in seinem Bericht „Aufsicht über die Sicherheitskultur von Kernanlagen“ (Ausgabe Dezember 2016[3]) dargelegt, welche Elemente zu einer guten Sicherheitskultur beitragen.

Zu Kap. 4.3 Bst. d Ziff. 1: Qualitätssichernde Massnahmen für Behälter und Rohrleitungen (BRK) sind in der Richtlinie ENSI-G11 geregelt.

[3] https://www.ensi.ch/wp-content/uploads/sites/2/2017/01/ENSI-Bericht-Aufsicht_Sicherheitskultur_Ausg_2_DE.pdf

Zu Kap. 4.3 Bst. d Ziff. 2: Massnahmen zur Gewährleistung einer guten Sicherheitskultur sind in der Richtlinie ENSI-G07 und der Verordnung über die Anforderungen an das Personal von Kernanlagen (VAPK) geregelt.

Zu Kap. 4.3 Bst. e: Die Staffelung sicherheitsrelevanter Grössen kann in Anlehnung an den IAEA Safety Guide DS497a (Draft), Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, 2021, erfolgen. Am Beispiel der Temperatur im Primärkreis eines Kernkraftwerks ist die dort beschriebene Staffelung sicherheitsrelevanter Grössen nachfolgend beispielhaft dargestellt.



Temperaturverlauf bei Überschreitung eines Alarmwerts (Kurve 1)

Die überwachten Parameter können den Bereich des stabilen Dauerbetriebs beispielsweise auf Grund von Laständerungen oder einer Störung im Regelsystem verlassen. Steigt die Temperatur an und erreicht den Alarmwert, wird der Operateur alarmiert. Er wird Massnahmen veranlassen, die das Regelsystem unterstützen, die Temperatur wieder in den Bereich des stabilen Dauerbetriebs zurückzuführen. Dadurch wird ein Verletzen der Betriebsgrenze vermieden. Eine verzögerte Reaktion des Operateurs ist dabei zu berücksichtigen.

Temperaturverlauf bei Überschreitung einer Betriebsgrenze (Kurve 2)

Die Betriebsgrenzen sind unter Berücksichtigung der Ergebnisse aus den Sicherheitsanalysen im Bereich zwischen der Grenze eines stabilen Dauerbetriebs und dem Auslösewert des Sicherheitssystems festzulegen. Normalerweise besteht ein Abstand zwischen dem Alarmwert und der Betriebsgrenze, um im Normalbetrieb auftretende Schwankungen zu berücksichtigen. Häufig ist auch ein Abstand zwischen der Betriebsgrenze und dem Auslösewert des Sicherheitssystems vorhanden, um dem Operateur eine Eingriffsmöglichkeit zur Beherrschung einer Transiente zu bieten ohne dass das Sicherheitssystem ausgelöst wird. Wird eine Betriebsgrenze erreicht und der Operateur ist in der Lage, durch einen Eingriff das Auslösen des Sicherheitssystems zu vermeiden, wird die Transiente einen Verlauf wie in der Kurve 2 dargestellt, nehmen.

Temperaturverlauf bei Überschreitung eines Auslösewerts des Sicherheitssystems (Kurve 3)

Ein überwachter Parameter kann auf Grund einer Störung des Regelsystems, eines Operateurfehlers oder aus anderen Gründen den Auslösewert des Sicherheitssystems erreichen. Dadurch wird das Sicherheitssystem ausgelöst. Die vom Sicherheitssystem ausgelöste Reaktion sollte ausreichen, ein Erreichen der Sicherheitsgrenze zu verhindern.

Temperaturverlauf bei Überschreitung einer Sicherheitsgrenze (Kurve 4)

Für den Fall einer auslegungsüberschreitenden Störung oder eines Mehrfachversagens von Sicherheitssystemen kann ein Überschreiten der Sicherheitsgrenze nicht ausgeschlossen werden. Weitere Sicherheitssysteme sollen durch andere Parameter aktiviert werden, um die Konsequenzen aus dem Überschreiten der Sicherheitsgrenzen zu lindern. Hierbei werden bedarfsweise auch Accident-Management-Massnahmen eingesetzt.

5.4 Kapitel 5 „Anforderungen an Schutzzielfunktionen“

Schutzzielfunktionen sind Funktionen, die zur Einhaltung der Schutzziele erforderlich sind. Diese Funktionen werden in der Regel durch unterschiedliche Vorsorgemassnahmen auf den Sicherheitsebenen 1 bis 4 sichergestellt (vgl. Anhang 2 der ENSI-G02). In einzelnen Fällen wurden für die Sicherheitsebene 4b auch spezifische Funktionen zum Erhalt der Containmentintegrität definiert. Die Gliederung der vier Schutzziele S1 bis S4 in Schutzzielfunktionen ist international nicht einheitlich geregelt und bis zu einem gewissen Grad reaktorspezifisch. Schutzzielfunktionen auf der Sicherheitsebene 3 werden in der Kernenergieverordnung als Sicherheitsfunktionen bezeichnet, in der ENSI-G02 als SE3-Funktionen, die ihrerseits durch Sicherheits- oder Notstandsysteme ausgeführt sind. In der ENSI-G02 werden Anforderungen an Strukturen, Systeme und Komponenten (SSK) für alle Sicherheitsebenen festgeschrieben. Bisher wurden im schweizerischen Regelwerk Anforderungen primär an SSK der Sicherheitsebene 3 gestellt.

Schutzzielfunktionen können durch Konstruktionsmerkmale, inhärente Eigenschaften, passive und aktive Massnahmen realisiert sein und zwar für alle Anlagezustände, also für den Normalbetrieb, Betriebsstörungen, Auslegungsstörfälle und auslegungsüberschreitende Störfälle.

Zur Überwachung, Regelung und Aktivierung von Schutzzielfunktionen sind entsprechende Mess-, Begrenzungs-, Alarm- und Auslösesysteme notwendig. Das ENSI behandelt die Überwachung, Regelung und Aktivierung von Schutzzielfunktionen nicht als separate Schutzzielfunktionen.

Ergänzend zu den Schutzzielfunktionen sind auch schutzzielübergreifende Aufgaben und Prozesse notwendig, um die Schutzziele einzuhalten. Dazu gehören insbesondere qualitätssichernde Massnahmen und Massnahmen zur Sicherheitskultur. Diese Massnahmen wirken auf allen Sicherheitsebenen und können nicht spezifisch einzelnen Ebenen zugeordnet werden.

Beispiele von Schutzzielfunktionen sind im Anhang 1 aufgeführt. Im Anhang des Erläuterungsberichts zur Richtlinie ENSI-G08 sind weitere Beispiele aufgeführt.

Wichtige Anforderungen an Schutzzielfunktionen auf der Sicherheitsebene 3 (SE3-Funktionen) sind bereits in der KEV festgeschrieben. Dies sind insbesondere die Grundsätze der nuklearen Sicherheit in den Art. 7 bis 10 KEV, die formal nur für neu zu errichtende Kernkraftwerke gelten. Für in Betrieb stehende Kernkraftwerke gelten diese Grundsätze unter Berücksichtigung von Art. 22 Abs. 2 Bst. g KEG, das heisst unter Beachtung des Standes der Nachrüstungstechnik und der Erfahrung und darüber hinaus, soweit dies zu einer weiteren Verminderung der Gefährdung beiträgt und angemessen ist. Ausgehend von den in der KEV festgelegten Grundsätzen der nuklearen Sicherheit sind in der ENSI-G02 die für in Betrieb stehenden Kernkraftwerke anzuwendenden Auslegungsanforderungen an SE3-Funktionen sowie auch an SE1-, SE2- und SE4-Funktionen festgelegt. Dabei werden die spezifisch schweizerischen sowie internationalen Erfahrungen berücksichtigt.

Die in Betrieb stehenden schweizerischen Kernkraftwerke verfügen alle über Notstandsysteme. Notstandsysteme stellen primär einen Schutz gegen extreme äussere Einwirkungen und unbefugte Einwirkungen dar. Sie ermöglichen zudem auch beim Verlust des Hauptkommandoraums ein sicheres Abfahren der Anlage und die Abfuhr der Nachzerfallswärme. Für die Kernkraftwerke Gösgen und Leibstadt wurden diese bereits beim Bau realisiert, bei den Kernkraftwerken Beznau und Mühleberg wurden sie nachgerüstet. Entsprechende Nachrüstforderungen wurden von der Aufsichtsbehörde bereits anfangs der 1980er Jahre formuliert. In den Kernkraftwerken Beznau und Mühleberg wurden mit den Notstandsystemen zudem die bisherigen SE3-Funktionen verbessert, insbesondere durch die Erhöhung des Redundanzgrades.

5.4.1 Kapitel 5.1 „Allgemeine Anforderungen“

Schutzzielfunktionen werden durch Strukturen, Systeme und Komponenten (SSK) umgesetzt, an die hohe Qualitätsanforderungen gestellt werden.

Die grundlegenden Anforderungen sind vor allem Präzisierungen entsprechender gesetzlicher Anforderungen der KEV und spiegeln die heutigen Anforderungen an die Qualität sicherheitsrelevanter Anlageteile wider. Mit der Forderung nach ausreichenden Sicherheitszuschlägen für SSK wird die Robustheit der gestaffelten Sicherheitsvorsorge gestärkt, sodass das Ansprechen von Systemen der nachfolgenden Sicherheitsebene möglichst verhindert wird.

Zu Bst. a: Werden SSK auf mehreren Sicherheitsebenen eingesetzt, haben diese die entsprechenden Anforderungen für alle diese Sicherheitsebenen zu erfüllen. In der Praxis trifft dies insbesondere für SSK der Sicherheitsebenen 1 und 2 zu. So muss beispielsweise ein Regelsystem, das auch als Begrenzungssystem wirkt, die Auslegungsanforderungen der Sicherheitsebenen 1 und 2 erfüllen. Auch SSK der Sicherheitsebene 3 werden gezielt auf der Sicherheitsebene 4a eingesetzt. In begründeten Fällen können für die langfristige Sicherstellung der Nachwärmeabfuhr SSK der Sicherheitsebene 4a auch auf der Sicherheitsebene 3 eingesetzt werden, ohne dass diese alle Anforderungen der Sicherheitsebene 3 erfüllen.

Zu Bst. c: Die Auslegung, Fertigung und Montage von SSK muss den spezifischen Anforderungen der Kerntechnik betreffend Qualität und Qualitätssicherung genügen. Werden industrielle Komponenten verwendet, sind entsprechende Qualitätssicherungs- und Qualifizierungsnachweise beizubringen. Für mechanische Komponenten (BRK) sind die entsprechenden Qualitätsanforderungen in der Richtlinie ENSI-G11 geregelt.

Zu Bst. d: Durch geeignete Werkstoffwahl, insbesondere von Komponenten die mit Kühlmittel des Primärkreislaufs in Kontakt kommen oder sich in erhöhtem Strahlenfeld befinden, soll die Aktivierung dieser Komponenten möglichst begrenzt bleiben. Damit wird die Instandhaltung solcher Komponenten erleichtert.

Zu Bst. g: Komponenten, die gemäss anerkannten Normen oder Prüfnormen gefertigt und geprüft beziehungsweise über eine entsprechende Zulassungen verfügen, gelten als umfassend geprüft.

5.4.2 Kapitel 5.2 „Auslegungsanforderungen für die verschiedenen Sicherheitsebenen“

Ergänzend zu den grundlegenden Anforderungen an Schutzzielfunktionen haben die SSK auf den Sicherheitsebenen 1 bis 4 (SE1- bis SE4-Funktionen) spezifische Auslegungsanforderungen zu erfüllen. Basis für diese Anforderungen sind die in Art. 10 KEV festgelegten Grundsätze für die Auslegung von Kernkraftwerken, die sinngemäss auf die einzelnen Sicherheitsebenen übertragen wurden.

Weitere spezifische Anforderungen an SSK sind Gegenstand fachspezifischer ENSI-Richtlinien.

5.4.2.1 Kapitel 5.2.1 „SE1- und SE2-Funktionen“

Zu Bst. a: Es sind SE1- und SE2-Funktionen so umfassend vorzusehen und mit hoher Qualität auszuführen, dass Abweichungen vom Normalbetrieb selten sind (hohe Zuverlässigkeit der SE1-Funktionen). Treten Abweichungen auf, sollen diese wenn immer möglich durch Alarm- und Meldesysteme mit anschliessenden Operateurhandlungen oder durch Begrenzungssysteme (SE2-Funktionen) aufgefangen und die Anlage wieder in den Normalbetrieb zurückgeführt werden. Das Ansprechen von Sicherheits- oder Notstandsystemen soll dadurch möglichst selten notwendig werden.

Zu Bst. c: Zu den Operateureingriffen im Rahmen des Normalbetriebes gehören auch Handlungen als Folge von Alarmen. Werden diese nicht ausgeführt oder sind sie nicht wirksam, greift die automatische Begrenzungsfunktion auf der Sicherheitsebene 2. Diese soll soweit wie möglich und angemessen automatisch erfolgen.

5.4.2.2 Kapitel 5.2.2 „SE3-Funktionen“

Art. 10 KEV legt die grundsätzlichen Vorgaben für SE3-Funktionen (in der KEV als Sicherheitsfunktionen bezeichnet) bereits fest, wie sie für neu zu errichtende Kernkraftwerke umzusetzen wären. Die Richtlinie ENSI-G02 präzisiert diese grundsätzlichen Vorgaben für in Betrieb stehende Kernkraftwerke unter Beachtung der Verhältnismässigkeit. Diese Präzisierungen leiten sich vor allem aus der bisherigen Richtlinie HSK-R-101 sowie aus IAEA Safety Standards ab, insbesondere des IAEA Safety Standard SSR-2/1.

Zu Bst. a: SE3-Funktionen werden in den Schweizer Kernkraftwerken durch Sicherheitssysteme und gegen externe Einwirkungen besonders geschützte Notstandsysteme realisiert. Weitere Ausführungen finden sich in Kapitel 4.4 dieses Erläuterungsberichts.

Zu Bst. c: Eine ausreichende Vorsorge gegen den Ausfall von SSK aufgrund einer gemeinsamen Ursache kann insbesondere Diversität sowie eine Test-, Instandhaltungs- und Betriebsstrategie beinhalten.

Zu Bst. d: Notstandsysteme müssen während 10 Stunden autark funktionieren. Diesem Auslegungsgrundsatz liegt die Annahme zugrunde, dass aktive Eingriffe und die Überwachung der Anlage vom Hauptkommandoraum nicht mehr möglich sind. Ausser zum Starten der Notstandsysteme sollen deshalb für deren weiteren Betrieb keine Operateureingriffe mehr notwendig sein.

Zu Bst. e: Die Basis dieser Anforderung ist in Kapitel 4.4 dieses Erläuterungsberichts dargelegt und widerspiegelt die Vorgaben für technische Sicherheitsanalysen gemäss Richtlinie ENSI-A01. Spezifische Auslegungsstörfälle sind beispielsweise Brände oder Überflutungen.

