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

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

Ausgabe Juli 2009

Erläuterungsbericht zur Richtlinie **ENSI-A01/d**

Inhalt

Erläuterungsbericht zur Richtlinie ENSI-A01/d

1 Einleitung

1.1 Veranlassung zur Richtlinie

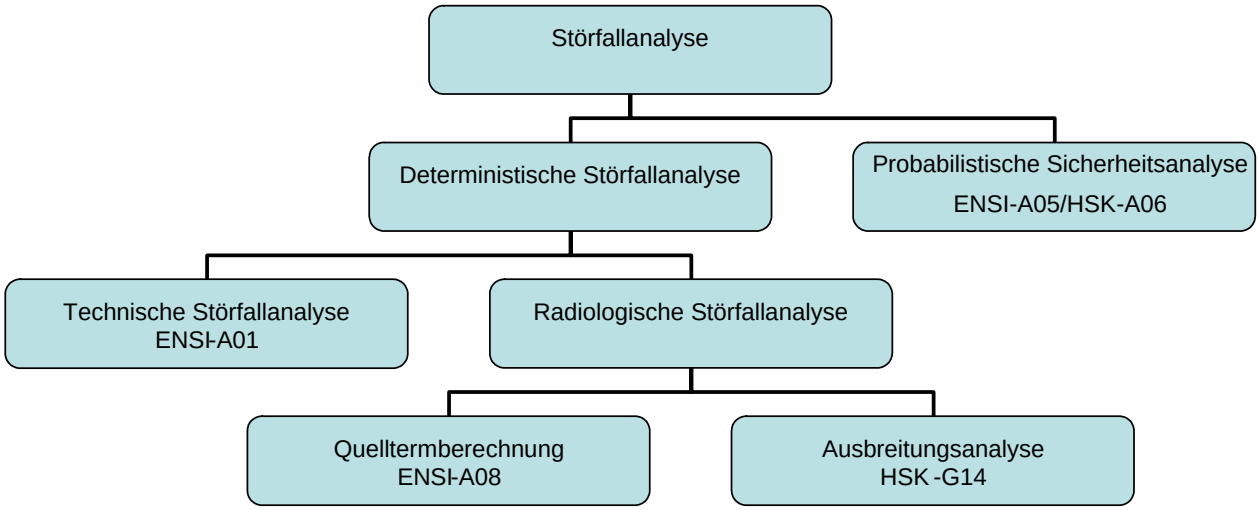
Am 1. Februar 2005 ist die neue Kernenergiegesetzgebung (Kernenergiegesetz vom 21.3.2003, SR 732.1, KEG; Kernenergieverordnung vom 10.12.2004, SR 732.11, KEV) in Kraft getreten. Gestützt auf Art. 8 Abs. 6 KEV wurde die Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen (SR 732.112.2) erlassen. Diese Verordnung legt fest, welche Gefährdungsannahmen zu treffen und nach welchen Kriterien diese zu bewerten sind. Die Aufsichtsbehörde wird dort beauftragt, die Anforderungen an die deterministische Störfallanalyse in Richtlinien zu regeln (Art. 2 Abs. 4). Mit der Richtlinie ENSI-A01 wird diesem Auftrag für die technische Störfallanalyse Rechnung getragen. Für die radiologische Störfallanalyse gelten die Richtlinien ENSI-A08 und ENSI-G14.

1.2 Zweck von Störfallanalysen

Bei der Nutzung der Kernenergie ist Vorsorge gegen eine unzulässige Freisetzung radioaktiver Stoffe sowie gegen eine unzulässige Bestrahlung von Personen im Normalbetrieb und bei Störfällen zu treffen (Art. 4 Abs. 1 KEG). Anforderungen an die Schutzmassnahmen gegen Störfälle werden in Art. 8 KEV konkretisiert. Der Nachweis des ausreichenden Schutzes gegen Störfälle ist mittels einer Störfallanalyse zu erbringen (Art. 2 Abs. 1 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen). Störfallanalysen sind im Rahmen von Bewilligungen und von Freigaben für Kernanlagen (Anhang 4 KEV) einzureichen. Ihre Aktualität ist nach der Betriebsaufnahme bei Anlageänderungen, bei Periodischen Sicherheitsüberprüfungen (PSÜ), bei neuen Gefährdungsannahmen (Art. 13 Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen) sowie bei der Umsetzung von Betriebserfahrungen und bei Änderungen des Standes von Wissenschaft und Technik (SWT) zu überprüfen und zu bewerten (Art. 33 ff. KEV).

