BfS

SAFETY CODES AND GUIDES - TRANSLATIONS

Edition 08/05

Contents

Safety Review for Nuclear Power Plants pursuant to
§ 19a of the Atomic Energy Act
- Guide Probabilistic Safety Analysis -

of 30 August 2005

Sicherheitsüberprüfung für Kernkraftwerke gemäß
§ 19a des Atomgesetzes
- Leitfaden Probabilistische Sicherheitsanalyse -

vom 30. August 2005

bilingual

Bundesamt für Strahlenschutz
Salzgitter

The German original of this translation was published in Bundesanzeiger 2005, No. 207a.

In case of discrepancies the German text shall prevail
.

Sicherheitsüberprüfung gemäss § 19a des Atomgesetzes
- Leitfaden Probabilistische Sicherheitsanalyse -
Stand 31. Januar 2005

Inhaltsverzeichnis

Safety Review for Nuclear Power Plants pursuant to § 19a of the Atomic Energy Act
- Guide Probabilistic Safety Analysis -
31 January 2005

Contents

1 Einleitung

Zur Sicherheitsüberprüfung, die der Betreiber einer Anlage zur Spaltung von Kernbrennstoffen zur gewerblichen Erzeugung von Elektrizität (Kernkraftwerk) gemäß § 19a Abs. 1 des Atomgesetzes durchzuführen und der Aufsichtsbehörde vorzulegen hat, gehört eine probabilistische Sicherheitsanalyse (PSA).

Probabilistische Sicherheitsanalysen gehören zum Stand von Wissenschaft und Technik bei der Sicherheitsbeurteilung von Kernkraftwerken. PSA werden in Ergänzung der auf deterministischen Grundlagen beruhenden Sicherheitsbeurteilung eingesetzt. Auf diese Weise kann der Einfluss von Komponenten, Systemen und Strukturen sowie von Personalhandlungen auf das sicherheitstechnische Anlagenverhalten ganzheitlich dargestellt und somit das Sicherheitsniveau quantitativ bewertet werden.

2 Aufgaben und Ziele der probabilistischen Sicherheitsanalyse

Probabilistische Analysen können für einen unterschiedlich großen Umfang auslösender Ereignisse (interne und externe Auslöser), für unterschiedliche Betriebszustände wie Leistungs- und Nichtleistungsbetrieb und mit unterschiedlicher Reichweite (Stufen 1 bis 3)[1] durchgeführt werden.

Die PSA ist bis einschließlich der Stufe 2[2] mit Methoden des Standes von Wissenschaft und Technik und unter Verwendung von Daten, die nach Stand von Wissenschaft und Technik vorzugsweise anlagenspezifisch ermittelt wurden, durchzuführen.

Für Ereignisse bei Nichtleistungsbetrieb (einschließlich An- und Abfahrvorgänge der Reaktoranlage) werden die Analysen bis zum Verlust von Reaktivitätskontrolle, des Einschlusses radioaktiver Stoffe oder von Brennelementkühlung (Gefährdungs- bzw. Kernschadenszustände) durchgeführt. Analysen der Stufe 2 für Betriebsphasen des Nichtleistungsbetriebs fordert dieser Leitfaden nicht.

Die PSA dient insbesondere dazu, eventuell bestehende Schwachstellen (Schwachstellenanalyse) einer Anlage qualitativ und quantitativ festzustellen und die Ausgewogenheit des sicherheitstechnischen Anlagenkonzepts zu beurteilen. Dabei wird aufgezeigt, mit welcher Häufigkeit Störungen und Störfälle infolge anlageninterner und –externer Ursachen sowie unter Berücksichtigung möglicher Ausfälle und Fehler der nach deterministischen Kriterien ausgelegten Sicherheits-einrichtungen sowie fehlerhaften Personalhandlungen zu nicht auslegungsgemäß beherrschten Anlagenzuständen führen können. Die Ermittlung von Gefährdungszuständen zusätzlich zu den Kernschadenszuständen erfolgt, um eine Beurteilung der Auslegung gegen Störfälle unabhängig von Maßnahmen und Einrichtungen der 4. Sicherheitsebene vornehmen zu können.

1 Introduction

The safety review which is to be performed by the operator of a plant used for industrial electricity generation based on the fission of nuclear fuels (nuclear power plant) according to § 19a , para. (1) of the Atomic Energy Act and which is to be submitted to the supervisory authority must include a Probabilistic Safety Analysis (PSA).