Zu Bst. f: SE3-Funktionen sind unter anderem gegen das Sicherheitserdbeben (SSE) auszulegen. Als Auslegungsgrundlage gilt dabei das zum Zeitpunkt des Baus oder der Anlageän-

derung von den Aufsichtsbehörden akzeptierte SSE. Die Basis für diese Anforderung ist in Kapitel 4.2 des vorliegenden Erläuterungsberichts dargelegt. Es ist zu beachten, dass die durch äussere Einwirkungen bedingten Gefährdungen standortspezifisch sind und deshalb keine für alle Standorte gleichen Gefährdungsannahmen festgelegt werden können.

Zu Bst. h: Die gemeinsame Nutzung elektrischer oder mechanischer Komponenten für SE3-Funktionen bei Mehrblockanlagen ist nur zulässig, wenn die Sicherheit der einzelnen Blöcke nicht beeinträchtigt und insgesamt erhöht wird.

Zu Kap. 5.2.2.1 Bst. a: Eine SE3-Funktion kann durch mehrere Systeme wahrgenommen werden. Ein vom auslösenden Ereignis unabhängiger Einzelfehler darf aber die SE3-Funktion nicht beeinträchtigen, zum Beispiel muss die Notkühlung weiterhin wirksam bleiben, auch wenn ein Einzelfehler in der Funktion (in einem zur Funktion gehörenden System) unterstellt wird.

Zu Kap. 5.2.2.1 Bst. b: Bei passiven Komponenten sind neben der nachweislich geforderten hohen Qualität deren Zuverlässigkeit aufgrund der Betriebserfahrung zu beachten. Als passiv gelten Gebäude und solche Komponenten, die keine bewegten Teile zur Erfüllung ihrer Sicherheitsfunktion benötigen. Beispielsweise gilt eine Rückschlagklappe dann als passive Komponente, wenn sie im Störfallablauf nicht bewegt werden muss.

Zu Kap. 5.2.2.1 Bst. c: Das Einzelfehlerkriterium ist für SE3-Funktionen einzuhalten, insbesondere auch bei Instandhaltungsarbeiten. Abweichungen sind nur zulässig, falls dies zu keiner bedeutenden Reduktion der Sicherheit führt. Konkret bedeutet dies, dass solche Zustände nur für beschränkte Zeiten zulässig sind, beispielsweise zur Instandsetzung einer defekten Komponente. Die maximal zulässigen Zeiten sind in der Technischen Spezifikation festgehalten.

Zu Kap. 5.2.2.2 Bst. a: Die Diversität soll vor allem zwischen Sicherheits- und Notstandsystemen umgesetzt werden.

Zu Kap. 5.2.2.2 Bst. b: Die Redundanzanforderung wird für bestehende Kernkraftwerke für aktive Komponenten umgesetzt, nicht aber durchgängig für passive Komponenten. Gewisse Rohrleitungen können für zwei oder drei redundante Stränge gemeinsam benutzt werden. Bei Anlageänderungen sollte die Redundanz wenn immer angemessen und möglich auch auf passive Komponenten angewendet werden.

Zu Kap. 5.2.2.3 Bst. c: Mit der Anforderung, dass Sicherheits- und Notstandsystemen soweit möglich funktional voneinander unabhängig sein müssen, wird die Sicherheit des Kernkraftwerks deutlich verbessert. Insbesondere zur Beherrschung systemübergreifender interner und externer Einwirkungen ist diese Auslegung der SE3-Funktionen von Nutzen und das Risiko der Kernkraftwerke wird dadurch deutlich reduziert.

Zu Kap. 5.2.2.4: Geeignete Massnahmen zur räumlichen Trennung sind vor allem die Unterbringung der einzelnen Stränge von Sicherheits- und Notstandsystemen in verschiedenen Räumen. Es ist aber auch eine Trennung durch eingezogene Trennwände im selben Raum oder ein ausreichender Abstand der Komponenten möglich.

Zu Kap. 5.2.2.5 Bst. b: Bei Prüfarbeiten an einem SE3-System darf die zugehörige SE3-Funktion nicht beeinträchtigt werden oder sie muss im Anforderungsfall innerhalb so kurzer Zeit wirksam sein, dass sie zur Störfallbeherrschung verfügbar ist. Dies gilt auch bei Unterstellung eines unabhängigen Einzelfehlers.

Zu Kap. 5.2.2.6 Bst. b: Zu automatisieren sind auch SE3-Funktionen, die erst nach 30 Minuten benötigt werden und für die keine ausreichende Diagnosezeit zur Verfügung steht. Ausreichend bedeutet in der Praxis, dass dem Personal ein Mehrfaches der Zeit zur Verfügung steht, die zur Diagnose und Durchführung der Inbetriebnahme der SE3-Funktion notwendig ist. Ist dies gegeben, ist eine Automatisierung nicht zwingend.

5.4.2.3 Kapitel 5.2.3 „SE4-Funktionen“

Mit SE4a-Funktionen sollen bestimmte auslegungsüberschreitende Störfälle ohne schweren Kernschaden beherrscht werden. Hierfür sind unter Umständen Systeme erforderlich, die eine hohe Robustheit gegen externe Ereignisse aufweisen und soweit möglich unabhängig von den aktiven Sicherheits- und Notstandsystemen betrieben werden können. Oft handelt es sich hier um Notfallausrüstungen, deren Inbetriebnahme Handmassnahmen vor Ort erfordert.

Ziel der SE4b-Funktionen ist eine Linderung der Konsequenzen auslegungsüberschreitender Störfälle mit schwerem Kernschaden. Zentral ist dabei insbesondere die Aufrechterhaltung der Containmentintegrität. Dazu sind fest installierte und mobile Notfallausrüstungen bereitzustellen, die unter den bei einem schweren Unfall herrschenden Randbedingungen noch zuverlässig funktionieren.

Es sind auslegungsüberschreitende Störfallabläufe denkbar, bei denen das Containment seine Integrität sehr früh verliert (sogenannte Containment-Bypass-Sequenzen). Bei diesen Störfallsequenzen wird versucht, die Containmentintegrität so schnell wie möglich wieder herzustellen oder die Freisetzung radioaktiver Stoffe mit anderen Mitteln möglichst zu begrenzen. Ergänzend wird versucht, durch externe Notfallschutzmassnahmen (Massnahmen auf der Sicherheitsebene 5) die radiologischen Konsequenzen für die Umgebung, vor allem für die Bevölkerung, möglichst gering zu halten.

Ein Beispiel einer fest installierten Notfallausrüstung ist die gefilterte Druckentlastung des Primärcontainments. Beispiele für mobile Notfallausrüstungen sind Feuerwehrpumpen und mobile Dieselgeneratoren, die seit der Katastrophe in Fukushima in allen schweizerischen Kernkraftwerken vorhanden sind.

Zu Kap. 5.2.3 Bst. c: Dies betrifft diejenigen Orte, an denen Ausrüstungen zur Beherrschung respektive Milderung des spezifischen Störfalls bedient werden müssen.

Zu Kap. 5.2.3 Bst. e: Notfallausrüstungen müssen vom Eigenpersonal in Betrieb genommen werden können. Ausrüstungen, die möglicherweise bereits in den ersten Stunden in Betrieb genommen werden müssen, sind somit vom Betriebspersonal auf der Anlage zu bedienen. Das Betriebspersonal ist folglich entsprechend auszubilden. Notfallausrüstungen, die erst 72

Stunden nach dem auslösenden Ereignis in Betrieb genommen werden müssen, können auch durch externes Fachpersonal bedient werden.

Zu Kap. 5.2.3 Bst. f: Zum Betrieb von Notfallausrüstungen sind oft Versorgungsfunktionen wie Strom- und Steuerluftversorgung notwendig. Deren Verfügbarkeit im Notfall ist somit entscheidend zur Beherrschung oder Linderung von Notfällen.

Zu Kap. 5.2.3.1 Bst. a: Jede Komponente einer SE4-Funktion muss eine Reihe von Anforderungen erfüllen. Bei der Auslegung dieser Komponenten müssen diese Anforderungen berücksichtigt werden. SSK der Sicherheitsebene 4 sollen ihrem Verwendungszweck entsprechend auch schwere interne und externe Auswirkungen überstehen, da sie gerade zur Beherrschung solcher Ereignisse oder zur Linderung deren Auswirkungen eingesetzt werden.

Zu Kap. 5.2.3.1 Bst. b: Spezifische Notfallausrüstungen und Systeme, die erst auf der Sicherheitsebene 4a benötigt werden, sollen gegenüber den Sicherheits- und Notstandsystemen diversitär ausgelegt sein. Werden solche spezifischen Notfallausrüstungen und Systeme benötigt, muss davon ausgegangen werden, dass die vorgelagerten Systeme der gestaffelten Sicherheitsvorsorge zumindest teilweise versagt haben. Es ist deshalb sinnvoll, diese spezifischen Notfallausrüstungen und Systeme nach anderen Funktionsprinzipien auszuführen und diese sollten unabhängig von denjenigen der Sicherheits- und Notstandsystemen sein.

Zu Kap. 5.2.3.1 Bst. c: Da davon ausgegangen werden muss, dass die SE3- und SE4a-Funktionen versagten, ist es sinnvoll, die SE4b-Ausrüstungen diversitär und funktional unabhängig zu den Ausrüstungen der SE3- und SE4a-Funktionen aufzubauen.

Zu Kap. 5.2.3.1 Bst. d: SE4b-Funktionen sollten zudem wenn immer möglich ohne Versorgungssysteme auskommen, da letztere bei einem schweren Unfall kaum verfügbar sind. Deshalb sollten die SE4b-Ausrüstungen möglichst auf passiv wirkenden Funktionsweisen beruhen.

Zu Kap. 5.2.3.2: Bst. a: Mobile Notfallausrüstungen sind so zu lagern, dass sie auch extreme äussere Einwirkungen ohne Schaden überstehen, so dass ihre Funktionsfähigkeit gewahrt bleibt. Als Basis gelten die zum Zeitpunkt der Errichtung der Notfallausrüstungen von der Aufsichtsbehörde akzeptierten Gefährdungsannahmen.

Zu Kap. 5.2.3.2 Bst. f: Diese Anforderung ist eine Konsequenz aus der Katastrophe in Fukushima. Es ist entscheidend, dass vor Ort alle vorhandenen Wasservorräte im Notfall zur Kühlung des Reaktorkerns und der Brennelemente in den Lagerbecken verwendet werden können.

Zu Kap. 5.2.3.2 Bst. g: Bei Mehrblockanlagen sind ausreichend Notfallausrüstungen bereitzustellen, damit insbesondere bei blockübergreifenden Ereignissen wie Erdbeben oder Überflutung Eingriffe bei allen betroffenen Blöcken möglich sind. Bei einem Kernkraftwerk muss in jedem Fall auch die ausreichende Kühlung der Brennelemente in den Lagerbecken sichergestellt werden. Auch dafür sind die entsprechenden Notfallausrüstungen bereitzustellen.

5.5 Kapitel 6 „Auslegungsanforderungen zum Schutz gegen Störfälle“

5.5.1 Kapitel 6.1 „Allgemeine Anforderungen“

Ein Kernkraftwerks muss so ausgelegt sein, dass Störfälle, die nach der Erfahrung während der Lebensdauer zu erwarten oder nach menschlichem Ermessen nicht auszuschliessen sind, so beherrscht werden, dass sie keine schwerwiegenden Auswirkungen in der Umgebung haben. Diese Ereignisse werden unter dem Sammelbegriff Auslegungsstörfälle zusammengefasst. Zudem wird heute für die in Betrieb stehenden Kernkraftwerke verlangt, dass auch bestimmte auslegungsüberschreitende Störfälle ohne Kernschmelzen auf der Sicherheitsebene 4a beherrscht werden.

Das Vorgehen zur Festlegung der Gefährdungsannahmen und des zu betrachtenden Störfallspektrums richten sich nach der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen (SR 732.112.2) und den Richtlinien ENSI-A01 und ENSI-A05.

Für ausgewählte Störfallszenarien, insbesondere für sogenannte systemübergreifende Einwirkungen von innen und aussen, werden in der Richtlinie ENSI-G02 Vorgaben für zu ergreifende Vorsorgemassnahmen gemacht. Diese Vorgaben sind zum Teil neu (z. B. für interne und externe Überflutung, Absturz schwerer Lasten oder Blitzeinwirkungen) und sind bisher im schweizerischen Regelwerk nicht festgeschrieben worden. Bisher hat das ENSI fallspezifisch Vorgaben gemacht. Mit der einheitlichen Regelung in der Richtlinie ENSI-G02 soll gewährleistet werden, dass die Auswirkungen dieser Ereignisse so begrenzt werden, dass mindestens die zu deren Beherrschung erforderlichen Sicherheits- und Notstandstränge sowie weitere, störfallspezifisch qualifizierte Ausrüstungen noch verfügbar sind. Ebenso sind die Auslegungsvorgaben des Strahlenschutzes bei der Umsetzung der Vorsorgemassnahmen so zu berücksichtigen, dass notwendige Eingriffe des Personals vor Ort ohne unzulässige Strahlenbelastung ausgeführt werden können und die potentielle Belastung der Bevölkerung begrenzt bleibt.

5.5.2 Kapitel 6.2 „Intern ausgelöste Störfälle“[4]

Ein Kernkraftwerk muss eine Reihe von intern ausgelösten Ereignissen ohne Kernschaden beherrschen. Das Spektrum der zu beherrschenden Störfälle muss mindestens die in Art. 8 Abs. 2 KEV und in der Richtlinie ENSI-A01 aufgeführten Ereignisse abdecken und die störfallspezifischen Gefährdungsannahmen gemäss Art. 4 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen berücksichtigen.

[4] geändert am 1. Oktober 2024 aufgrund der Richtlinie ENSI-G18

Die in den Kapiteln 6.2.1 bis 6.2.4 festgeschriebenen Vorsorgemassnahmen sind in jedem Fall umzusetzen. Diese zielen darauf ab, das Auftreten dieser Ereignisse möglichst zu verhindern und falls dies nicht gelingt, die Auswirkungen auf sicherheitsrelevante Anlagenbereiche durch bauliche, technische und organisatorische Massnahmen zu begrenzen. Darüber hinaus hat der Bewilligungsinhaber weitere Vorsorgemassnahmen zu treffen, wenn sich solche als angemessen erweisen.

Zu Kap. 6.2.3 Bst. c Ziff. 1 ist zu bemerken, dass potenzielle Quellen für Bruchstücke sinnvoll zu bestimmen sind. Ein Bruch des Reaktordruckbehälters oder von Dampferzeugern wird international aufgrund höchster Qualitätsanforderungen und der erforderlichen Überprüfungen nicht unterstellt.

5.5.3 Kapitel 6.3 „Extern ausgelöste Störfälle“

Ein Kernkraftwerk muss eine Reihe von extern ausgelösten Ereignissen ohne Kernschaden beherrschen. Das Spektrum der zu beherrschenden Störfälle muss mindestens die in Art. 8 Abs. 3 KEV und in der Richtlinie ENSI-A01 aufgeführten Ereignisse abdecken und die störfallspezifischen Gefährdungsannahmen gemäss Art. 5 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen berücksichtigen.