1.3 Struktur der Störfallanalyse

Um den Nachweis des ausreichenden Schutzes zu erbringen, sind die möglichen Störfallabläufe mit unterschiedlichen Methoden zu analysieren. Der Zusammenhang zwischen den verschiedenen Teilen der Störfallanalyse ist im unten stehenden Bild dargestellt.



Mit der deterministischen Störfallanalyse ist nachzuweisen, dass ein abdeckendes Spektrum von Auslegungsstörfällen durch die Schutzmassnahmen wirksam und zuverlässig beherrscht wird. Die Ergebnisse der technischen Störfallanalyse dienen als Grundlage für die radiologische Störfallanalyse (ENSI-A08 und HSK-G14). Ob die Schutzmassnahmen gegen Störfälle angemessen und ausgewogen sind, wird zudem mit Hilfe einer probabilistischen Sicherheitsanalyse bewertet (ENSI-A05, HSK-A06).

1.4 Aufbau der Richtlinie

Die Richtlinie ist in 5 Kapitel unterteilt und enthält 3 Anhänge. Kapitel 1 ist für alle Richtlinien der HSK identisch; es beschreibt die Funktion und den Stellenwert von Richtlinien. Gegenstand und Geltungsbereich der Richtlinie werden in Kapitel 2 festgelegt. In Kapitel 3 werden die Bestimmungen aufgeführt, auf welche sich die Richtlinie stützt. Kapitel 4 legt fest, wie Auslegungsstörfälle technisch zu analysieren sind (Bestimmung der Häufigkeit von Störfällen, Ereignisspektrum, Einzelfehler, Berechnungsprogramme, Anlagemodelle, Anlageverhalten). Kapitel 5 macht Vorgaben für die technische Analyse auslegungsüberschreitender Störfälle. In den Anhängen werden Begriffe definiert sowie der Umfang der Analysen festgelegt (auslösende Ereignisse, die mindestens zu analysieren beziehungsweise für die nicht zwingend Störfallanalysen durchzuführen sind).

2 Erläuterungen einzelner Bestimmungen

2.1 Übersicht über den Inhalt

Die Richtlinie regelt Umfang, Methodik und Randbedingungen der technischen Störfallanalyse. Unter technischer Störfallanalyse wird die Analyse des technischen Anlageverhaltens bei Störfällen verstanden. Darauf basiert die radiologische Analyse, die Gegenstand weiterer Richtlinien des ENSI ist (ENSI-A08 Berechnung von Quelltermen (noch nicht veröffentlicht), HSK-G14 Berechnung der Strahlenexposition). Die Methodik der probabilistischen Sicherheitsanalyse wird in der Richtlinie ENSI-A05 geregelt, die Anwendungen der probabilistischen Sicherheitsanalyse in der HSK-A06.

2.2 Gegenstand und Geltungsbereich (Kapitel 2)

Die Anforderungen an die technische Störfallanalyse in der Richtlinie ENSI-A01 gelten für Kernanlagen in der Schweiz. Da sie nicht auf geologische Tiefenlager anwendbar sind, sind diese davon ausgenommen. Die Richtlinie ENSI-A01 ist ebenfalls nicht anwendbar auf die Eignungskriterien für geologische Tiefenlager. Diese werden in der Rahmenbewilligung festgelegt (Art. 14 Abs. 1 Bst. f Ziff. 1 KEG).

2.3 Rechtliche Grundlagen (Kapitel 3)

Die HSK wird beauftragt, Anforderungen an die Störfallanalyse in Richtlinien zu regeln. Die massgeblichen Bestimmungen für den Erlass dieser Richtlinie sind:

a. In Art. 94 Abs. 8 StSV wird die Aufsichtsbehörde beauftragt, im Einzelfall die Methodik und Randbedingungen für die Störfallanalyse festzulegen.

b. In Art. 2 Abs. 4 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen wird die Aufsichtsbehörde beauftragt, die Anforderungen an die deterministische Störfallanalyse in Richtlinien zu regeln.

Der in Art. 2 Abs. 4 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen geregelte Auftrag geht weiter, indem nicht nur die Methodik und die Randbedingungen, sondern auch der Umfang der deterministischen Störfallanalyse zu regeln sind.