Probabilistic Safety Analyses belong to the stateof-the-art of science and technology with respect to the safety assessment of nuclear power plants. PSA are used as a supplement to the safety assessment made on a deterministic basis. This approach is used for a holistic representation of the influence of components, systems and structures as well as of human actions on the installation behaviour with respect to safety so that the safety level can be quantitatively evaluated.

2 Function and objectives of the Probabilistic Safety Analysis

Probabilistic analyses can be performed for different extent of initiating events (internal and external initiators), for different operational conditions such as full power operation or low-power and shutdown modes and within different scopes (Level 1 to Level 3)1.

A PSA up to and including Level 2 is to be performed with the help of methods corresponding to the state-of-the-art of science and technology and has to make use of preferably plant-specific data ascertained according to the state-of-the-art of science and technology.

For events occurring in low-power and shutdown modes (including startup and shutdown processes in the reactor plant), the analyses are conducted up to the loss of reactivity control, of the confinement of radioactive materials or of the fuel element cooling (hazard states and/or core damage states). This guide does not require Level 2 analyses for operating periods during low-power and shutdown modes.

The PSA serves in particular to determine the quality and quantity of potentially existing vulnerabilities (vulnerability analysis) of a plant and to assess the balance of the safety-related plant concept. It is used to show the frequency in which operational occurrences and accidents due to internal and external causes, also considering potential failures and faults of the safety devices designed on the basis of deterministic criteria and considering human errors, can lead to plant conditions which can not be controlled according to the design. Hazard states are determined in addition to core damage states in order that the design against accidents can be assessed independently of measures and functions associated with safety level 4.

---

[1] Erläuterungen zum Umfang der Stufen siehe Anhang A

[2] Es besteht Einvernehmen zwischen den atomrechtlichen Aufsichtsbehörden und den Betreibern der Kernkraftwerke in Deutschland, dass im Zusammenhang mit der Stufe 1 der PSA auch eine Stufe 2 der PSA durchgeführt wird. Mit der Behandlung der Stufe 2 der PSA ist aber keine rechtliche Einordnung, insbesondere im Hinblick auf die erforderliche Vorsorge nach § 7 Abs. 2 Nr. 3 des Atomgesetzes, verbunden.

[1] For details on the scope of the Levels see Appendix A

[2] The nuclear supervisory authorities and the operators of nuclear power plants in Germany have agreed that in the context of a PSA Level 1 they will also conduct a PSA Level 2.
A performance of a PSA Level 2, however, is not associated with a legal classification, in particular with respect to the necessary precaution according to § 7, para (2), subpara. 3 of the Atomic Energy Act.

Im Einzelnen wird die PSA mit den Zielen durchgeführt, um

- das Sicherheitsniveau quantitativ zu ermitteln;
- aufzuzeigen, ob die sicherheitstechnische Auslegung und die Betriebweise in dem Sinne ausgewogen sind, dass kein auslösendes Ereignis einen überproportionalen oder signifikant erhöhten Beitrag zur Gesamthäufigkeit von nicht beherrschten Anlagenzuständen leistet;
- mittels einer Schwachstellenanalyse zu erkennen, ob anlagenspezifische Schwachstellen (insbesondere bei Systemfunktionen, Betriebsweise und -reglement, Personalhandlungen) hinsichtlich der zu behandelnden Ereignisabläufe vorliegen;
- im Rahmen der Analyse zu erkennen, ob in der Realität vorkommende Streubreiten in den Eingangsgrößen für die Ereignisabläufe und Sicherheitsfunktionen zu gravierenden Auswirkungen auf das Ergebnis führen können (Sensitivitätsanalyse);
- präventive und mitigative anlageninterne Notfallmaßnahmen zu beurteilen und
- mögliche unfallbedingte Freisetzungen (Quellterme) und ihre Häufigkeiten, insbesondere für frühe große Freisetzungen, abzuschätzen.