Die in den Kapiteln 6.3.1 bis 6.3.5 festgeschriebenen Vorsorgemassnahmen sind in jedem Fall umzusetzen. Darüber hinaus hat der Bewilligungsinhaber weitere Vorsorgemassnahmen zu treffen, wenn sich solche als angemessen erweisen.

Für die Auslegung der Kernkraftwerke gegen einen Flugzeugabsturz gelten weiterhin die Anforderungen gemäss Richtlinie HSK-R-102.

5.5.3.1 Kapitel 6.3.1 „Erdbeben“

Zu Bst. a und b: Kernkraftwerke sind grundsätzlich gegen die Einwirkungen von Erdbeben ausgelegt. International wird als Auslegungserdbeben das Sicherheitserdbeben (SSE) berücksichtigt. Die Festlegung des Sicherheitserdbebens ist international nicht einheitlich und vor allem in der Methodik zur Bestimmung der Erdbebengefährdung sind unterschiedliche Ansätze festzustellen. In der Schweiz wurden die Kernanlagen gegen das zum Zeitpunkt der Baubewilligung festgelegte Sicherheitserdbeben mit einer Überschreitenshäufigkeit von 10^{-4} pro Jahr ausgelegt. Die der Auslegung ursprünglich zugrunde gelegten Erdbebengefährdungsannahmen, unter anderem die frequenzabhängigen Bodenbeschleunigungen, mussten im Laufe der Zeit infolge neuer Erkenntnisse höher angesetzt werden.

Die gegen Erdbebeneinwirkungen auszulegenden SSK sind über die sicherheitstechnische Klassierung gemäss Richtlinie ENSI-G01 festgelegt.

Zu Bst. c und d: BK-II und EK-II-klassierte SSK sind gegen die zum Zeitpunkt ihrer Errichtung von den Aufsichtsbehörden akzeptierten Belastungen durch das Betriebserdbeben (OBE) auszulegen. In jedem Fall ist aber nachzuweisen, dass die Anlage bei einem Erdbe-

ben mit einer Eintrittshäufigkeit von 10^{-3} pro Jahr die Vorgaben von Art. 123 Abs. 2 Bst. c StSV erfüllt. Die für diesen Nachweis massgebenden Beschleunigungsspektren sind aus aktuell gültigen Erdbebengefährdungsstudien abzuleiten.

International gibt es keine einheitliche Regelung zur Festlegung des OBE, das im Übrigen nur in einzelnen Ländern festgelegt wird. Das von der US NRC festgelegte Betriebserdbeben ist beispielsweise so angesetzt, dass ein Weiterbetrieb nach einem OBE sichergestellt werden muss. Ein OBE nach amerikanischem Verständnis entspricht somit einem Erdbeben mit dessen Eintreten während der Lebensdauer eines Kernkraftwerks zu rechnen ist. Es entspricht damit gemäss Auslegung der Anlage einem 40-jährlichen Erdbeben.

5.5.3.2 Kapitel 6.3.2 „Externe Überflutung“

Als Konsequenz aus dem Unfall in Fukushima wurden in der Richtlinie ENSI-G02 die Anforderungen an den Schutz sicherheitsklassierter Bauwerke gegen externe Überflutung erhöht. Hierbei wurde zwischen bestehenden und neu zu errichtenden Gebäuden unterschieden. Bei neu zu errichtenden sicherheitsklassierten Gebäuden ist durch bauliche Massnahmen zwingend ein Wassereintrag zu vermeiden. Soweit permanente Hochwasserschutzmassnahmen bei bestehenden, sicherheitsklassierten Gebäuden nicht möglich oder nicht angemessen sind, ist auch die Errichtung temporärer Hochwassersperren durch das Betriebspersonal zulässig, sofern diese Wassersperren aufgrund der vorhandenen Vorwarnsysteme rechtzeitig aufgestellt werden können.

Zu Bst. d und f: Als permanente Hochwasserschutzmassnahme gilt auch ein Standort, der nachweislich nicht überflutet werden kann, ein sogenannter „trockener Standort“.

Zu Bst. g: Da aufgrund bisheriger Erfahrungen bei extremen Ereignissen eine Verstopfung der Kühlwasseransaugleitungen nicht ausgeschlossen werden kann, wird eine vom Fluss unabhängige Kühlwasserversorgung gefordert. Dies können z. B. Brunnenwassersysteme sein.

5.5.3.3 Kapitel 6.3.4 „Blitz“

Auf der Basis von Messungen der ETH-Zürich in den 1950er- und 1960er-Jahren sowie mit Hilfe von Experten der damaligen Schweizerischen Meteorologischen Anstalt (SMA) – heute Bundesamt für Meteorologie und Klimatologie MeteoSchweiz – legte die damalige nukleare Aufsichtsbehörde ASK bereits Ende der 1970er-Jahre drei Auslegungsblitze fest, denen die Kernkraftwerke standhalten müssen. Diese Auslegungsblitze wurden den Betreibern brieflich mitgeteilt, aber bisher nicht in einer Richtlinie festgehalten. Die Erfahrung über einige Jahrzehnte zeigte, dass diese Auslegungsblitze auch heute noch abdeckend sind. Eine Anpassung dieser Auslegungsblitze drängt sich deshalb vorläufig nicht auf, weshalb sie unverändert in die Richtlinie ENSI-G02 übernommen wurden (siehe Kap. 6.3.4.2 Bst. a der Richtlinie).

Zu Kap. 6.3.4.1 Bst. a: Gemäss Vorgaben der Vereinigung Kantonaler Feuerversicherungen (VKF) haben Blitzschutzanlagen Bauten und Anlagen sowie die sich darin aufhaltenden Personen vor den Auswirkungen von Blitzschlägen zu schützen. Zur Erreichung dieses Zieles müssen Blitzschutzanlagen gemäss den Vorgaben der VKF folgende grundlegenden Vorgaben erfüllen:

- Blitzschutzanlagen müssen den Blitzstrom auf ungefährlichen Bahnen in die Erde leiten. Sie bestehen aus Ausrüstungen für den äusseren Blitzschutz (z. B. Fangleiter, Ableitungen, Erdungen) sowie für den inneren Blitzschutz (z. B. Potenzialausgleich, Überspannungsschutz).
- Blitzschutzanlagen müssen ganze Gebäude umfassen. Zusammengebaute Gebäude sind gesamthaft zu schützen oder die Gebäude müssen mit Brandmauern voneinander getrennt sein.
- Die für den äusseren, die Nahtstelle zum inneren und den inneren Blitzschutz von Bauten und Anlagen vorzukehrenden Massnahmen richten sich nach Bauart und Nutzung.

Zu Kap. 6.3.4.2 Bst. b: Notstandsysteme sind zwingend gegen die Auslegungsblitze auszulegen. Das Notstandgebäude ist mittels Faradaykäfig gegen die Einwirkungen von Blitzen zu schützen.

5.6 Kapitel 7 „Spezifische Auslegungsanforderungen“

5.6.1 Kapitel 7.1 „Reaktorabschaltsystem“

Zu Bst. b: Die Anforderung, welche ein zur Reaktorschnellabschaltung diversitäres Abschaltsystem verlangt, entspricht dem Stand der Technik und wurde bereits bei der Errichtung der schweizerischen Kernkraftwerke erfüllt. Eine sichere langfristige Abschaltung der nuklearen Kettenreaktion ist eine Voraussetzung für die Erfüllung des technischen Schutzziels „Kontrolle der Reaktivität“.

Zu Bst. d: Die mechanische Auslegung der Kerneinbauten orientiert sich an den aufgrund bruchmechanischer Analysen zu postulierenden Leckagen und Brüchen an Leitungen der druckführenden Umschliessung. Die dynamischen Belastungen auf die Kerneinbauten resultieren primär aus den Entlastungsdruckwellen, die sich nach einem Bruch ergeben. Kann aufgrund bruchmechanischer Analysen, zum Beispiel aufgrund einer Leck-vor-Bruch-Analyse, oder aufgrund einer basissicheren Auslegung der Komponente ein Bruch ausgeschlossen werden, erübrigt sich eine detaillierte Belastungsanalyse für die Kerneinbauten.

5.6.2 Kapitel 7.2 „Reaktorkühlsystem“

Zu Bst. c Ziff. 1: Leck-vor-Bruch bedeutet, dass ein wanddurchdringender Riss unter allen Belastungen auf den Sicherheitsebenen 1 bis 3 begrenzt bleibt und ein Leck aus diesem

wanddurchdringenden Riss rechtzeitig erkannt wird, bevor ein globaler Integritätsverlust der Komponente eintreten kann.

Zu Bst. c Ziff. 2: Auch beim zu unterstellenden Integritätsverlust einer Komponente des Reaktorkühlsystems (Kühlmittelverlust) dürfen die zur Beherrschung erforderlichen Sicherheitsfunktionen nicht gefährdet werden. Ein Integritätsverlust des Reaktordruckbehälters ist nicht zu unterstellen.

Zu Bst. d: Bereits in der Richtlinie ENSI-G09 (Kap. 6.3.2 Bst. a) wird die Festschreibung von Sicherheitsgrenzwerten verlangt. Die Anforderung ist somit eine Konkretisierung für das Reaktorkühlsystem und erfüllt den WENRA SRL E7.3.

Zu Bst. e: Mit Druckbegrenzungseinrichtungen wird der Druck im Reaktorkühlsystem auf einen vorbestimmten Druck eingestellt und gehalten. Überdruckabsicherungen stellen sicher, dass bei einem festgelegten, maximal zulässigen Druck automatisch eine Druckentlastung eintritt und zwar solange, bis der Druck auf einen vorgegebenen Druck abgesunken ist. Dann schliesst die Druckabsicherung wieder automatisch.

Zu Bst. g: Dazu gehören Kühlmittelreinigungs- und -entgasungsanlagen, mit denen korrosionsfördernde Stoffe, Korrosionsprodukte, Aktivierungs- und Spaltprodukte, Radiolyseprodukte sowie sichtbehindernde Schwebstoffe aus dem Kühlmittel entfernt werden.

Zu Bst. h: Durch geeignete Leitungsführung im Reaktorkühlsystem soll unter anderem verhindert werden, dass kaum oder schlecht durchmischte Bereiche entstehen, in denen sich zündfähiges Radiolysegas ansammeln kann.

5.6.3 Kapitel 7.3 „Wasser-Dampf-Kreislauf“

Zu Bst. a: Mit dieser Anforderung wird sichergestellt, dass eine Beeinträchtigung der Integrität der druckführenden Umschliessung des Reaktorkühlsystems durch Rückwirkungen des Wasser-Dampf-Kreislaufs ausgeschlossen werden kann. Die Anforderung leitet sich aus Requirement 77 des IAEA Safety Standard SSR 2/1 ab.

5.6.4 Kapitel 7.4 „Druckentlastung“

Zu Bst. a Ziff. 1: Die Druckentlastung des Primärkreises bei Druckwasserreaktoren erfolgt auslegungsgemäss durch die Druckentlastung des Sekundärkreislaufes. Dabei wird der Druck im Primärkreis über die Druckentlastungsventile der Dampferzeuger abgesenkt. Die direkte primärseitige Druckentlastung bei Druckwasserreaktoren ist nur für den Fall von SE4-Störfällen vorgesehen, sollte dabei die sekundärseitige Druckentlastung versagen.

Zu Bst. a Ziff. 2: Bei SE4b-Störfällen kann ein Versagen der Druckentlastungsfunktion nicht absolut ausgeschlossen werden. Das Versagen soll aber so unwahrscheinlich sein, dass ein sogenanntes Hochdruckversagen des Reaktordruckbehälters nach menschlichem Ermessen ausgeschlossen werden kann. Erkenntnisse aus Schwerunfallanalysen zeigen, dass bei

Versagen der Druckentlastungsfunktion die Wahrscheinlichkeit hoch ist, dass eine Druckentlastung des Reaktorkühlsystems durch vorher versagende Leitungen erfolgt.

Zu Bst. b Ziff. 3: Die sekundärseitige Druckentlastung muss bei Druckwasserreaktoren auch bei Verlust der gesamten Stromversorgung durch manuelles Öffnen der Druckentlastungsventile eingeleitet werden können. Damit wird bei niedrigem Reaktordruck mittels Accident-Management-Massnahmen eine Kernkühlung ermöglicht.

Zu Bst. c Ziff. 2: Die Druckentlastung muss bei Siedewasserreaktoren auch bei Ausfall der Wechselstromversorgung aus der Notstromanlage und der Notstand-Notstromanlage (sogenannter Station-Blackout, SE4a-Störfall) gewährleistet sein, um bei niedrigem Reaktordruck die Kernkühlung mittels Accident-Management-Massnahmen zu ermöglichen.

5.6.5 Kapitel 7.5 „Kernnotkühlung“

Zu Bst. b: Bei Verlust der Wechselstromversorgung aus der Notstromanlage und der Notstand-Notstromanlage (Station-Blackout) kann die Kernnotkühlung zum Beispiel über dampfgetriebene Einspeisesysteme, fest installierte passive oder mobile (aktive) Einspeisemöglichkeiten sichergestellt werden.

Zu Bst. c: Der doppelendige Bruch (2F-Bruch) einer Hauptkühlmittelleitung (DWR) beziehungsweise Umwälzleitung (SWR) bestimmt die Dimensionierung der Not- und Nachkühlsysteme, die Druckauslegung des Primärcontainments und die Störfallfestigkeit aller zur Störfallbeherrschung erforderlichen sicherheitstechnisch wichtigen Komponenten im Primärcontainment. Die durch die Notkühlsysteme zu fördernde Kühlwassermenge muss somit den Kühlwasserverlust bei einem doppelendigen Bruch einer beliebigen Leitung des Reaktorkühlsystems überspeisen können.

5.6.6 Kapitel 7.6 „Nachwärmeabfuhr“

Zu Bst. c: Zwei voneinander diversitäre Wärmesenken sind beispielsweise durch Kühlwasserversorgung aus dem Fluss und Notstandbrunnen gewährleistet.

Zu Bst. d: Massnahmen zur Vermeidung von Verunreinigungen im Containment sind beispielsweise der Einsatz von Kassettenisolierungen der Rohrleitungen sowie die Verwendung von erosions- und korrosionsresistenten Materialien.

Zu Bst. e: Massnahmen zur Vermeidung einer Verstopfung der Ansaugöffnungen der primärseitigen Nachwärmeabfuhrsysteme sind beispielsweise eine Vergrösserung und die Möglichkeit zur Rückspülung der Ansaugsiebe.

5.6.7 Kapitel 7.7 „Containment“

Zu Bst. b Ziff. 2: Damit sind auch die Brennelementlager innerhalb des Containments geschützt.