2.4 Technische Analyse von Auslegungsstörfällen (Kapitel 4)

In diesem Kapitel werden die Rahmenbedingungen definiert, die im Rahmen der Auslegung der Kernanlage für die technische Analyse der Störfallabläufe und deren Auswirkungen auf die Anlage von Bedeutung sind. Die Störfallanalyse umfasst die Verwendung von zuverlässigen und verifizierten Berechnungsprogrammen, physikalischen Modellen sowie von Anlage-

modellen und -daten. Dabei sind konservative Annahmen zu treffen, um sicherzustellen, dass die technische Störfallanalyse ein umhüllendes Spektrum der Auslegungsstörfälle abdeckt.

2.4.1 Bestimmung der Störfallhäufigkeit (Kapitel 4.1)

Die Störfallhäufigkeit, welche für die Zuordnung der Störfallabläufe massgebend ist (Art. 3 Abs. 1 Bst. c der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen) wird bestimmt, indem die Eintrittshäufigkeit eines auslösenden Ereignisses pro Jahr mit der Wahrscheinlichkeit eines zusätzlichen Einzelfehlers multipliziert wird (Kap. 4.1.1 Bst. a). Falls die Zuordnung zu einer Störfallkategorie nicht eindeutig ist, ist der Störfall im Sinne der Vorsicht der tieferen Kategorie (mit den strengeren Anforderungen) zuzuweisen (Kap. 4.4.1 Bst. c). Die Quellen der Grunddaten, welche für die Bestimmung der Eintrittshäufigkeit eines auslösenden Ereignisses unter Berücksichtigung des dabei herrschenden Betriebszustandes anzuwenden sind, sind anzugeben (Kap. 4.1.2), ebenfalls die Art der Festlegung der Wahrscheinlichkeit eines Einzelfehlers (Kap. 4.1.3). Grundsätzlich ist die Wahrscheinlichkeit eines Einzelfehlers mit einem Wert von 0,1 anzunehmen. Da dieser Wert im Lichte der Erfahrungen mit den anlagespezifischen PSA eher konservativ ist, wird die Möglichkeit offen gelassen, einen kleineren Wert – bis minimal 0,01 – anzunehmen, allerdings nur dann, wenn die Betriebserfahrungen zeigen, dass eine solche Annahme zulässig ist.

2.4.2 Ereignisspektrum und Art des Einzelfehlers (Kapitel 4.2)

Um zu zeigen, dass die grundlegenden Schutzziele nach Art. 1 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen eingehalten werden, ist mindestens ein umhüllendes Spektrum auslösender Ereignisse und Störfallabläufe zu betrachten (Bst. a). Das gesamte zu analysierende Störfallspektrum umfasst die der Auslegung zugrunde gelegten Ereignisse, hingegen nicht Einwirkungen Dritter. Die Untersuchung der Störfallabläufe mit den strengsten Anforderungen an die Einhaltung der Schutzziele ist ein besonderes Merkmal der technischen Störfallanalyse (Bst. b). Das zu analysierende Störfallspektrum ergibt sich aus anlagespezifisch anzunehmenden auslösenden Ereignissen (Bst. a). Die insbesondere zu analysierenden Störfälle und deren mindestens anzunehmenden Auswirkungen sind in Art. 4 und 5, zusätzlich für Kernkraftwerke mit Leichtwasserreaktoren in Art. 6 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes gegen Störfälle in Kernanlagen festgehalten. Der Mindestumfang der technisch zu analysierenden auslösenden Ereignisse ist in Anhang 2 nur für Druck- und Siedewasserreaktoren angegeben. Dies deshalb, weil alle heute in Betrieb stehenden Reaktoren Leichtwasserreaktoren sind und in absehbarer Zeit in der Schweiz keine anderen Reaktortypen zu erwarten sind.

Andere Ereignisse mit Ursprung innerhalb und ausserhalb der Kernanlagen benötigen keine technische Störfallanalyse, falls gezeigt wird, dass ihre Auswirkungen geringer sind als diejenigen, die aus den analysierten Störfällen resultieren (Anhang 3).

Es ist nachzuweisen, dass Störfälle auch dann beherrscht werden, wenn zusätzlich und unabhängig vom auslösenden Ereignis ein Einzelfehler auftritt (Kap. 4.2.2). Es ist dabei der schwerwiegendste Einzelfehler für das jeweilige Ereignis anzunehmen (Kap. 4.2.2. Bst. c).

2.4.3 Berechnungsprogramme und Anlagemodelle (Kapitel 4.3)

Die Anforderungen an die Modellierung der Anlage und an die Berechnungsprogramme sowie an deren Anwendung werden festgelegt. Die angewendeten Berechnungsprogramme und Anlagemodelle sind wenn möglich durch Experiment und Vergleich mit bereits anerkannten Methoden zu verifizieren und zu validieren (Bst. b).