A PSA is conducted in detail with the following objectives, so that:

- the safety level can be quantitatively evaluated;
- it can be shown if the safety-related design and the operating modes are well balanced in a sense that no initiating event contributes disproportionately or in a significantly enhanced manner to the total frequency of plant conditions beyond control;
- it can be recognized with the help of a vulnerability analysis if plant-specific vulnerabilities exist (in particular in system functions, operating modes and operating regulations, human actions) with respect to the event sequences to be treated;
- it can be determined in the analysis if variations in the initial parameters for the event sequences and safety functions occurring in reality can have serious consequences on the result (sensitivity analysis);
- preventive and mitigative on-site accident management measures can be evaluated; and
- potential releases caused by accident (source terms) and their frequencies, in particular for large early releases, can be estimated.

3 Allgemeine Anforderungen

Als Ausgangsbedingungen sind diejenigen Anlagenzustände anzusetzen, die hinsichtlich der zu analysierenden Ereignisabläufe die Anforderungen an die Sicherheitseinrichtungen realistisch repräsentieren.

Die PSA umfasst die im Ablaufdiagramm aufgezeigten konkreten Arbeitsschritte für eine PSA der Stufe 1 (Abbildung 1 und 2) und der Stufe 2 (Abbildung 3).

Die PSA ist unter maßgeblicher und intensiver Beteiligung anlagenkundigen Personals des Betreibers durchzuführen.

Bei der Durchführung der PSA können Modelle und Teilergebnisse, einschließlich der Ergebnisse aus Störfall- und Unfallanalysen, aus entsprechenden Analysen für vergleichbare Anlagen übernommen werden, wenn die Übertragbarkeit dieser Modelle und Ergebnisse nachgewiesen ist.

Die Einzelheiten sind in den PSA-Fachbänden *„Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“* und *„Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“* festgelegt. Diese PSA-Fachbände enthalten eine nähere Bestimmung des Standes von Wissenschaft und Technik der PSA.

3.1 PSA der Stufe 1 für den Leistungs- und Nichtleistungsbetrieb

Gegenstand der PSA der Stufe 1 sind Ermittlung und Quantifizierung von Ereignisabläufen, die ausgehend von einem Spektrum auslösender Ereignisse[3] nicht mehr auslegungsgemäß beherrscht werden (Gefährdungszustände[4]) oder zu Kernschäden bzw. Kernschmelzen (Kernschadenszustände[5]) führen können. Die Häufigkeiten der Gefährdungszustände und der Kernschadenszustände sind explizit auszuweisen.

3 General requirements

Such plant conditions shall be used as initial conditions which give a realistic representation of the requirements of the safety devices with respect to the event sequences to be analysed.

A PSA shall comprise the concrete work steps shown in the flow chart for a PSA Level 1 (figures 1 and 2) and Level 2 (figure 3).

Experienced staff of the operator must be significantly and intensively involved in the PSA.

When performing a PSA, models and partial results, including the results from incident and accident analyses, from the respective analyses of comparative plants can be used if it is proven that these models and results can be applied to the present analysis.

The details are set out in the PSA-Fachbänden *„Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“* (methods-volume) und *„Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke“* (data-volume). These technical documents include a more detailed analysis of the state-of-the-art of science and technology with respect to PSA.

3.1 PSA Level 1 for full power operation and low-power and shutdown operation

Subject of a PSA Level 1 is the determination and quantification of event sequences, based on a spectrum of initiating events[3], which cannot be controlled according to the design (hazard states[4]) or can lead to core damage and/or core meltdown (core damage states[5]). The frequencies of hazard states and core damage states must be explicitly assessed.

[3] Begriffserläuterung im Anhang A
[4] Begriffserläuterungen im Anhang A
[5] Begriffserläuterung im Anhang A

[3] Explanation of terms see Appendix A
[4] Explanations of terms see Appendix A
[5] Explanation of terms see Appendix A

Technische Einrichtungen und präventive Maßnahmen des anlageninternen Notfallschutzes, die Notfallprozeduren für die Durchführung von Hand- und Reparaturmaßnahmen umfassen können sowie vorhandene technische Einrichtungen nutzen, sind probabilistisch zu bewerten und in die Bestimmung der Häufigkeit von Kernschadenszuständen einzubeziehen.

Für das Spektrum der für die jeweilige Anlage relevanten auslösenden Ereignisse sind Ereignisablauf- und Fehlerbaumanalysen zusammen mit Importanz-, Sensitivitäts- und Unsicherheitsanalysen betriebszustandsbezogen durchzuführen. Wirksamkeitsbedingungen sind abhängig von den Ereignisabläufen zu ermitteln. Die Anlagentechnik sowie die Betriebsweisen der Systeme einschließlich der Personalhandlungen sind zu modellieren; Folgeausfälle, funktionale Abhängigkeiten zwischen Systemfunktionen, gemeinsam verursachte Ausfälle sowie Personalhandlungen sind zu berücksichtigen.