Zu Bst. d: Massnahmen zum Abbau zündfähiger Gase sind beispielsweise die Durchmischung von Wasserstoff zur Verhinderung einer lokalen Aufkonzentration, die Verbrennung von Wasserstoff durch geeignete Zündsysteme oder der Abbau von Wasserstoff durch passiv funktionierende autokatalytische Rekombinatoren.

5.6.7.1 Kapitel 7.7.1 „Primärcontainment“

Zu Bst. e: Die erwähnten Schleusen umfassen auch diejenigen, die für die Materialanlieferung eingesetzt werden. Während Revisionen können die Verriegelungen bestimmter Schleusen aufgehoben oder sogar bestimmte Schleusentüren geöffnet sein. Die betreffenden Schleusentüren gelten bei Ausfall der Stromversorgung während der Revisionen als ausreichend schnell wieder verschliessbar, wenn unter der zusätzlichen Bedingung eines dauerhaften Ausfalls der Brennstoffkühlung durch vorbereitete Notfallmassnahmen sichergestellt ist, dass das Schliessen innerhalb eines Zeitfensters möglich ist, in dem die Brennelemente noch vollständig mit Wasser überdeckt sind.

Zu Bst. f: Mit den geforderten Massnahmen soll die generelle Integrität des Containments wie auch eine Umgehung des Containments (Containment-Bypass) bei Störfällen möglichst vermieden werden. Damit wird sichergestellt, dass bei Störfallszenarien, die sich bis zu einem Kernschaden weiterentwickeln, kein direkter Freisetzungspfad in die Umgebung auftritt.

Zu Bst. g: Massnahmen sind beispielsweise die Kontrolle der Isolationsarmaturen oder das schnelle Kaltfahren der Anlage. Mit dieser Anforderung wird zusammen mit der Anforderung von Bst. f der WENRA SRL F4.8 erfüllt (siehe Anhang 2).

5.6.8 Kapitel 7.8 „Baustrukturen“

5.6.8.1 Kapitel 7.8.1 „Grundlegende Anforderungen“

Zu Bst. a: Die Gewährleistung der Abtragung der Lasten wird durch entsprechende Nachweise belegt, siehe Kapitel 7.8.3. Für die Sicherheitsebene 4a dürfen die bautechnischen Nachweise unter Berücksichtigung der realistischen bzw. effektiven Einwirkungen und Widerstände (Best Estimate) geführt werden.

Zu Bst. b Ziff. 1: Gemeint sind zum Beispiel die Anforderungen an den biologischen Schild im Containment.

Zu Bst. f: Zu den spezifisch für die Kernkraftwerke festgelegten Einwirkungen gehören spezifische Nutzlasten und Erdbeben.

5.6.8.2 Kapitel 7.8.2 „Tragsicherheit und Gebrauchstauglichkeit“

Zu Bst. a bis c: Die Nachweise für Betonbauten sind nach Norm SIA 262 und diejenigen für Stahlstrukturen nach Norm SIA 263 zu führen. Die Themenbereiche, die in den SIA-Normen nicht oder nicht ausreichend detailliert geregelt sind, können unter Anwendung anderer Nor-

men behandelt und nachgewiesen werden, falls dies mit vergleichbarem Anforderungsniveau und methodisch konsistent zu den SIA-Normen erfolgt (z. B. Berechnung von Rissbreiten nach Norm DIN EN 1045).

Zu Bst. c: Die durchzuführenden Nachweise werden grundsätzlich nach dem Konzept der Partialsicherheitsfaktoren gemäss SIA- oder entsprechenden Eurocode-Tragwerksnormen geführt. Dabei werden die Unsicherheiten bezüglich der Modellierung und die Streuung der Materialkennwerte (z. B. Festigkeit) durch Verwendung der Lastfaktoren (Erhöhung der Einwirkung) und Widerstandsbeiwerte (Reduktion des Widerstandes) berücksichtigt.

5.6.8.3 Kapitel 7.8.3 „Erdbeben“

Zu Bst. a: Besonders für grosse, schwere und relativ steife im Boden eingebettete Bauwerke wie das Reaktorgebäude ist der Einfluss der Boden-Bauwerk-Interaktion von grosser Bedeutung.

Die Streuung der Bodenwerte wird in der Regel durch Verminderung und Erhöhung der mittleren Baugrundsteifigkeit um den Faktor 1,5 abgebildet. Somit werden mindestens 3 Bodenmodelle in den Berechnungen berücksichtigt. Pro Bodenmodell werden mindestens 3 Sets mit jeweils 3 statistisch unabhängigen Erdbebenzeitverläufen verwendet. Die Ergebnisse aus den Berechnungsdurchgängen der einzelnen Sets pro Bodenmodell werden gemittelt. Die Ergebnisse der Berechnung mit unterer, mittlerer und oberer Baugrundsteifigkeit werden hingegen eingehüllt.

Alternativ zu dieser an der KTA-Regel 2201.1 angelehnten deterministischen Vorgehensweise können auch Sampling Methoden unter Verwendung einer statistisch ausreichenden Anzahl von Erdbebenszenarien und Beschleunigungszeitverläufen benutzt werden. Streuungen und Unsicherheiten in den Baugrund- und Bauwerkseigenschaften werden dabei durch entsprechende Parametervariation berücksichtigt.

Zu Bst. b: Die sogenannte Freifeld-Bodenerschütterung im Referenzpunkt muss den vom ENSI festgelegten zum Zeitpunkt der Errichtung gültigen Gefährdungsannahmen (Erdbebeneinwirkung) entsprechen. In welchem Punkt die Erdbebeneinwirkung in der Boden-Bauwerks-Interaktionsberechnung angesetzt wird, hängt von weiteren Faktoren (u. a. vom verwendeten Berechnungsprogramm) ab. Es sind zu den betrachteten Spektren kompatible Erdbebenzeitverläufe zu verwenden.

Zu Bst. c: Sowohl die Materialdämpfung als auch die dynamische Steifigkeit des Bodens hängen vom Wert der Schubverzerrung ab, was in der Boden-Bauwerks-Interaktion zu berücksichtigen ist.

Ein nichtlineares Bauwerksverhalten kann einen relevanten Einfluss auf die Steifigkeit und die Dämpfung der Baustrukturen haben. Es beeinflusst dadurch die Boden-Bauwerks-Interaktion, die resultierenden Etagenantwortspektren sowie die Auswirkungen der Baustruktur selbst. Deshalb sind sowohl bei der Boden-Bauwerks-Interaktion als auch bei der Erdbebenberechnung der Baustrukturen dem betrachteten Auswirkungsniveau entsprechende

Bauteilsteifigkeiten zu verwenden. Damit werden realistische Eigenfrequenzen und Verschiebungen ermittelt. Bei Anwendung von linear elastischen Berechnungsmethoden kann dies durch die Reduktion des E-Moduls des Betons erfolgen. Ohne genauere Betrachtung darf für die Dämpfung von Stahlbetonstrukturen 7 % der kritischen Dämpfung bei aktuell gültigem SSE und 4 % bei aktuell gültigem Auslegungserdbeben für BK-II-Gebäude angesetzt werden.

Zu Bst. d: Aus den seismisch induzierten Bauwerksbewegungen werden die sogenannten Etagenantwortspektren abgeleitet, die als standortabhängige Erdbebeneinwirkung für Systeme und Komponenten dienen. Sie werden im Englischen auch Floor Response Spectra (FRS) oder In-Structure Response Spectra (ISRS) genannt. Etagenantwortspektren werden in massgebenden Punkten der Bauwerksstruktur in drei orthogonalen Richtungen für verschiedene Dämpfungswerte bestimmt. Aus den Etagenantwortspektren werden durch Umhüllung, Verbreitung und Glättung die Etagenbemessungsspektren konstruiert, siehe auch KTA-Regel 2201.3.

Probabilistische, unter Anwendung von Sampling-Methoden ermittelte Etagenantwortspektren können für die klassischen deterministischen Nachweise verwendet werden, falls aufgezeigt wird, dass sie gleichwertig zu den deterministisch ermittelten Etagenbemessungsspektren sind.

Zu Bst. f: Als anerkannte Methoden für die modale Überlagerung gelten die SRSS-Methode (Square Root of the Sums of the Squares) oder für den Fall, wenn Eigenfrequenzen nah beieinander liegen, die CQC-Methode (Complete Quadratic Combination). Für die Richtungsüberlagerung kommen ebenfalls die SRSS-, die CQC-Methode mit drei Komponenten (CQC3) oder alternativ – als in den meisten Fällen zulässige Vereinfachung – die 100-40-40-Regel zur Anwendung.

In der Regel gilt, dass die Summe der effektiven modalen Massen der berücksichtigten Schwingungsformen mindestens 90 % der Gesamtmasse des Tragwerks erreichen soll. Dadurch werden die Auswirkungen aus allen Schwingungsformen, die wesentlich zum Schwingungsverhalten beitragen, berücksichtigt.

Zu Bst. g: Ein linear-elastisches Strukturverhalten bei der Auslegung der Bauwerke bedeutet, dass die Verhaltensbeiwerte der Normen des SIA nicht anzuwenden sind und dass die Auslegung mit elastischen Antwortspektren erfolgt.

In begründeten Ausnahmefällen kann es erforderlich sein, nichtlineare Berechnungsverfahren zu verwenden, zum Beispiel das nichtlineare Zeitverlaufsverfahren und das verformungsbasierte Verfahren. Bei einer nichtlinearen Zeitverlaufsberechnung gilt die ausreichende Erdbebenkapazität als nachgewiesen, wenn die Versagenskriterien während der gesamten Zeitverläufe bei einer die Gefährdung abdeckenden Auswahl von Erdbeben nicht erreicht werden. Als Versagenskriterien gelten beispielsweise Grenzwerte für die Schubverzerrung oder für Rotationen in den plastischen Gelenken der Bauteile.

Bei einer verformungsbasierten Berechnung (z. B. Pushover-Berechnung) gilt der Nachweis als erbracht, wenn der ausgewiesene Verformungsbedarf geringer ist als der entsprechende Bemessungswert des Verformungsvermögens. Bei nichtlinearen Berechnungen ist der Anforderung von Bst. h besondere Beachtung zu schenken.

Zu Bst. h: Der Einfluss von Unsicherheiten und Modellierungsannahmen, die nicht durch die Partialsicherheitsfaktoren (Last- und Widerstandsbeiwerte) abgedeckt sind, wird durch Sensitivitätsanalysen und Grenzwertbetrachtungen erfasst.

5.6.9 Kapitel 7.9 „Steuerstellen“

5.6.9.1 Kapitel 7.9.1 „Technische Vorgaben“

Zu Bst. a: Bei gewissen Störfällen werden nicht alle Eingriffe vom Hauptkommandoraum aus durchgeführt, sondern auch von der Notsteuerstelle aus. Letztere kann in mehrere örtlich voneinander getrennte Steuerstellen aufgeteilt sein. Die Anforderung verlangt, dass die notwendigen Ausrüstungen im Hauptkommandoraum für diejenigen Störfälle vorhanden sind, für deren Beherrschung gemäss internen Vorgaben Handlungen im Hauptkommandoraum durchgeführt werden müssen. Die Abstimmung der Ausrüstungen mit denjenigen in der Notsteuerstelle ist deshalb zentral wichtig.

Zu Bst. b: Die Aufteilung der Notsteuerstelle in mehrere örtlich voneinander getrennte Steuerstellen kann sich aus der Grundauslegung einer Anlage ergeben, beispielsweise aufgrund einer systematischen Trennung von elektrischen Versorgungsredundanzen (Divisionen, Stränge), oder aus der grundsätzlichen Trennung von automatisierten durch Notstandsysteme ausgeführten SE3-Funktionen von anderen Funktionen (Sicherheitsfunktionen, manuelle Betätigungen).

Zu Bst. d: Unter Brandeinwirkungen werden Einwirkungen durch Flammen, Wärme, Rauch und Funken verstanden.

Zu Bst. e: Die manuelle Auslösung von mehreren Steuerstellen aus wird nicht gefordert, ist aber je nach zu betrachtendem Störfallszenario zu berücksichtigen. Sind zum Beispiel zur Beherrschung von Auslegungsstörfällen Notstandsysteme notwendig, sollen diese auch vom Hauptkommandoraum aus angesteuert werden können.

Zu Bst. f: Unter unbefugten Eingriffen in der Steuerstelle sind manuelle Betätigungen einer Person zu verstehen, welche nicht berechtigt ist, diese durchzuführen. Eine Fehlbedienung ist eine Handlung einer Person, welche zwar berechtigt ist, eine spezifische Handlung durchzuführen, diese jedoch durch Fehlhandlung, Verwechslung oder Fehlüberlegung falsch ausführt.

5.6.9.2 Kapitel 7.9.2 „Ergonomische Vorgaben“

Zu Bst. c: Die Anzeigen in der Notsteuerstelle sollen auf die wesentlichen Anzeigen optimiert sein, die für die Störfallbeherrschung oder Linderung der Konsequenzen von Störfällen not-

wendig sind. Damit soll sichergestellt werden, dass die Operateure nicht durch zu viele und nicht relevante Anzeigen abgelenkt werden. Sie müssen aber über die notwendigen Anzeigen verfügen, um klare Entscheide fällen zu können.

5.6.10 Kapitel 7.10 „Leittechnik“

Unter Leittechnik versteht man die grundlegende Technik für die Aufgaben Messen, Steuern und Regeln. Der Begriff Leittechnik ist hersteller- und systemneutral.

Unter Leitsystem wird die Gesamtheit aufeinander abgestimmter, zusammenarbeitender Komponenten, Geräte und Module verstanden. Das Leitsystem ist hersteller- und teilweise branchenspezifisch und besteht aus einer oder mehreren Gerätefamilien und wird vom Hersteller mit einem Markennamen benannt (Name der Leittechnikfamilie). Ein Leitsystem kann generisch, nicht jedoch anlagespezifisch qualifiziert sein.

Als Leitanlage wird die konkrete Implementierung eines leittechnischen Systems oder leittechnischer Einrichtungen in einer Anlage verstanden. Leitanlagen führen die entsprechenden anlagespezifischen leittechnischen Funktionen aus. Die konkret in einer Anlage implementierten sicherheitsrelevanten Leitanlagen einschliesslich der zugehörigen Bedienelemente und Anzeigen erfüllen somit die Aufgaben Messen, Steuern (einschliesslich Schutzauslösungen), Regeln, Schutz (Komponentenschutz), Überwachung, Visualisierung und Registrierung. Die durch Leitanlagen umgesetzten leittechnischen Funktionen sind Bestandteil der entsprechenden Schutzzielfunktionen während des Normalbetriebs (SE1-Funktionen), bei Betriebsstörungen (SE2-Funktionen), zur Beherrschung von Auslegungsstörfällen (SE3-Funktionen) und in beschränktem Umfang auch bei auslegungsüberschreitenden Störfällen (Notfallmassnahmen, SE4-Funktionen).