In der Vergangenheit wurden für die Störfallanalysen ausschliesslich konservativ abdeckende Modellparameter und konservative Anfangsbedingungen verwendet. Das führte teilweise dazu, dass Störfallabläufe nicht richtig vorausberechnet wurden, dass unrealistische Zeitbereiche vorausbestimmt wurden und physikalische Phänomene unberücksichtigt blieben. Aufgrund dieser Mängel und der aktuellen Ausgereiftheit der sog. „best estimate codes“ sind nun derartige Programme anzuwenden. Zudem sind angemessene konservative Eingabedaten zu verwenden und Sensitivitätsstudien durchzuführen.

Die Dokumentation der Berechnungsprogramme und Anlagemodelle ist notwendig (Bst. g).

2.4.4 Anlageverhalten (Kapitel 4.4)

Die bei der Störfallanalyse zu treffenden Annahmen und Randbedingungen beziehen sich insbesondere auf Betriebsbedingungen beim Störfalleintritt, auf die Verfügbarkeit und das Verhalten von Systemen und Komponenten, auf die Beherrschung von Fehlern und Ausfällen sowie auf Handlungen des Betriebspersonals. Zusätzlich für Kernkraftwerke kommen dazu massgebende Ausgangsbedingungen wie Reaktorleistung, Kernbeladung, Zykluszeitpunkt und Nachzerfallsleistung. Die Methodik für die Störfallanalyse des Reaktorkerns mit von Zyklus zu Zyklus veränderlichen Hauptmerkmalen (Brennelementeinsatzstrategie, Kernbeladung, Zyklusdauer, Abbrand usw.) kann sich für Nachladungen auf Eingangsgrössen stützen, die als unveränderlich angesehen werden, wie konstruktive Vorgaben und Materialkonstanten (Kapitel 4.4.1).

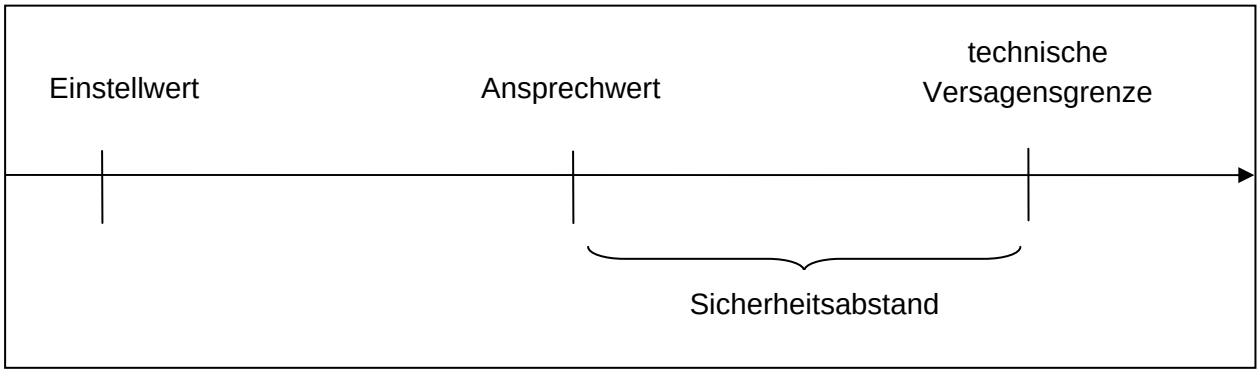
Grundsätzlich dürfen für die Durchführung der technischen Störfallanalyse ausschliesslich die zur Beherrschung des Störfalles ausgelegten Sicherheitssysteme einschliesslich ihrer Unterstützungs- und Versorgungssysteme berücksichtigt werden (Kapitel 4.4.2, Bst. a). Falls jedoch das Betriebsverhalten anderer Ausrüstungen den Störfallablauf nachteilig beeinflussen kann, ist dies ebenfalls zu bewerten (Kapitel 4.4.2, Bst. a). Konservativerweise soll die technische Störfallanalyse solche Systeme und Einrichtungen, für welche eine zeitlich begrenzte, präventive Instandhaltung während des betrachteten Betriebszustandes vorgesehen ist, als nicht verfügbar betrachten (Kapitel 4.4.2, Bst. b).