Die Endzustände der Ereignisablaufpfade sind einschließlich Eintrittshäufigkeiten und Ergebnisse der Sensitivitäts- und Unsicherheitsanalysen auszuweisen (siehe Abschnitte 4.1.9 und 4.1.10).

Technical installations and preventive measures relating to on-site accident management, which may include emergency procedures for the implementation of manual actions and repair measures and may use existing technical installations, must be assessed probabilistically and taken into account for the determination of frequencies of core damage states.

Event sequence and fault tree analyses as well as importance, sensitivity and uncertainty analyses have to be carried out with respect to the operating conditions for the spectrum of initiating events which are relevant for the plant. Effectivity conditions of systems have to be determined depending on the event sequences. Plant technology as well as operating modes of the systems, including human actions, have to be modelled; subsequent failures and functional dependencies between system functions, common cause failures as well as human actions have to be considered.

The end states of event sequence paths must be indicated including the relevant frequencies of occurrence and the results of sensitivity and uncertainty analyses (see sections 4.1.9. and 4.1.10.).

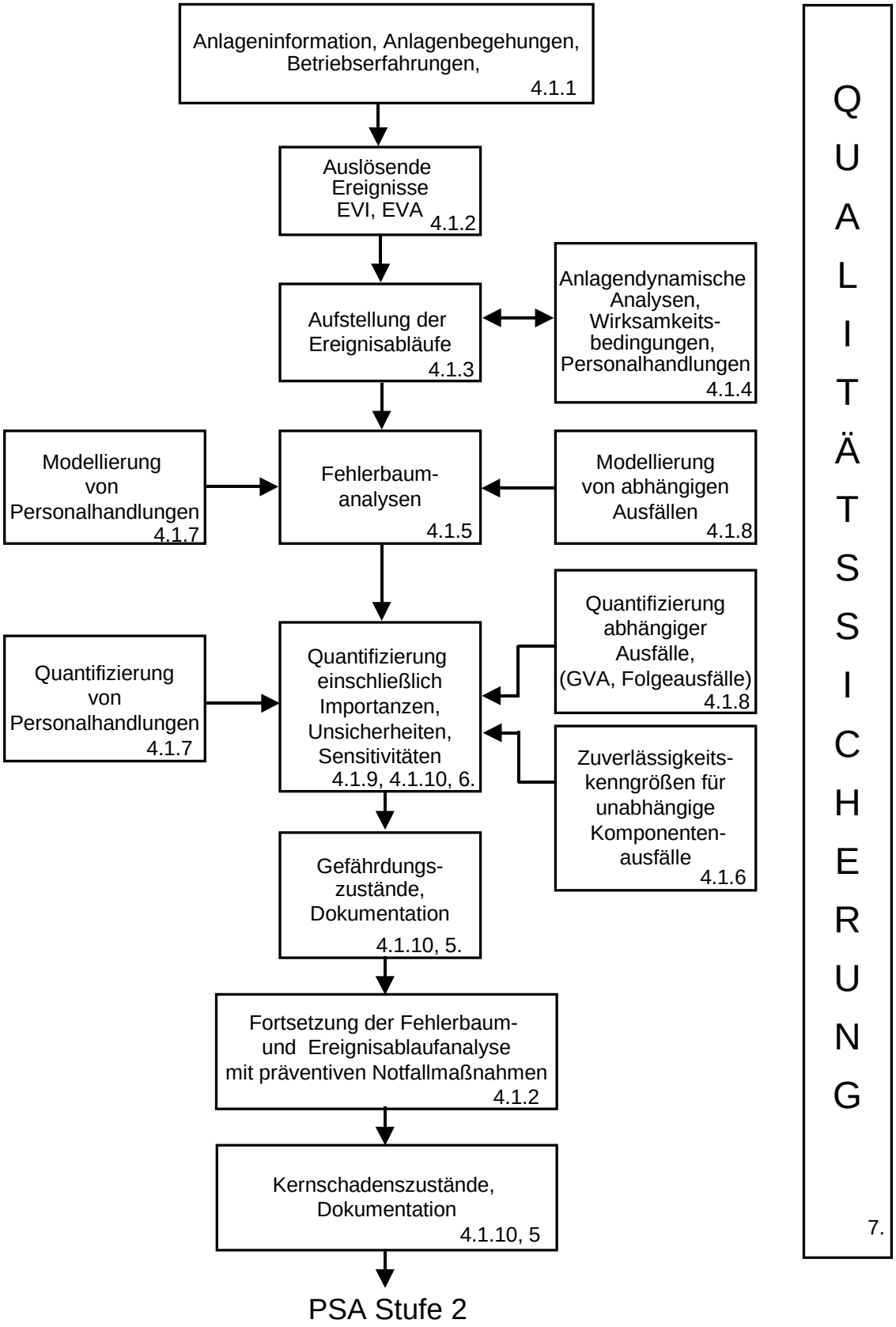

Abb. 1: Ablauf der Probabilistischen Sicherheitsanalyse (PSA) der Stufe 1 im Leistungsbetrieb (mit Hinweisen auf die entsprechenden Abschnitte im vorliegenden Leitfaden)