SE1-Leitanlagen umfassen betriebliche Steuer- und Regeleinrichtungen, SE2-Leitanlagen umfassen leittechnischen Einrichtungen, die geeignet sind, bei Betriebsstörungen eine Anforderung der Schutzaktionen der Sicherheitsebene 3 zu vermeiden. SE3-Leitanlagen steuern und regeln Sicherheitssysteme und lösen bei Erreichen festgelegter Ansprechwerte Schutzaktionen aus. Zu den SE3-Leitanlagen gehört insbesondere das Reaktorschutzsystem.

5.6.10.1 Kapitel 7.10.1 „Grundlegende Anforderungen an Leitanlagen“

Zu Bst. a*:* Bei Ansteuerung mehrerer Systeme auf verschiedenen Sicherheitsebenen sind alle Anforderungen dieser Sicherheitsebenen gemäss Kap. 5.1 Bst. a zu erfüllen. Leittechnische Funktionen auf der Sicherheitsebene 4a werden meistens durch SE3-Leitanlagen wahrgenommen.

Zu Bst. b*:* Mit dieser Anforderung wird eine wesentliche Voraussetzung dafür geschaffen, dass das Prinzip der gestaffelten Sicherheitsvorsorge umgesetzt wird und dass insbesondere SE3-Funktionen nicht gleichzeitig mit SE1- oder SE2-Funktionen ausfallen.

Zu Bst. d: Ausfälle aufgrund gemeinsamer Ursachen wird durch das Prinzip der funktionalen Diversität begegnet, indem sicherheitsrelevante Funktionen diversitär realisiert werden. Dies kann beispielsweise durch die Nutzung unterschiedlicher verfahrenstechnischer Prozessgrössen (z. B. Neutronenfluss und Reaktordruck beim Siedewasserreaktor) erfolgen, begleitet durch die unterschiedliche Verarbeitung in der Leittechnik (z. B. Nutzung von unterschiedlichen Ein-/Ausgabebaugruppen und anderen Softwarebausteinen).

Zu Bst. e: Falls eine Funktionskonzentration vorliegt, ist durch Ausfallanalysen unter anderem zu belegen, dass dadurch kein gleichzeitiger Ausfall mehrerer zentral wesentlicher Regelungsfunktionen für den sicheren Betrieb der Anlage entsteht. Zu den wesentlichen Regelungsfunktionen zählen u. a. die Reaktor- und Speisewasserregelungen.

Zu Bst. f: Die Vermeidung der Zusammenlegung gestaffelter Funktionen auf den Sicherheitsebenen 1 und 2 (z. B. Begrenzungen als nachgelagerte Funktionen zu Regelungen) auf einzelnen physikalischen Einheiten von zentralen Leittechnikkomponenten (z. B. Prozessoren, Ein-/Ausgabemodulen) dient der verbesserten Einhaltung der gestaffelten Sicherheitsvorsorge.

Zu Bst. g: Bei mehrkanaligem Aufbau von Funktionssträngen ist die Aufteilung auf physisch unterschiedliche Teilsysteme durchgängig beizubehalten, um bei Einzelausfällen nicht mehrere Stränge gleichzeitig zu verlieren.

Zu Bst. i: Falls Abweichungen zur Diversitätsforderung bei SE3-Funktionen begründet werden sollen, soll dies vorzugsweise im Rahmen der von der Richtlinie ENSI-A04 geforderten funktionsorientierten Diversitätsanalyse erfolgen. Die funktionsorientierte Diversitätsanalyse soll aufzeigen, dass der Grundsatz der Diversität (funktional und gerätetechnisch) umgesetzt ist und hat sich primär auf die Leittechnikfunktionen (z. B. RESA-, ESFAS-, Notstrom-Kriterien) bzw. Gerätefunktionen zu beziehen und soll diese Funktionsebene behandeln. Hierbei sind, wo notwendig, die Schutzziele, die zugehörigen verfahrenstechnischen Sicherheitsfunktionen und ihre Eigenschaften sowie die abzudeckenden Störfallszenarien einzubeziehen. Bei der Unterstellung eines CCF (Common Cause Failure, systematischer Ausfall) in der programmierten Leittechnik ist für eine Abweichung zur Diversitätsforderung aufzuzeigen, warum das Weglassen der diversitär realisierten SE3-Funktion aus sicherheitstechnischer Sicht akzeptiert werden kann. Insbesondere ist für den unterstellten CCF-Fall jeweils auch die Einhaltung der Schutzziele gemäss Kapitel 4.1 aufzuzeigen.

Mit der Anforderung von Bst. i der Richtlinie werden verschiedene Anwendungsfälle abgedeckt. Nachfolgend werden denkbare Anwendungen beispielhaft erläutert:

Für den Fall, dass zwei verschiedene programmierbare Leitsysteme, Leittechnik-Teilsysteme oder Leittechnikkomponenten eingesetzt werden, soll die diversitäre Gerätetechnik bei diesen programmierbaren Teilen so realisiert werden, dass jeweils zueinander hardware- und softwaremässig diversitäre Leittechnikkomponenten zum Einsatz kommen, um den CCF zu beherrschen, der bei programmierbaren Technologien aufgrund von komplexerer und empfindlicherer Leittechnik-Hardware oder komplexer Software grundsätzlich unterstellt wird. Die Diversitätsbetrachtungen (Eigenschaften, Massnahmen) sind zu dokumentieren. Die Erstel-

lungssoftware von anwendungsspezifisch programmierten Elektronikbausteinen muss bezüglich der Diversitätsüberlegungen berücksichtigt werden und ist gegebenenfalls Bestandteil der Diversitätsbetrachtungen.

Falls die Diversität zu einer programmierbaren Leittechnikkomponente mittels festverdrahteter Komponenten realisiert wird, kann die Diversitätsforderung ohne weitere Analysen als erfüllt betrachtet werden. Anwendungsspezifisch programmierte Elektronikbausteine gelten in diesem Kontext beispielsweise nicht als rein festverdrahtete Komponenten, weil diese Bausteine für die spezifische Anwendung programmiert oder parametriert werden, wozu anwendungsspezifische Software eingesetzt wird.

Die im Anlagedesign vorhandenen systemtechnischen, elektrotechnischen und leittechnischen Sicherheitsredundanzen können bei der Umsetzung der Diversitätsforderung mitberücksichtigt werden. Insbesondere kann die Leittechnik im gesicherten Bereich (Notstandsysteme) beziehungsweise der Diversität zum ungesicherten Bereich mitberücksichtigt werden. Die Diversität kann beispielsweise innerhalb jeder der vorhandenen systemtechnischen und elektrotechnischen Redundanzen realisiert werden oder es kann, bei weniger komplexen Geräten, für einen Anwendungsfall eine gesamthafte Lösung passend zum Anlagedesign konzipiert werden. Beispielsweise können bei programmierbaren starkstromtechnischen Schutzgeräten die diversitären Geräte einzelnen Sicherheitsredundanzen zugeordnet werden, um gesamthaft das Ziel der CCF-Beherrschung zu erreichen.

Die Formulierung „bezüglich der programmierten Systemteile“ soll dem Missverständnis vorzubeugen, ganze Funktionsketten (z. B. Messwertgeber bis Stellgliedansteuerung), die solche programmierten Systemteile enthalten, seien gerätetechnisch diversitär auszuführen. Beim Einsatz von zentralen Sicherheitsleitsystemen (z. B. RESA-, ESFAS-, Notstrom-Kriterien) kann es jedoch angemessen sein, die Diversität auf diese zentralen Teile der Leitsysteme und damit auf einen erweiterten Bereich von Systemteilen, Baugruppen und Geräten gesamthaft anzuwenden. Dazu können beispielsweise ganze Baugruppenträger, komplexere Kommunikationsverbindungen oder elektrische Versorgungsgeräte mit bekanntermassen höheren Ausfallanfälligkeiten respektive -häufigkeiten gezählt werden.

Zu Bst. l: Beim Einsatz von neuen leittechnischen Ausrüstungen ist es Stand der Technik, dass 0E-klassierte leittechnische Ausrüstungen mit programmierbarer Leittechnik selbstüberwachend ausgeführt werden und während des Normalbetriebs ohne Einschränkung der Funktion prüfbar sind.

Zu Bst. m: Die Anforderung verlangt eine möglichst umfassende integrale Prüfung der leittechnischen Funktion bis zum Aktuator. Das bedeutet, dass die Prüfung die Funktionsfähigkeit des Aktuators (z. B. Pumpe, Ventil) nicht einschliessen muss. Die Prüfung der Funktionsfähigkeit des Aktuators erfolgt normalerweise im Rahmen von Wiederholungsprüfungen.

5.6.10.2 Kapitel 7.10.2 „Vorrangbildung von Signalen“

Zu Bst. a Ziff. 1: Von Interesse sind insbesondere die Bedienorte Hauptkommandoraum und Notsteuerstelle, gegebenenfalls auch weitere örtliche Steuerstellen mit einem systembezo-

genen beschränkten Funktionsumfang. Die Anregekriterien für die Notstandsysteme sind insbesondere so gewählt, dass sie später ansprechen, als die der Sicherheitssysteme. Falls letztere nicht funktionieren, werden die Notstandsysteme also aktiviert und haben in der Regel Vorrang. Der Vorrang für die Notstandsignale wird auf der Vorrangebene entsprechend projektiert. Zudem wird der Vorrang für die Handbetätigungssignale üblicherweise von Hand auf die Betätigungselemente der Notsteuerstelle umgeschaltet, wenn der Hauptkommandoraum (HKR) aufgrund eines Ereignisses (z. B. HKR-Brand, UEW) nicht mehr benutzbar ist.

Zu Bst. a Ziff. 3: Üblicherweise werden Sicherheitsleittechnik (SILT) und betriebliche Leittechnik (BELT) unterschieden. Die sicherheitsbezogenen Funktionen können Teil der SILT oder Teil der BELT sein. Die betrieblichen Funktionen der BELT teilen sich auf in sicherheitsbezogene betriebliche Funktionen und sonstige betriebliche Funktionen.

5.6.11 Kapitel 7.11 „Instrumentierung und Anzeigesysteme“

Zum Begriff „Instrumentierung“: Die Ausrüstungen der Instrumentierung umfassen die analoge und binäre Zustandserfassung (Sensorik) einschliesslich der zugehörigen Verarbeitung der Messsignale. Sie dienen der Regelung und Kontrolle der Kraftwerksanlage und ihrer Systeme und Komponenten. Die Instrumentierung kann je nach System und Anwendungsfall auch komplexere Datenübertragungsteile und zentrale Verarbeitungseinheiten wie auch Anzeige- und Registriereinheiten mit umfassen.

Die Begriffe „Störfallinstrumentierung“ und „Betriebsinstrumentierung“ sind im Anhang 1 der Richtlinie definiert.

5.6.11.1 Kapitel 7.11.1 „Allgemeine Anforderungen“

Zu Bst. a: Gemäss KEV ist ein Störfall jeder vom Normalbetrieb abweichende Anlagezustand, der ein Eingreifen eines SE3-Systems (wird in der KEV als Sicherheitssystem bezeichnet) erfordert. Entsprechend umfasst die Störfallinstrumentierung alle Instrumente, die zur Beherrschung oder Linderung von Störfällen notwendig sind, also für SE3- und SE4-Störfälle. In den schweizerischen Kernkraftwerken wird unter Störfallinstrumentierung im engeren Sinn oft nur die Instrumentierung für SE3-Störfalle verstanden.

Zu Bst. b: Als Zeitsignal ist beispielsweise das Signal des Langwellensenders DCF77 denkbar. Dieser Langwellensender steht in Mainflingen bei Frankfurt am Main und dient der Verbreitung der gesetzlichen Zeit für Deutschland, das heisst der mitteleuropäischen Zeit MEZ beziehungsweise der Mitteleuropäischen Sommerzeit MESZ. Der Empfang des Senders DCF77 ist nahezu überall in Deutschland und im angrenzenden Ausland möglich. Der Sender wird durch die Atomuhren der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig gesteuert. Die Zeitsynchronisierung ist für eine rasche und effektive Störfallanalyse zwingend notwendig.

5.6.11.2 Kapitel 7.11.2 „Betriebsinstrumentierung und Anlageinformationssysteme“

Zu Kap. 7.11.2.1 Bst. a: Die Bezeichnung Anlageinformationssystem (ANIS) ist nicht einheitlich. In einigen Anlagen wird dafür die Bezeichnung Prozessrechneranlage (PRA) verwendet. Die Anforderungen betreffend ANIS gelten unabhängig von der verwendeten Bezeichnung.

Zu Kap. 7.11.2.2 Bst. d: Die Formulierungen „Alarmindikationen“ und „Indikation für einen Ausfall des SPDS“ bringen zum Ausdruck, dass das Vorliegen eines Alarms oder Ausfalls durch die Veränderung eines vorhandenen Elements angezeigt wird, zum Beispiel durch einen Farbumschlag oder ein Blinken. Es handelt sich bei dieser möglichen Realisierungsart also nicht um ein zusätzliches grafisches oder textliches Alarm-/Anzeigeelement.

Zu Kap. 7.11.2.2 Bst. h: Das SPDS ist heute in allen in Betrieb stehenden schweizerischen Kernkraftwerken auch in der Notsteuerstelle aufgeschaltet, muss aber nicht 1E-qualifiziert werden. Im Normalfall ist die SPDS-Anzeige festen Anzeigeeinheiten (Bildschirmen) zugeordnet. Bei Ausfall einer dieser fest zugeordneten Anzeigeeinheiten, muss das SPDS auch von anderen, nicht fest zugeordneten Bildschirmen aus benutzt werden können.

5.6.11.3 Kapitel 7.11.3 „Störfallinstrumentierung“

Zu Bst. a Ziff. 3: Aufgrund der Information der Störfallinstrumentierung muss zum Beispiel eine Abschätzung des Quellterms durch den Betreiber der Anlage möglich sein. Mit dieser Information wird das ENSI die Konsequenzen in der Umgebung der Anlage abschätzen.

Zu Bst. b: Zur Milderung der Konsequenzen schwerer Unfälle (SE4b-Störfälle) sind anlagespezifisch symptomorientierte Entscheidungshilfen (SAMG) bereitzustellen, die sich auf noch vorhandenen Messungen abstützen. Die Vorgaben an die für SAMG-Massnahmen verwendete Instrumentierung sind in Kap. 8.3.5 der Richtlinie ENSI-B12 enthalten.

Zu Bst. g: Die Stromversorgung der Störfallübersichtsanzeigen ist gemäss Anforderung von Bst. f unterbrechungsfrei über Batterien zu gewährleisten. Bei Verlust der Notstromanlage und der Notstand-Notstromanlage ist die Stromversorgung über die Batterien nur für eine begrenzte Zeit gewährleistet. Daher muss diese mittels spezieller Notfallaggregate vor der Erschöpfung der Batteriekapazität sichergestellt werden.

Zu Bst. i Ziff. 4: Mit der Anforderung bezüglich Qualifizierungsdaten sind die ortsspezifischen Störfallbedingungen zu berücksichtigen, das heisst es ist anzugeben, wie die Komponenten der Messkette für die auftretenden Störfallbedingungen qualifiziert werden.