In Kapitel 4.4.3 werden Ausfallannahmen festgelegt, die für die technische Störfallanalyse zu treffen sind. Folgeausfälle des auslösenden Ereignisses sind zu berücksichtigen (Bst. a). Konservativerweise sind beim Nachweis der Wirksamkeit der geforderten Sicherheitsfunk-

tion(en) weitere Einschränkungen anzunehmen (Kapitel 4.4.3, Bst. b bis d). Falls eine Anforderung des Notstromversorgungssystems den Störfallablauf beeinflussen kann, ist der Ausfall der externen Stromversorgung (Notstromfall) in die Analyse einzubeziehen (Kapitel 4.4.3, Bst. b).

Handlungen des Betriebspersonals werden in werksinternen Vorschriften geregelt. Fehlhandlungen des Personals sind entweder als auslösendes Ereignis oder als Einzelfehler zu betrachten.

In Kapitel 4.4.5 werden anzunehmende Randbedingungen für Rechenparameter in Bezug auf Kenngrössen zur Anregung der Schutzaktionen (Bst. a) und auf die Verzugszeit der Signalverarbeitung bis zu deren Auslösung (Bst. b) festgelegt. Die tatsächlichen Einstellwerte enthalten eine Marge, welche Messungenauigkeiten, Drift, Kalibrierungstoleranzen usw. gegenüber den der Auslegung zugrunde gelegten Grenzwerten beinhaltet. Für die technische Störfallanalyse ist davon auszugehen, dass die Schutzaktionen nicht schon beim Einstellwert, sondern erst beim „Ansprechwert“ angeregt werden. Mit dem bei der Auslegung zu berücksichtigenden Sicherheitsabstand wird gewährleistet, dass die Schutzfunktionen auf jeden Fall vor der technischen Versagensgrenze ansprechen.



Zusätzlich ist beim Nachweis der Wirksamkeit der Sicherheitsfunktionen die ungünstige Wirkung der zur Störfallbeherrschung benötigten Ausrüstungen beim entsprechenden Anlagezustand anzunehmen (Kapitel 4.4.5, Bst. c, 1. Satz). Als minimale Wirksamkeit gelten die Mindestanforderungen an die Ausrüstungen gemäss Auslegungsspezifikationen. Eine höhere Wirksamkeit, die ungünstigere Folgen für den Störfallablauf haben kann, wie z. B. steilere Gradienten von Füllstands-, Druck- oder Temperaturänderungen, soll untersucht werden (Kapitel 4.4.5, Bst. c, 2. Satz).

2.5 Technische Analyse ausgewählter auslegungsüberschreitender Störfälle (Kapitel 5)

Auslegungsüberschreitende Störfälle können durch ein extrem seltenes Ereignis ausgelöst oder wegen Mehrfachfehlern in den zur Störfallbeherrschung erforderlichen Sicherheitsvorkehren auftreten. Die Analyse auslegungsüberschreitender Störfälle zielt gemäss Art. 12 der Verordnung des UVEK über die Gefährdungsannahmen und die Bewertung des Schutzes

gegen Störfälle in Kernanlagen darauf ab, die Wirksamkeit realistischer (vorbeugender oder lindernder) Massnahmen zur Bewältigung solcher extrem seltenen Störfälle nachzuweisen.

Einige generelle Randbedingungen wie die Verwendung realistischer Berechnungsprogramme und Randbedingungen, verfügbare Systeme und vorbeugende und lindernde Vorkehren, die bei der technischen Analyse auslegungsüberschreitender Störfälle verwendet werden können, sind in der Richtlinie angegeben. Diese Randbedingungen sind nicht so restriktiv wie der Analyse von Auslegungsstörfällen zugrunde liegenden Randbedingungen.

Für Kernkraftwerke sind besondere physikalische Prozesse, die nach einem Kernschaden auftreten können, festgehalten, welche mit anerkannten Berechnungsprogrammen zu untersuchen sind. Im Vordergrund steht dabei die Analyse des Verhaltens der Barrieren zum Einschluss der radioaktiven Stoffe. Im Weiteren sind bei Kernkraftwerken auslösende Ereignisse aufgrund von mehrfachen Fehlern und Ausfällen in diesem Rahmen zu analysieren.

Die Ergebnisse der technischen Analyse auslegungsüberschreitender Störfälle sind auf ihre Unsicherheiten hin zu prüfen.