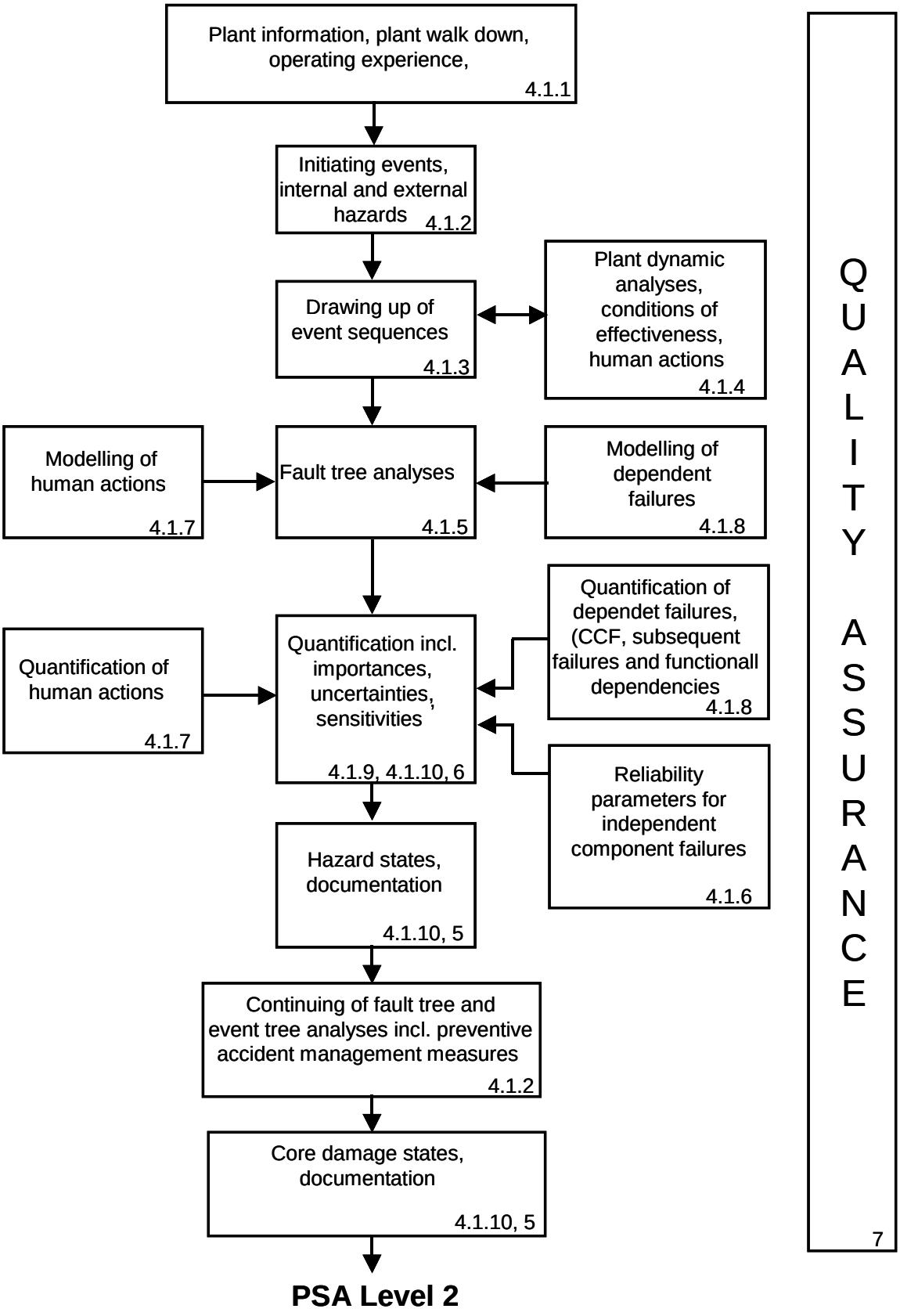

Fig. 1: Flow chart of the Probabilistic Safety Analysis (PSA) Level 1 during full power operation (including references to the respective sectins in the present guide)