Zu Bst. i Ziff. 6: Relevant sind hier gegebenenfalls Alarm- oder Auslösegrenzwerte, die gemäss Störfallvorschriften zu einem Operateureingriff führen.

5.6.11.4 Kapitel 7.11.4 „Gefahrmeldeanlagen“

Zu Bst. e: Die Gefahrmeldeanlagen (GMA) umfassen klassierte (1E, 0E) und unklassierte Anzeigen. Die Klassierung erfolgt entsprechend der Sicherheitsbedeutung ihrer Funktionen.

So sind beispielsweise Anzeigen, die beim Sicherheitserdbeben SSE notwendig sind, als 1E zu klassieren und entsprechend gegen das SSE auszulegen.

5.6.11.5 Kapitel 7.11.5 „Erdbebeninstrumentierung“

Zu Bst. a Ziff. 2: Mit der Überschreitung von festgelegten Grenzwerten sind beispielsweise die Auslegungswerte für das Sicherheitserdbeben (SSE) gemeint.

Zu Bst. g: In den zentralen Instrumentierungsausrüstungen werden die lokalen Daten gesammelt und davon abgeleitet Alarme an den Hauptkommandoraum weitergeleitet. Die zentrale Leittechnik besitzt keine vollständige 1E-Auslegung, beispielsweise müssen der Speicher und der Drucker nicht gegen SSE ausgelegt sein, weil die lokalen Instrumente (gegen SSE ausgelegt) die Speicherung der Daten übernehmen (vgl. Anforderung von Bst. f von Kap. 4.11.5).

Zu Bst. h: Nur die erdbebenbedingten Erschütterungen sollen beim Überschreiten der Grenzwerte zur Alarmierung der Schichtmannschaft führen, weil verhindert werden soll, dass nicht-erdbebenbedingte Erschütterungen (z. B. durch Bauarbeiten, Bohrarbeiten oder Lastwagen), die erfahrungsgemäss wegen ihrer geringen Energie unbedeutend sind, zu Fehlalarmen führen.

5.6.12 Kapitel 7.12 „Stromversorgung“

5.6.12.1 Kapitel 7.12.1 „Grundlegende Anforderungen“

Die Stromversorgung eines Kernkraftwerks erfolgt durch externe und interne Stromquellen. Sie muss so zuverlässig sein, dass sie die Nichtverfügbarkeit der zu versorgenden Systeme nicht massgeblich beeinflusst. Diese Anforderung ist zentral, da der Verlust der Stromversorgung in Kernkraftwerken zu einem schweren Unfall führen kann.

Die Stromversorgung der schweizerischen Kernkraftwerke kann in 7 hintereinander gestaffelten Ebenen unterteilt werden, sogenannte elektrische Versorgungsebenen. Diese lassen sich gemäss nachfolgender Tabelle den Sicherheitsebenen der gestaffelten Sicherheitsvorsorge zuordnen. Es ist zu beachten, dass diese Tabelle lediglich eine vereinfachte Übersicht und keine exakte Zuordnung darstellt. Insbesondere ist anzumerken, dass die in der Tabelle aufgeführten Stromquellen Wechselstromquellen sind. Je nach Notwendigkeit und angeschlossenen Verbrauchern sind den einzelnen Versorgungsebenen auch batteriegestützte Versorgungen, das heisst Gleichstromversorgungen beziehungsweise unterbrechungsfreie Wechselstromversorgungen (mit Gleichstromteil zur Energie-Zwischenspeicherung mittels Batterien) zugeordnet. Diese jeweils von den genannten Wechselstromversorgungen angespeisten Unterversorgungen sind in der Richtlinie im Kapitel 7.12.4 behandelt.

Sicherheitsebene der gestaffelten Sicherheitsvorsorge	**elektrische Versorgungsebene**	**Stromquellen**	Behandlung in Richtlinie ENSI-G02
Sicherheitsebenen 1 und 2 betriebliche Versorgung des Eigenbedarfs inklusive betriebliche Versorgung der Notstromanlage, der Notstand-Notstromanlage und der Sicherheitssysteme	**elektrische Versorgungsebene 1**	externer Hauptnetz-Anschluss, Versorgung ab Blockgenerator oder Hauptnetz	Kap. 7.12.1 Bst. b
	elektrische Versorgungsebene 2	Eigenbedarfsversorgung durch Blockgenerator im Inselbetrieb[5]	Kap. 7.12.1 Bst. b und c
	elektrische Versorgungsebene 3	zweiter externer Anschluss (z. B. Reservenetz), Versorgung ab Reservenetz	Kap. 7.12.1 Bst. b
Sicherheitsebene 3 Stromversorgungen von Sicherheits- und Notstandsystemen	**elektrische Versorgungsebene 4**	Notstromversorgung	Kap. 7.12.1 Bst. d und e
	elektrische Versorgungsebene 5	gebunkerte Notstandversorgung	Kap. 7.12.1 Bst. d und e
Sicherheitsebenen 4a und 4b Stromversorgung notwendiger Verbraucher beim Totalverlust der elektrischen Versorgungsebenen 1 bis 5	**elektrische Versorgungsebene 6**	lokal vorhandene mobile AM-Notstromaggregate, Aufbau einer Verbindung zu einem externen Netz	Kap. 7.12.1 Bst. f und g
	elektrische Versorgungsebene 7	extern gelagerte AM-Notstromaggregate	Kap. 7.12.1 Bst. f

Zu Bst. g: Die Verbindung zu einem externen Netz soll es ermöglichen, dass langfristig die Stromversorgung durch die Notstromanlage und Notstand-Notstromanlage durch das externe Netz abgelöst werden kann. Die Verbindung zu einem externen Netz hat gegenüber den treibstoffversorgten Anlagen den Vorteil, dass sie vom Treibstoff und seinem Nachschub unabhängig ist.

5.6.12.2 Kapitel 7.12.3 „Notstromversorgung“

Zu Bst. c: Die Notstromanlage und die Notstand-Notstromanlage müssen nicht nur die unter Bst. b geforderte, notwendige Leistung erbringen. Sie müssen diese auch unter Einhaltung der notwendigen elektrischen Bedingungen (z. B. geringe Frequenz- und Spannungs-

[5] Der Blockgenerator oder die Blockgeneratoren des Kraftwerks versorgen nach einem Lastabwurf auf Eigenbedarf via den oder die Eigenbedarfstransformatoren nur noch die eigenen elektrischen Verbraucher des Kraftwerks. Diese Betriebsart wird als Inselbetrieb bezeichnet.

schwankungen) erbringen, damit die Verbraucher nicht wegen ungenügender Qualität der Stromversorgung ausfallen.

Zu Bst. d: Die Notstromanlage und die Notstand-Notstromanlage sind jede für sich redundant aufzubauen, was heisst, dass jede für sich auch bei einem Einzelfehler verfügbar bleiben muss. Die Notstand-Notstromanlage ist aber nicht redundant zur Notstromanlage auszulegen. Sie muss also nicht den gleichen Umfang an zu versorgenden Systemen und Komponenten umfassen.

Zu Bst. e: Die Notstromanlage und die Notstand-Notstromanlage müssen für eine Betriebsdauer von 10 Tagen ausgelegt sein, was nicht gleichbedeutend ist mit 10 Tagen Volllastbetrieb. Je nach Störfallablauf reduziert sich die notwendige Belastung der Notstromanlagen. Deshalb sind nur für den ersten Tag Betriebsmittel für einen 24-stündigen Volllastbetrieb notwendig. Für weitere 6 Tage müssen Betriebsmittel vorhanden sein, die auch für den anspruchsvollsten Störfallablauf für die Not- und Nachkühlphase ausreichen.

5.6.12.3 Kapitel 7.12.4 „Unterbrechungsfreie Stromversorgung (USV)“

Zu Bst. c: Die Auslegung auf die geforderte Versorgungszeit bezieht sich auf den direkt zugeordneten Verbraucherstrang und nicht auf die Versorgung von zwei oder mehreren Verbrauchersträngen. Die geforderte Versorgungszeit von 4 Stunden leitet sich aus folgenden Punkten ab:

- Im bisherigen Regelwerk (Richtlinie HSK-R-101) wurde ein uneingeschränkter Betrieb über mehrere Stunden bei Ausfall der internen Notstromversorgung gefordert.
- Für gewisse Ausfallszenarien soll dem Personal, auch für wesentliche 0E-klassierte Ausrüstungen, genügend Zeit zur Wiederherstellung der Batterienachladung zur Verfügung stehen.

Zu Bst. d: Beispielsweise wird für die Instrumentierungen zur Überwachung des Entlastungsvorgangs sowie zur Überwachung und Registrierung der an die Umgebung abgegebenen radioaktiven Stoffe bei einer Containmentdruckentlastung eine autarke Versorgungsdauer von 100 Stunden gefordert (siehe Anhang 2, Allgemeine Auslegungsvorgaben, Bst. h).

Zu Bst. e: Technologiebedingte Reduktion der Batteriekapazität kann beispielsweise durch höhere Strombelastung und fortschreitende Alterung bedingt sein.

Zu Bst. f: Für die Entkopplung der Einspeisungen von Gleichstromverbrauchern sind Dioden zulässig.

5.6.13 Kapitel 7.13 „Elektrische Ausrüstungen und Beleuchtung“

5.6.13.1 Kapitel 7.13.1 „Spezifische Anforderungen an elektrische Ausrüstungen“

Zu Bst. a: Diese Anforderung entspricht den Vorgaben der Starkstromverordnung und nachgelagerten Verordnungen.

Zu Bst. c: Die nukleare Sicherheit hat bei der Funktionsausführung grundsätzlich Vorrang gegenüber dem Komponentenschutz (Aggregateschutz). Es ist aber nicht generell die Absicht, eine Komponente bis zu deren Versagen zu betreiben. Beispielsweise gibt es bei den Notstromdieseln Signale des Aggregateschutzes, die nicht übersteuert werden.

5.6.13.2 Kapitel 7.13.2 „Beleuchtung“

Zu Bst. a: Gute Sichtverhältnisse implizieren die Berücksichtigung ergonomischer Aspekte und die Optimierung der Lichtstärke.

Zu Bst. b und c: Die in der Richtlinie verwendeten Bezeichnungen für Notbeleuchtung, Sicherheitsbeleuchtung und Ersatzbeleuchtung richten sich nach der internationalen Norm SN EN 1838.

Zu Bst. b und f: Die grundlegenden Anforderungen an die Flucht- und Rettungswege sind in Kap. 10.2 der Richtlinie ENSI-B12 festgelegt.

Zu Bst. d: Die schweizerische Norm SN EN 1838 – entspricht der entsprechenden europäischen Norm – muss bei der Auslegung der Notbeleuchtung beachtet werden, da Normen grundsätzlich zum Regelwerk gehören und somit einzuhalten sind.

Zu Bst. g: Die für die Auslegung der Sicherheitsbeleuchtung sind insbesondere die VKF-Richtlinie 16 und 17 zu beachten. Abweichend von der entsprechenden VKF-Vorgabe muss nach Ausfall der Normalbeleuchtung die Sicherheitsbeleuchtung für mindestens eine Stunde sichergestellt sein – siehe Anforderung von Bst. h der Richtlinie. (Die aktuell gültige VKF-Richtlinie 17 verlangt nur 30 Minuten).

Zu Bst. h: Die notwendige Dauer der autonomen, batteriegestützte Versorgung der Sicherheitsbeleuchtung ist so zu bemessen, dass im Brandfall eine Flucht via Fluchtwege von jedem Anlageraum aus möglich ist, das heisst die Fluchtwege beleuchtet sind. Die Stromversorgung muss aber mindestens für eine Stunde gewährleistet sein.

Zu Bst. i: Insbesondere das Erkennen und Lesen von wesentlichen Beschriftungen, Informationen und Meldungen muss mit der Ersatzbeleuchtung weiterhin möglich sein. Beispiele von Örtlichkeiten, die eine Ersatzbeleuchtung benötigen, sind die Steuerstellen und zu bedienende Leittechnik- und Starkstromräume. Die Ersatzbeleuchtung ist auch im Störfall da wichtig, wo Instandsetzungsarbeiten, beispielsweise zur Wiederinbetriebnahme ausgefallener Dieselgeneratoren, notwendig sein kann.

Zu Bst. k: Die Erdbebenauslegung der Notbeleuchtung und die mechanische Auslegung der Normalbeleuchtung richten sich nach der Erdbebenauslegung des Anlageraumes und dessen Komponenten. Ziel ist, die mechanische Sicherheit, mechanische Integrität und den Funktionserhalt der Beleuchtungsausrüstungen zu gewährleisten. Die Ausrüstungen der Notbeleuchtung und betroffenen Ausrüstungen der Normalbeleuchtung sollen im Erdbebenfall nicht aus ihrer Befestigung herausfallen, um sicherheitstechnisch wichtige Ausrüstungen oder notwendige Tätigkeiten im Erdbebenfall nicht zu behindern.

Zu Bst. l: Der Einsatz mobiler Notstromaggregate dient der Speisung ausgewählter Notstromschienen, um zumindest zentral wichtige Teile der Notbeleuchtung wieder herzustellen.

5.6.14 Kapitel 7.14 „Lüftungstechnische Anlagen“

Zu Bst. g: Es ist beispielsweise nachzuweisen, dass ein Brand eines Aktivkohlefilters nicht zu Folgeschäden in anderen sicherheitstechnisch wichtigen Komponenten führt.

Zu Bst. k: Beanspruchungen sind beispielsweise Druck, Druckstösse, Feuchte, Temperatur, ionisierende Strahlung, Schwingungen und korrosive Stoffe.

Zu Bst. n: Diese Anforderung entspricht dem ALARA-Prinzip.

5.6.15 Kapitel 7.15 „Brennstofflagerung und -handhabung“

5.6.15.1 Kapitel 7.15.1 „Trockenlagerung“

Die Anforderungen beziehen sich auf die Trockenlagerung unbestrahlter Brennelemente.

5.6.15.2 Kapitel 7.15.2 „Nasslagerung“

Zu Bst. c: Füllstand und Temperatur müssen insbesondere auch im Störfall verfügbar sein. Deshalb müssen beide Messungen die Anforderungen der Sicherheitsebenen 1 bis 4a erfüllen.

Zu Bst. e: Anschlussstutzen im Aussenbereich werden zur Beherrschung oder Linderung von SE4-Störfällen verlangt.

Zu Bst. g: Das Leckageüberwachungssystem muss im Normalbetrieb seine Aufgabe erfüllen und ist deshalb als Betriebssystem auszulegen.

Zu Bst. n: Diese Anforderung gilt sinngemäss auch für spezielle, zum Abstellen von Transportbehälter vorhandene Lagerbecken, falls diese ausserhalb des eigentlichen Brennelementlagerbeckens angeordnet sind.

Zu Bst. o: Brennelementlager sind gegen Erdbeben ausgelegt, das heisst nach einem Erdbeben sind Brennelement-Handhabungen kurzfristig nicht notwendig. Für längerfristige Massnahmen können Notfallausrüstungen verwendet werden.