3 Harmonisierung mit internationalen Anforderungen

Die grundsätzlichen Anforderungen an die deterministische Störfallanalyse sind in internationalen Empfehlungen (Safety Standards) der IAEA (International Atomic Energy Agency) festgelegt. Die Western European Nuclear Regulators' Association (WENRA) hat u. a. daraus so genannte Referenzniveaus (Reactor Safety Reference Levels) ausgearbeitet. Im Folgenden wird aufgezeigt, dass die für die Richtlinie in Frage kommenden Anforderungen und Empfehlungen der IAEA, insbesondere in den Standards NS-R-1 und NS-G-1.2, sowie jene der WENRA berücksichtigt werden.

3.1 Safety Standards der IAEA

Von den IAEA Safety Standards der Kategorien „Requirements" und „Guide" sind für die Richtlinie ENSI-A01 folgende Empfehlungen relevant:

a. Safety of Nuclear Power Plants: Design, Section 5, par. Safety Analysis (IAEA Safety Standards Series No. NS-R-1, Vienna, 2000)

b. Safety Assessment and Verification for Nuclear Power Plants, Section 4 Safety Analysis (IAEA Safety Standards Series No. NS-G-1.2, Vienna, 2001)

Zudem liegt der Entwurf eines weiteren IAEA Safety Guides vor: „Deterministic Safety Analysis for Nuclear Power Plants", DS 395 Draft 8, Vienna, October 2007. Dieser Standard stellt

eine ausführliche Anleitung für die Durchführung und Anwendung der deterministischen Störfallanalyse dar und ergänzt somit die generellen Ausführungen der Richtlinie.

Im Anhang 1 wird aufgezeigt, dass die relevanten Empfehlungen in den zutreffenden Abschnitten aus den erwähnten IAEA-Standards in der Richtlinie ENSI-A01 berücksichtigt werden.

3.2 Reference Levels der WENRA

Im Anwendungsbereich der Richtlinie ENSI-A01 sind WENRA Reference Levels von „Issue E“ (Design Basis Envelope for existing reactors), „Issue F“ (Design Extension of Existing Reactors), „Issue H“ (Operational Limits and Conditions) sowie von „Issue S“ (Protection against Internal Fires) massgebend.

Im Anhang 2 sind dementsprechend die relevanten „WENRA Reactor Safety Reference Levels“ (January 2008) aufgeführt und es wird aufgezeigt, über welche Kapitel der Richtlinie diese abgedeckt sind.

Anhang 1: Safety Standards der IAEA

Ref.	Requirement	Verhältnis zur Richtlinie ENSI-A01
NS-R-1	5.70. The computer programs, analytical methods and plant models used in the safety analysis shall be verified and validated, and adequate consideration shall be given to uncertainties.	Berücksichtigt in Kap. 4.3 a, e und f
NS-R-1	5.72. The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified. The safety analysis of the plant design shall be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and shall be consistent with the current or as built state.	Nicht explizit in der A01 behandelt, da übergeordnet in Art. 22 KEG und Art. 33 KEV festgelegt
NS-G-1.2	4.1. The aim of the safety analysis should be by means of appropriate analytical tools to establish and confirm the design basis for the items important to safety, and to ensure that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant condition category. …	Berücksichtigt in Kap. 2
NS-G-1.2	4.5. The plant design models and data (which are essential foundations for the safety analysis) should be kept up to date during the design phase and throughout the lifetime of the plant, including decommissioning. …	Berücksichtigt in Kap. 4.3 e
NS-G-1.2	4.9. The safety analysis should formally assess the performance of the plant under various operational and accident conditions, against goals or criteria for safety and radiological releases as may have been established by … the regulatory body, or other national or international authorities, as applicable to the plant.	Berücksichtigt in Kap. 2, mit Verweis auf die UVEK-VO
NS-G-1.2	4.15. The safety analysis should demonstrate by test, assessment, calculation or engineering analysis that the equipment incorporated to prevent escalation of anticipated operational occurrences or design basis accidents to severe accidents and to mitigate their effects, as well as emergency operating procedures and the accident management measures, is effective in reducing risk to acceptable levels.	Berücksichtigt in Kap. 2