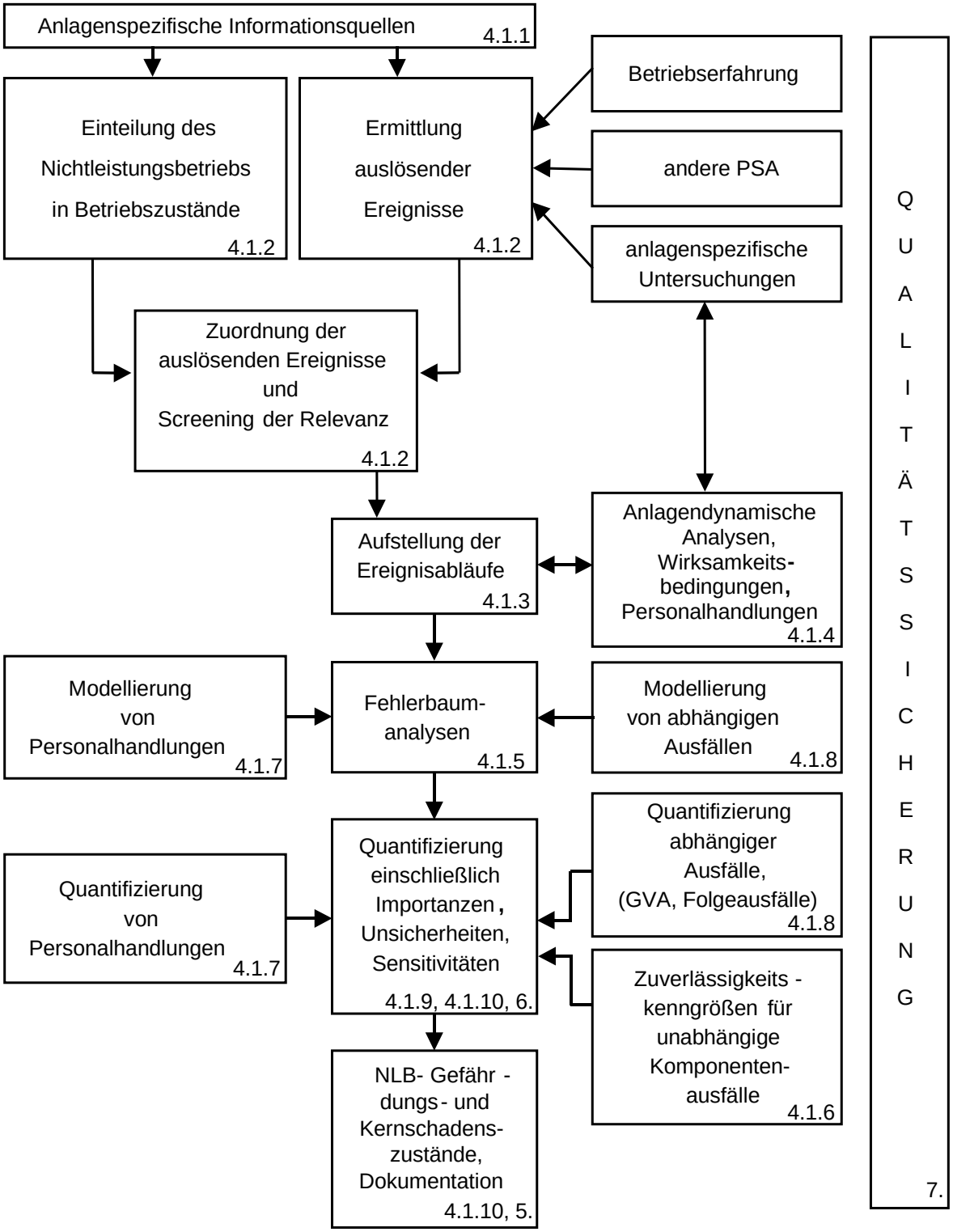

Abb. 2: Ablauf der Probabilistischen Sicherheitsanalyse (PSA) der Stufe 1 im Nichtleitsugnsbetrieb (mit Hinweisen auf die entsprechenden Abschnitte im vorliegenden Leitfaden)