5.7 Anhang 3 „Gefilterte Druckentlastung des Primärcontainments“

5.7.1 Kapitel A3.1 „Allgemeine Auslegungsvorgaben“

Zu Bst. c: Das Druckentlastungssystem muss bei einem Druck im Containment, der zwischen Auslegungsdruck des Containments und Ansprechdruck der Berstscheibe liegt, aktiviert werden.

Zu Bst. h: Diese Anforderung geht über die entsprechenden Anforderungen für die Betriebsdauer der USV-Anlagen gemäss Kap. 4.12.4 hinaus. Die Druckentlastung des Containments bei einem Kernschmelzunfall kann nach vielen Stunden notwendig sein. Aus diesem Grunde ist es wichtig, dass auch dann noch eine Instrumentierung vorhanden ist, um die Entlastung durchführen und verfolgen zu können.

5.8 Anhang 4 „Störfallübersichtsanzeigen“

Die Tabellen mit den Störfallübersichtsanzeigen wurden von der Richtlinie ENSI-B12 (Ausgabe April 2009, Revision 1 vom 31. Oktober 2015) in die Richtlinie ENSI-G02 verschoben. Die Neuausgabe der Richtlinie ENSI-B12 vom August 2019 enthält deshalb die Störfallübersichtsanzeigen nicht mehr.

Bei den angegebenen Messbereichen handelt es sich um Richtwerte.

Anhang 1: Beispiele von Schutzzielfunktionen

Übergeordnete Schutzziele	Schutzzielfunktionen
Kontrolle der Reaktivität	Kontrolle der Änderung von Reaktivität und Leistung im Kern • inhärente Selbststabilisierung • Begrenzung von Reaktivität, Leistung und Leistungsdichte nachhaltige Beendigung der Kettenreaktion im Kern • Reaktorabschaltung • langfristiges Halten im unterkritischen Zustand Kontrolle der Reaktivität von Brennelementen (BE) ausserhalb des Reaktorkerns • Sicherstellung der Unterkritikalität bei BE-Handhabung und BE-Lagerung
Kühlung der Brennelemente	Wärmeabfuhr • Wärmeabfuhr aus dem Reaktorkern • sekundärseitige Wärmeabfuhr (DWR) • Wärmeabfuhr aus Containment • Wärmeabfuhr aus der Kondensationskammer (SWR) • Wärmeabfuhr aus BE-Lagerbecken • Wärmeabfuhr über die Kühlkette Sicherstellung des Kühlmittelinventars • Kühlmittelergänzung • Begrenzung Kühlmittelverlust • Ergänzung des BE-Beckenwassers • Begrenzung Wasserverlust aus BE-Becken Sicherstellung des sekundärseitigen Wasserinventars (DWR) • Dampferzeugerbespeisung • Minderung Wasser-/Dampfverlust aus Sekundärkreislauf Sicherstellung der Integrität kühlmittelführender Systeme • Druck- und Temperaturbegrenzung im Reaktorkühlsystem • sekundärseitige Druckbegrenzung (DWR) • Temperatur- und Druckbegrenzung im Containment • Füllstands-, Druck- und Temperaturbegrenzung in der Kondensationskammer (SWR) • Überspeisungsabsicherung Reaktorsystem • Überspeisungsabsicherung Dampferzeuger (DWR) • Druckbegrenzung Reaktorgebäude

Einschluss radioaktiver Stoffe	Einschluss des Aktivitätsinventars des Reaktorkerns • Integrität der Brennstabhülle und Stabilität der Brennelementstrukturbauteile • Integrität der druckführenden Umschliessung des Reaktorkühlmittels • Integrität des Containments Einschluss des sonstigen Aktivitätsinventars in der Anlage • Aktivitätseinschluss über lüftungstechnische Anlagen • Aktivitätseinschluss über Anlagen zur Abgasbehandlung • Aktivitätseinschluss über Anlagen zur Abwasserbehandlung • Aktivitätseinschluss über weitere kühlmittelführende Systeme
Begrenzung der Strahlenexposition	Begrenzung der Strahlenexposition innerhalb der Anlage • Kontrolle des Aktivitätsinventars und -flusses innerhalb der Anlage • baulicher Strahlenschutz • technischer Strahlenschutz • administrativer und personeller Strahlenschutz Begrenzung der Strahlenexposition in der Umgebung • Begrenzung der Ableitung und Freisetzung radioaktiver Stoffe • Umgebungsüberwachung

Anhang 2: WENRA Safety Reference Levels

Nr.	Anforderung	Abbildung im Schweizer Regelwerk
E1.1	The design basis* shall have as an objective the prevention or, if this fails, the mitigation of consequences resulting from anticipated operational occurrences and design basis accidents conditions. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed prescribed limits and are as low as reasonably achievable. *The design basis shall be reviewed and updated during the lifetime of the plant (see SRL E11.1).	Art. 4 KEG sowie Art. 7 Bst. c und d KEV Art. 123 und 125 StSV Kap. 4 ENSI-G02
E2.1	Defence-in-depth* shall be applied in order to prevent, or if prevention fails, to mitigate harmful radioactive releases. *For further information see IAEA SSR-2/1 (2012).	Art. 5 Abs. 1 KEG Art. 7 KEV Art. 1 Bst. c SR 732.112.2 Kap. 4.1 und 4.3 ENSI-G02
E2.2	The defence-in-depth concept shall be applied to provide several levels of defence including a design that provides a series of physical barriers to prevent uncontrolled releases of radioactive material to the environment, as well as a combination of safety features that contribute to the effectiveness of the barriers. The design shall prevent as far as practicable: • challenges to the integrity of the barriers; • failure of a barrier when challenged; • failure of a barrier as consequence of failure of another barrier.	Art. 5 Abs. 1 KEG Art. 7 KEV Kap. 4 ENSI-G02

E3.1	During normal operation*, anticipated operational occurrences and design basis accidents, the plant shall be able to fulfil the fundamental safety functions**: • control of reactivity, • removal of heat from the reactor core and from the spent fuel, and • confinement of radioactive material. *Normal operation includes start-up, power operation, shutting down, shutdown, maintenance, testing and refuelling. **Under the conditions specified in the following paragraphs	Art. 1 Bst. d und e sowie Art. 2 SR 732.112.2 Kap. 4.1 Bst. a ENSI-G02
E4.1	The design basis shall specify the capabilities of the plant to cope with a specified range of plant states* within the defined radiation protection requirements. Therefore, the design basis shall include the specification for normal operation, anticipated operational occurrences and design basis accidents from Postulated Initiating Events (PIEs), the safety classification, important assumptions and, in some cases, the particular methods of analysis. *Normal operation, anticipated operational occurrences and design basis accident conditions.	Art. 8 KEV Art. 1 Bst. a und b sowie Art. 4 bis 6 SR 732.112.2 Kap. 6 ENSI-G02
E4.2	A list of PIEs shall be established to cover all events that could affect the safety of the plant. From this list, a set of anticipated operational occurrences and design basis accidents shall be selected using deterministic or probabilistic methods or a combination of both, as well as engineering judgement.* The resulting design basis events shall be used to set the boundary conditions according to which the structures, systems and components important to safety shall be designed, in order to demonstrate that the necessary safety functions are accomplished and the safety objectives met. *Depending on the specific topic being under review, not all types of insights (deterministic, probabilistic or engineering judgement) may be relevant or needed.	Art. 8 KEV, Art. 4 bis 6 SR 732.112.2 Kap. 4.1 Bst. a und b ENSI-A01 Kap. 6.2 Bst. a sowie Kap. 6.3 Bst. a ENSI-G02

E4.3	The design basis shall be systematically defined and documented to reflect the actual plant.	Art. 8 und 10 bis 12, Art. 41 Abs. 1, Anhang 3 Ziff. 2 sowie Anhang 4 Ziff. 2 KEV Kap. 4.1 ENSI-A01 Kap. 5.1.3 ENSI-A03 Kap. 4 bis 7 ENSI-G02
E5.1	Internal events such as loss of coolant accidents, equipment failures, maloperation and internal hazards, and their consequential events, shall be taken into account in the design of the plant.* The list of events shall be plant specific and take account of relevant experience and analysis from other plants. *Additional information on internal hazards is provided in IAEA Safety Standards NS-G-1.7 and NS-G-1.11.	Art. 8 Abs. 2 KEV Art. 4 und 6 SR 732.112.2 Anhang 1 Kap. 2.2 VBRK Kap. 4.1 Bst. b sowie Kap. 4.7 ENSI-A01 Kap. 4.4.1.1 ENSI-A05 Kap. 6.1 und 6.2 ENSI-G02
E5.2	External hazards shall be taken into account in the design of the plant. In addition to natural hazards*, human made external hazards – including airplane crash and other nearby transportation, industrial activities and site area conditions which reasonably can cause fires, explosions or other threats to the safety of the nuclear power plant – shall as a minimum be taken into account in the design of the plant according to site specific conditions. *See Issue T.	Art. 8 Abs. 3 KEV Art. 5 SR 732.112.2 Anhang 1 Ziff. 2.2 VBRK Kap. 4.1 Bst. c sowie Kap. 4.7 ENSI-A01 Kap. 4.6.1 ENSI-A05 Kap. 6.1 und 6.3 ENSI-G02
E7.3	Criteria for the protection of the primary coolant pressure boundary shall be specified, including maximum pressure, maximum temperature, thermal- and pressure transients and stresses	Anhang 1 Kap. 2.4 und 2.5 VBRK Kap. 6.3.2.1 ENSI-G09 Kap. 5.3 ENSI-G11 Kap. 7.2 Bst. d ENSI-G02
E7.4	If applicable, criteria in E7.3 shall be specified as well for protection of the secondary coolant system.	Kap. 6.3.2.1 ENSI-G09
E7.5	Criteria shall be specified for protection of containment, including temperatures, pressures and leak rates.	Kap. 6.3.2.1 ENSI-G09 Kap. 7.7.1 Bst. b und c ENSI-G02
E8.6	Any failure, occurring as a consequence of a postulated initiating event, shall be regarded to be part of the original PIE.	Kap. 4.4 Bst. a ENSI-A01 Kap. 6.1 Bst. e ENSI-G02
E9.1	The fail-safe principle shall be considered in the design of systems and components important to safety.	Art. 10 Abs. 1 Bst. h KEV

E9.2	A failure in a system intended for normal operation shall not affect a safety function.	Kap. 5.2.1 Bst. a sowie Kap. 5.2.2 Bst. b ENSI-G02 Kap. 7.10.1 Bst. b ENSI-G02
E9.3	Activations and control of the safety functions shall be automated or accomplished by passive means such that operator action is not necessary within 30 minutes of the initiating event. Any operator actions required by the design within 30 minutes of the initiating event shall be justified.* *The control room staff has to be given sufficient time to understand the situation and take the correct actions. Operator actions required by the design within 30 min after the initiating event have to be justified and sup-ported by clear documented procedures that are regularly exercised in a full scope simulator.	Art. 10 Abs. 1 Bst. f KEV Kap. 4.4 Bst. h ENSI-A01 Kap. 5.2.2.6 Bst. a ENSI-G02
E9.4	The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components*, redundancy, diversity**, physical and functional separation and isolation. *Proven by experience under similar conditions or adequately tested and qualified. **The potential for common cause failure, including common mode failure, shall be appropriately considered to achieve the necessary reliability.	Art. 7 Bst. a KEV Art. 10 Bst. a bis i KEV Kap. 5.1 (insbesondere Bst. b und c) und Kap. 5.2.2 (insbesondere Kap. 5.2.2.2 bis 5.2.2.4) ENSI-G02
E9.5	For sites with multiple units, appropriate independence between them shall be ensured.* *The possibility of one unit supporting another could be considered as far as this is not detrimental for safety.	Kap. 5.1 Bst. h sowie Kap. 5.2.2 Bst. h ENSI-G02
E9.6	The means for shutting down the reactor shall consist of at least two diverse systems.	Kap. 5.5.1 und 5.5.2 ENSI-G20 Kap. 7.1 Bst. b ENSI-G02
E9.7	At least one of the two systems shall, on its own, be capable of quickly* rendering the nuclear reactor sub critical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure. *Within 4-6 seconds, i.e. scram system.	Kap. 5.5.1 ENSI-G20 Kap. 7.1 Bst. a ENSI-G02

E9.9	Means for removing residual heat from the core after shutdown and from spent fuel storage, during and after anticipated operational occurrences and design basis accidents, shall be provided taking into account the assumptions of a single failure and the loss of off-site power.	Art. 8 Abs. 4 KEV Kap. 4.2 sowie Kap. 4.4 Bst. c ENSI-A01 Kap. 7.6 ENSI-G02
E9.10	A containment system shall be provided in order to ensure that any release of radioactive material to the environment in a design basis accident would be below prescribed limits. This system shall include: • leaktight structures covering all essential parts of the primary system; • associated systems for control of pressures and temperatures; • features for isolation; • features for the management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.	Art. 5 Abs. 1 und 2 KEG Art. 7 Bst. c und d KEV Kap. 7.7 ENSI-G02 Kap. 7.11.3 Bst. d zusammen mit Anhang 4 ENSI-G02
E9.11	Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a design basis accident. These lines shall be fitted with at least two containment isolation valves arranged in series. Isolation valves shall be located as close to the containment as is practicable.	Kap. 7.7.1 Bst. f Ziff. 1 sowie Kap. 7.9.1 Bst. e ENSI-G02
E9.12	Each line that penetrates the containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve. This valve shall be outside the containment and located as close to the containment as practicable.	Kap. 7.7.1 Bst. f Ziff. 2 ENSI-G02

E10.1	Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems, the containment, and the state of the spent fuel storage. Instrumentation shall also be provided for obtaining any information on the plant necessary for its reliable and safe operation, and for determining the status of the plant in design basis accidents. Provision shall be made for automatic recording* of measurements of any derived parameters that are important to safety. *By computer sampling and/or print outs.	Kap. 8.3.5 und Kap. 10.3 ENSI-B12 Kap. 5.4 ENSI-G20, ENSI-G13 Kap. 7 ENSI-G09 Kap. 7.11 ENSI-G02
E10.2	Instrumentation shall be adequate for measuring plant parameters and shall be environmentally qualified for the plant states concerned.	Kap. 7.11 ENSI-G02 (speziell zur Qualifizierung: Kap. 7.11.1 Bst. a) Kap. 8.3.5 ENSI-B12
E10.3	A main control room shall be provided from which the plant can be safely operated in all its operational states, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of anticipated operational occurrences and design basis accidents.	Kap. 7.9.ENSI-G02 Kap. 10.1 ENSI-B12
E10.4	Devices shall be provided to give in an efficient way visual and, if appropriate, also audible indications of operational states and processes that have deviated from normal and could affect safety. Ergonomic factors shall be taken into account in the design of the main control room. Appropriate information shall be available to the operator to monitor the effects of the automatic actions.	Kap. 7.9.2 ENSI-G02
E10.5	Special attention shall be given to identifying those events, both internal and external to the main control room, which may pose a direct threat to its continued operation, and the design shall provide for reasonably practicable measures to minimize the effects of such events.	Kap. 7.9.1 Bst. b und d ENSI-G02