Ref.	Requirement	Verhältnis zur Richtlinie ENSI-A01
NS-G-1.2	4.17. The achievement of a high level of safety should be demonstrated primarily in a deterministic way. However, the safety analysis should incorporate both deterministic and probabilistic approaches.	Berücksichtigt in Kap. 2
NS-G-1.2	4.39. All the PIEs should be defined quantitatively in terms of their frequency of occurrence. While the frequency of occurrence should be defined quantitatively for PSA applications, it is used qualitatively in the deterministic analysis.	Berücksichtigt in Kap. 4.1.2 a
NS-G-1.2	4.75. A large number of PIEs will be identified by following the guidance provided above. It is not necessary to analyse all of these PIEs. …	Berücksichtigt in Kap. 4.2.1 a
NS-G-1.2	4.77. The safety analysis should confirm that the grouping and bounding of initiating events is acceptable.	Berücksichtigt in Kap. 4.2.1 b
NS-G-1.2	4.78. The safety analysis of anticipated operational occurrences and DBAs should demonstrate that the safety systems are able to fulfil the safety requirements …	Berücksichtigt in Kap. 2 b
NS-G-1.2	4.81. The time periods evaluated for events should be sufficient to determine all the consequences of the design basis events. …	Berücksichtigt in Kap. 4.4.5 d
NS-G-1.2	4.86. The safety analysis of anticipated operational occurrences and DBAs should use suitable neutron physics, thermal-hydraulic, structural and radiological computer codes to determine the response of the reactor to the operational occurrences and accidents considered.	Berücksichtigt in Kap. 4.3 a
NS-G-1.2	4.87. The computer codes which are used to carry out the anticipated operational occurrences and DBA analysis should be properly verified and validated. …	Berücksichtigt in Kap. 4.3 b
NS-G-1.2	4.89. The computer code model parameters, initial conditions and equipment availability assumptions that underlie their use have traditionally been highly conservative with bounding, conservative values used for all analysis parameters. …	Berücksichtigt in Kap. 4.3 d

Ref.	Requirement	Verhältnis zur Richtlinie ENSI-A01
NS-G-1.2	4.92. The conservative assumptions made for the design basis analysis should typically include …	Berücksichtigt in Kap. 4.4.1
NS-G-1.2	4.93. The conservative assumptions made should take account of uncertainties in the initial conditions of the reactor, including safety system actuation set points.	Berücksichtigt in Kap.4.3 f und 4.5.2
NS-G-1.2	4.105. The safety analysis (of beyond design basis accidents) should aim to quantify a plant safety margin and demonstrate that a degree of defence in depth is provided for this class of accidents. …	Berücksichtigt in Kap. 5
NS-G-1.2	4.232. Use of the best estimate codes as recommended for both deterministic and probabilistic safety analysis should be complemented by sensitivity studies and/or by uncertainty analysis.	Berücksichtigt in Kap. 4.3
NS-G-1.2	4.238. All the computer codes used in the safety analysis should be validated and verified. …	Berücksichtigt in Kap. 4.3 b
NS-G-1.2	4.243. Regarding the users of the code, it should be ensured that: … , the users are sufficiently experienced in the use of the code and fully understand its uses and limitations, …	Berücksichtigt in Kap. 4.3 c
NS-G-1.2	4.244. Regarding the use of the computer code, it should be confirmed that: …, the nodalization and the plant models provide a good representation of the behaviour of the plant, …	Berücksichtigt in Kap. 4.3 e

Anhang 2: Reference Levels der WENRA

Issue E	**Verhältnis zur Richtlinie ENSI-A01**
4. Establishment of the design basis	
4.1 The design basis shall specify the capabilities of the plant to cope with a specified range of plant states[18] within the defined radiation protection requirements. Therefore, the design basis shall include the specification for normal operation and transients/accident conditions from Postulated Initiating Events (PIEs), the safety classification, important assumptions and, in some cases, the particular methods of analysis.	Anforderungen an die Methodik und Randbedingungen für die deterministische Störfallanalyse sind Gegenstand der A01.
4.2 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 design basis events shall be selected with deterministic or probabilistic methods or a combination of both, and 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.	In Kap. 4.2.1 und in den Anhängen 2 und 3 bezüglich deterministischer technischer Störfallanalyse berücksichtigt
8. Demonstration of reasonable conservatism and safety margins	
8.1 The initial and boundary conditions shall be specified with conservatism.	Berücksichtigt in Kap. 4.3, 4.4.1 und 4.4.3 c
8.2 The worst single failure[21] shall be assumed in the analyses of design basis events. However, it is not necessary to assume the failure of a passive component, provided it is justified that a failure of that component is very unlikely and its function remains unaffected by the PIE.	Berücksichtigt in Kap. 4.2.2
8.3 Only safety systems shall be credited to carry out a safety function. Non-safety systems shall be assumed to operate only if they aggravate the effect of the initiating event[22].	Berücksichtigt in Kap. 4.4.2
8.4 A stuck control rod shall be considered as an additional aggravating failure in the analysis of design basis events[23].	Berücksichtigt in Kap. 4.4.3 c
8.5 The safety systems shall be assumed to operate at their performance level that is most penalising for the initiator.	Berücksichtigt in Kap. 4.4.5 c