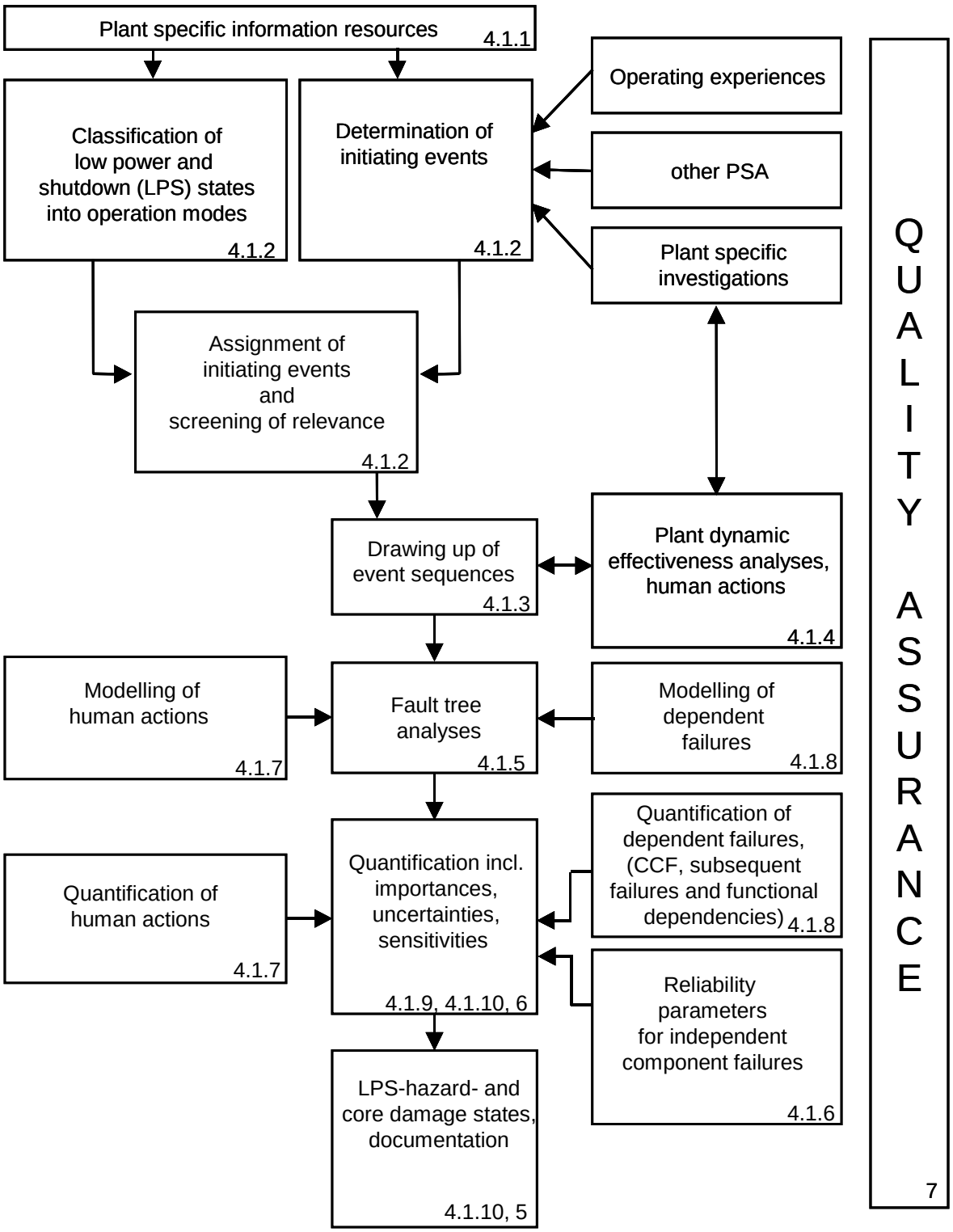

Fig. 2: Flow chart of the Probabilistic Safesty Analysis (PSA) Level 1 during low-power and shutdown operation (including references to the respective sections in the present guide)