E10.6	For times when the main control room is not available, there shall be sufficient monitoring and control equipment available, preferably at a single location that is physically, electrically and functionally separate from the main control room, so that, if the main control room is unavailable, the reactor can be placed and maintained in a shut-down state, residual heat can be removed from the reactor and spent fuel storage, and the essential plant parameters, including the conditions in the spent fuel storages, can be monitored.	Kap. 7.9.1 Bst. b und c sowie Anhang 4 ENSI-G02
E10.7	Redundancy and independence designed into the protection system shall be sufficient at least to ensure that: • no single failure results in loss of protection function; and • the removal from service of any component or channel does not result in loss of the necessary minimum redundancy.	Kap. 5.2.2 und Kap. 7.10 ENSI-G02 Kap. 5 HSK-R-46
E10.8	The design shall permit all aspects of functionality of the protection system, from the sensor to the input signal to the final actuator, to be tested in operation. Exceptions shall be justified.	Art. 10 Abs. 1 Bst. e KEV Kap. 5.2.2.5 ENSI-G02 Kap. 7.10.1 Bst. k, l und m ENSI-G02
E10.9	The design of the reactor protection system shall minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operation and anticipated operational occurrences. Furthermore, the reactor protection system shall not prevent operators from taking correct actions if necessary in design basis accidents.	Kap. 5.2.2.6 ENSI-G02, Kap. 7.10.2 ENSI-G02 Kap. 5.1 HSK-R-46
E10.11	It shall be ensured that the emergency power supply is able to supply the necessary power to systems and components important to safety, in any operational state or in a design basis accident, on the assumption of a single failure and the coincidental loss of off-site power.	Kap. 7.12.3 Bst. a, b und d ENSI-G02

F1.1	As part of defence in depth, analysis of Design Extension Conditions (DEC) shall be undertaken with the purpose of further improving the safety of the nuclear power plant by: • enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis, • minimising radioactive releases harmful to the public and the environment as far as reasonably practicable, in such events or conditions.	Art. 4 Abs. 1 und 3 KEG Art. 7 Bst. d sowie Art. 8 Abs. 5 KEV Kap. 5 ENSI-A01 Kap. 4 und 5 ENSI-A05 Kap. 6.1 ENSI-A06 Kap. 4.1, 4.3 und 5.2.3 ENSI-G02
F1.2	There are two categories of DEC: • DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved; • DEC B with postulated severe fuel damage. The analysis shall identify reasonably practicable provisions that can be implemented for the prevention of severe accidents. Additional efforts to this end shall be implemented for spent fuel storage with the goal that a severe accident in such storage becomes extremely unlikely to occur with a high degree of confidence. In addition to these provisions, severe accidents shall be postulated for fuel in the core and, if not extremely unlikely to occur with a high degree of confidence, for spent fuel in storage, and the analysis shall identify reasonably practicable provisions to mitigate their consequences.	Kap. 5 und 4 ENSI-A05 Kap. 5 ENSI-A01 Kap. 8.3 ENSI-B12 Kap. 4.3 und 5.2.3 sowie Anhang 2 ENSI-G02

F4.1	In DEC A, it is the objective that the plant shall be able to fulfil, the fundamental safety functions: • control of reactivity*, • removal of heat from the reactor core and from the spent fuel, and • confinement of radioactive material. In DEC B, it is the objective that the plant shall be able to fulfil confinement of radioactive material. To this end removal of heat from the damaged fuel shall be established.** *Preferably, this safety function shall be fulfilled at all times; if it is lost, it shall be re-established after a transient period. **For the fulfilment (or re-establishment) of the fundamental safety functions in DEC A and DEC B, the use of mobile equipment on-site can be taken into account, as well as support from off-site, with due consideration for the time required for it to be available.	Art. 4 Abs. 1 und 3 KEG Art. 7 Bst. d KEV Kap. 8.3.1 ENSI-B12 Kap. 4.1 Bst. c und d ENSI-G02
F4.2	It shall be demonstrated that SSCs* (including mobile equipment and their connecting points, if applicable) for the prevention of severe fuel damage or mitigation of consequences in DEC have the capacity and capability and are adequately qualified to perform their relevant functions for the appropriate period of time. *SSCs including their support functions and related instrumentation	Art. 4 Abs. 1 und 3 KEG Art. 7 Bst. d KEV Kap. 5.2.3.1 und 5.2.3.2 ENSI-G02
F4.3	If accident management relies on the use of mobile equipment, permanent connecting points, accessible (from a physical and radiological point of view) under DEC, shall be installed to enable the use of this equipment. The mobile equipment, and the connecting points and lines shall be maintained, inspected and tested.	Kap. 5.2.3.2 Bst. d und e ENSI-G02
F4.4	A systematic process shall be used to review all units relying on common services and supplies (if any), for ensuring that common resources of personnel, equipment and materials expected to be used in accident conditions are still effective and sufficient for each unit at all times. In particular, if support between units at one site is considered in DEC, it shall be demonstrated that it is not detrimental to the safety of any unit.	Kap. 4 ENSI-B12 Kap. 5.2.3.2 Bst. g ENSI-G02

F4.5	The NPP site shall be autonomous regarding supplies supporting safety functions for a period of time until it can be demonstrated with confidence that adequate supplies can be established from off site.	Kap. 5 Bst. i ENSI-A01 Kap. 5.2.3 Bst. f und Kap. 5.2.3.2 Bst. b ENSI-G02
F4.6	In design extension conditions, sub-criticality of the reactor core shall be ensured in the long term* and in the fuel storage at any time. *It is acknowledged that in case of DEC B, sub-criticality might not be guaranteed during core degradation and later on during some time in a fraction of the corium.	Kap. 5.1 Bst. d und f ENSI-G20 Kap. 6.5.3 Bst. a, b und c ENSI-G20 Kap. 7.1 Bst. a und b ENSI-G02 Kap. 7.15 Bst. a ENSI-G02
F4.7	There shall be sufficient independent and diverse means including necessary power supplies available to remove the residual heat from the core and the spent fuel. At least one of these means shall be effective after events involving external hazards more severe than design basis events.	Art. 7 Bst. d KEV Kap. 5 Bst. i ENSI-A01 Kap. 7.6, Kap. 7.12.3 und Kap. 7.15.2 ENSI-G02
F4.8	Isolation of the containment shall be possible in DEC. For those shutdown states where this cannot be achieved in due time, severe core damage shall be prevented with a high degree of confidence. If an event leads to bypass of the containment, severe core damage shall be prevented with a high degree of confidence.	Art. 7, Bst. d KEV Kap. 7.7.1 Bst. f und g ENSI-G02
F4.9	Pressure and temperature in the containment shall be managed.	Art. 7 Bst. d KEV Kap. 7.7.1 Bst. b ENSI-G02 Kap. 7.7.1 Bst. h ENSI-G02 Anhang 3 ENSI-G02
F4.10	The threats due to combustible gases shall be managed.	Art. 7 Bst. d KEV Kap. 7.7 Bst. c und d ENSI-G02
F4.11	The containment shall be protected from overpressure. If venting is to be used for managing the containment pressure, adequate filtration shall be provided.	Art. 7, Bst. d KEV Kap. 7.7.1 Bst. h mit Anhang 3 ENSI-G02
F4.12	High pressure core melt scenarios shall be prevented.	Art. 7, Bst. d KEV Kap. 7.4 Bst. a Ziff. 2 ENSI-G02
F4.13	Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.	Art. 7, Bst. d KEV Kap. 7.7.1 Bst. i ENSI-G02

F4.14	In DEC A, radioactive releases shall be minimised as far as reasonably practicable. In DEC B, any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable to: (a) allow sufficient time for protective actions (if any) in the vicinity of the plant; and (b) avoid contamination of large areas in the long term	Art. 7 Bst. d KEV Kap. 4.1 Bst. c und d ENSI-G02
F4.15	Adequately qualified instrumentation shall be available for DEC for determining the status of plant (including spent fuel storage) and safety functions as far as required for making decisions.* *This refers to decisions concerning measures on-site as well as, in case of DEC B, off-site.	Art. 7, Bst. d KEV Kap. 7.11 und Anhang 4 ENSI-G02 Kap. 8.3.5 ENSI-B12
F4.16	There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations.	Art. 7 Bst. d KEV Kap. 7.9.1 ENSI-G02 Kap. 10.1 ENSI-B12
F4.17	Adequate power supplies during DEC shall be ensured considering the necessary actions and the timeframes defined in the DEC analysis, taking into account external hazards.	Art. 7, Bst. d KEV Kap. 7.12 ENSI-G02
F4.18	Batteries shall have adequate capacity to provide the necessary DC power until recharging can be established or other means are in place.	Art. 7 Bst. d KEV Kap. 7.12.4 Bst. c, d und e ENSI-G02
LM2.6	Possibilities for one unit, without compromising its safety, supporting another unit on the site shall be covered by the set of procedures and guidelines.	Kap. 8.1 Bst. b ENSI-B12 Kap. 5.2.3.2 Bst. g ENSI-G02
LM3.4	EOPs for design basis accidents shall rely on adequately qualified equipment and instrumentation. EOPs for DEC and SAMGs shall primarily rely on adequately qualified equipment.	Kap. 8.2.2 Bst. d Ziff. 2, Kap. 8.3.3, Kap. 8.3.5 und Kap. 10.3.1 Bst. a ENSI-B12 Anhang 2 ENSI-G01 Kap. 7.11 ENSI-G02
LM3.5	The set of procedures and guidelines shall consider the anticipated on-site conditions, including radiological conditions, associated with the accident conditions they are addressing and the initiating event or hazard that might have caused it.	Kap. 8.2.1 Bst. g und Kap. 8.3.4 Bst. g ENSI-B12 Kap. 5.2.3 Bst. c ENSI-G02

R3.7	Arrangements to support on-site actions shall be in place with considerations for large-scale destruction of infrastructure in the vicinity of the site due to external hazards.	Kap. 10.1 Bst. f und g ENSI-B12 Kap. 5.2.3.2 ENSI-G02
R4.4	Instruments, tools, equipment, documentation, and communication systems for use in emergencies (including necessary mobile equipment and consumables such as fuel, lubrication oil etc.), whether located on-site or off-site, shall be stored, maintained, tested and inspected sufficiently frequently so that they will be available and operational during DBA and DEC. Access to these storage locations shall be possible even in case of extensive infrastructure damage.	Kap. 10.3.1 Bst. c und d, Kap. 10.4.1 Bst. i sowie Kap. 10.5 Bst. a ENSI-B12 Kap. 5.2.3 Bst. a ENSI-G02
S1.1	The licensee shall implement the defence in depth principle to fire protection, providing measures to prevent fires from starting, to detect and extinguish quickly any fires that do start and to prevent the spread of fires and their effects in or to any area that may affect safety.* *In this context, safety refers to all sources of nuclear safety risk, including radioactive waste facilities.	Kap. 6.2.1 und 6.3.5 ENSI-G02 Kap. 4.2 ENSI-G18
S5.1	In order to prevent fires, procedures shall be established to control and minimize the amount of combustible materials and minimize the potential ignition sources that may affect items important to safety. In order to ensure the operability of the fire protection measures, procedures shall be established and implemented. They shall include inspection, maintenance and testing of fire barriers, fire detection and extinguishing systems.	Kap. 6.2.1 und 6.3.5 ENSI-G02 Kap. 4.2 Bst. g und Kap. 11.1 ENSI-G18

T5.1	Protection shall be provided for design basis events.* A protection concept** shall be established to provide a basis for the design of suitable protection measures. *If the hazard levels of RL T4.2 for seismic hazards were not used for the initial design basis of the plant and if it is not reasonably practicable to ensure a level of protection equivalent to a reviewed design basis, methods such as those mentioned in IAEA NS-G-2.13 may be used. This shall quantify the seismic capacity of the plant, according to its actual condition, and demonstrate the plant is protected against the seismic hazard established in RL T4.2. **A protection concept, as meant here, describes the overall strategy followed to cope with natural hazards. It shall encompass the protection against design basis events, events exceeding the design basis and the links into EOPs and SAMGs.	Kap. 6.3 ENSI-G02 Kap. 8.3.3 ENSI-B12
T5.2	The protection concept shall be of sufficient reliability that the fundamental safety functions are conservatively ensured for any direct and credible indirect effects of the design basis event.	Kap. 4.6 und 4.8 ENSI-A01 Kap. 4.1, 4.3, 5.1, 5.2.2 sowie 6.1 und 6.3 ENSI-G02

T5.3	The protection concept shall: (a) apply reasonable conservatism providing safety margins in the design; (b) rely primarily on passive measures as far as reasonable practicable; (c) ensure that measures to cope with a design basis accident remain effective during and following a design basis event; (d) take into account the predictability and development of the event over time; (e) ensure that procedures and means are available to verify the plant condition during and following design basis events; (f) consider that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures; (g) ensure that sufficient resources remain available at multi-unit sites considering the use of common equipment or services; (h) not adversely affect the protection against other design basis events (not originating from natural hazards).	(a) Kap. 5.1 Bst. e ENSI-G02 (b) Kap. 5.2.3.1 Bst. d ENSI-G02 (c) Kap. 5.1 Bst. b ENSI-G02 (d) Kap. 4.4.5 Bst. d ENSI-A01 (e) Kap. 8.2 ENSI-B12 (f) Kap. 5.2.3 ENSI-G02 (g) Kap. 5.2.3, Kap. 5.1 Bst. h, Kap. 5.2.2. Bst. h sowie Kap. 5.2.3.2 Bst. d und g ENSI-G02 (h) Kap. 6.4 ENSI-A06
T5.6	During long-lasting natural events, arrangements for the replacement of personnel and supplies shall be available.	Kap. 4.1 Bst. f ENSI-B12 Kap. 5.2.2 Bst. e sowie Kap. 5.2.3.2 Bst. b ENSI-G02

T6.3	When assessing the effects of natural hazards included in the DEC analysis, and identifying reasonably practicable improvements related to such events, analysis shall, as far as practicable, include: (a) demonstration of sufficient margins to avoid “cliff-edge effects” that would result in loss of a fundamental safety function; (b) identification and assessment of the most resilient means for ensuring the fundamental safety functions; (c) consideration that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures; (d) demonstration that sufficient resources remain available at multi-unit sites considering the use of common equipment or services; (e) on-site verification (typically by walkdown methods).	(a) Kap. 6.2 ENSI-A06 Kap. 5 Bst. b und h ENSI-A01 (b) Kap. 6.1, 6.2, 6.3.1, 6.5 und 6.6.1 ENSI-A06 (c) Kap. 5.2.2 Bst. e sowie Kap. 5.2.3.2 Bst. a und b ENSI-G02 (d) Kap. 5.1 Bst. h, Kap. 5.2.2 Bst. h sowie Kap. 5.2.3.2 Bst. d und g ENSI-G02 (e) Kap. 4.6.2 bis 4.6.5 ENSI-A05