Issue E	Verhältnis zur Richtlinie ENSI-A01
8.6 Any failure, occurring as a consequence of a postulated initiating event, shall be regarded to be part of the original PIE.	Berücksichtigt in Anhang 1 (Begriffsbestimmung)
8.7 The impact of uncertainties, which in specific cases are of importance for the results, shall be addressed in the analysis of design basis events.	Berücksichtigt in Kap. 4.3 f.
9. Design of safety functions (General)	
9.3 Activations and manoeuvring of the safety functions shall be automated or accomplished by passive means such that operator action is not necessary within 30 minutes after the initiating event. Any operator actions required by the design within 30 minutes after the initiating event shall be justified[24].	Berücksichtigt in Kap. 4.4.4 b

---

18 Normal operation, anticipated operational occurrences and design basis accident conditions.

21 A failure and any consequential failure(s) shall be postulated to occur in any component of a safety function in connection with the initiating event or thereafter at the most unfavourable time and configuration.

22 This means that non-safety systems are either supposed not to function after the initiator, either supposed to continue to function as before the initiator, depending on which of both cases is most penalising.

23 This assumption is made to ensure the sufficiency of the shutdown margin. The stuck rod selected is the highest worth rod at Hot Zero Power and conservative values of reactor trip reactivity (conservative time delay and reactivity versus CR position dependence) are used. A stuck rod can be handled as single failure in the DBA-analysis if the stuck rod itself is the worst single failure.

24 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 supported by clear documented procedures that are regularly exercised in a full scope simulator.

Issue F	**Verhältnis zur Richtlinie ENSI-A01**
2. Selection and analysis of Beyond Design Basis Events	
2.1 Beyond design basis events shall be selected[31] and considered in the safety analysis to determine those sequences for which reasonable practicable preventive or mitigative measures can be identified and implemented (see Appendix for assessment of implementation).	Berücksichtigt in Kap. 5 e.
2.2 Realistic assumptions and modified[32] acceptance criteria may be used for the analysis of the beyond design basis events.	Berücksichtigt in Kap. 5 a bis d.
Appendix Interpretation of the reference level 2.1, for the purpose of benchmarking of implementation, in terms of types events to be analysed for design extension as a minimum, if not already considered in the design basis: - anticipated transient without scram (ATWS) - station black out - total loss of feed water - together with the complete loss of one emergency core cooling system[36] - uncontrolled level drop during mid-loop operation (PWR) or during refuelling - total loss of the component cooling water system - loss of core cooling in the residual heat removal mode - loss of fuel pool cooling - loss of ultimate heat sink function - uncontrolled boron dilution (PWR) - multiple steam generator tube ruptures (PWR, PHWR) - loss of required safety systems in the long term after a Postulated Initiating Event	Mit Ausnahme einer unkontrollierten Borverdünnung sowie einer unkontrollierten Niveauabsenkung bei offenem Reaktorkühlkreislauf sind im Kap. 5 alle aufgezählten Ereignisse berücksichtigt.

31 Based on a combination of deterministic and probabilistic assessments as well as engineering judgement.

32 Modified in relation to the conservative criteria used in the analysis of the design basis events.

36 Either the high pressure or the low pressure emergency core cooling system

Issue H	**Verhältnis zur Richtlinie ENSI-A01**
5. Safety limits, safety systems settings and operational limits	
5.2 Safety limits shall be established using a conservative approach to take uncertainties in the safety analyses into account.	Berücksichtigt in Kap. 5 (s. auch Darlegung im erläuternden Bericht)

Issue S	**Verhältnis zur Richtlinie ENSI-A01**
3. Fire hazard analysis	
3.1 A fire hazard analysis shall be carried out and kept updated to demonstrate that the fire safety objectives are met, that the fire design principles are satisfied, that the fire protection measures are appropriately designed and that any necessary administrative provisions are properly identified.	Übergeordnet in Kap. 4.2.1 b und d berücksichtigt
3.3 The fire hazard analysis shall demonstrate how the possible consequential effects of fire and extinguishing systems operation have been taken into account.	Übergreifende Einwirkungen sind in der UVEK-VO festgehalten. Berücksichtigt in Kap. 4.2.1