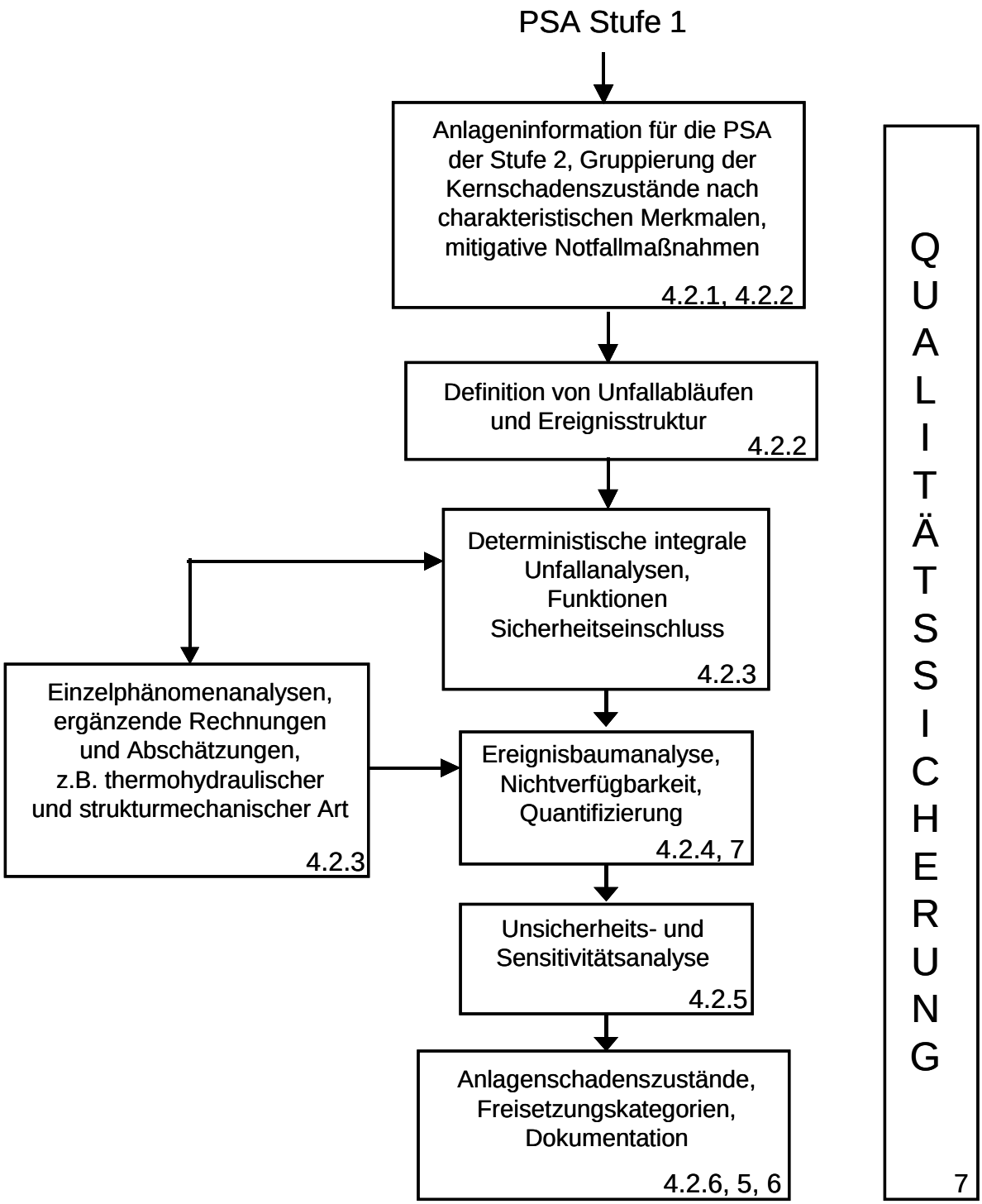

Abb. 3: Ablauf der Probabilistischen Sicherheitsanalyse der Stufe 2 (mit Hinweisen auf die entsprechenden Abschnitte im vorliegenden Leitfaden)

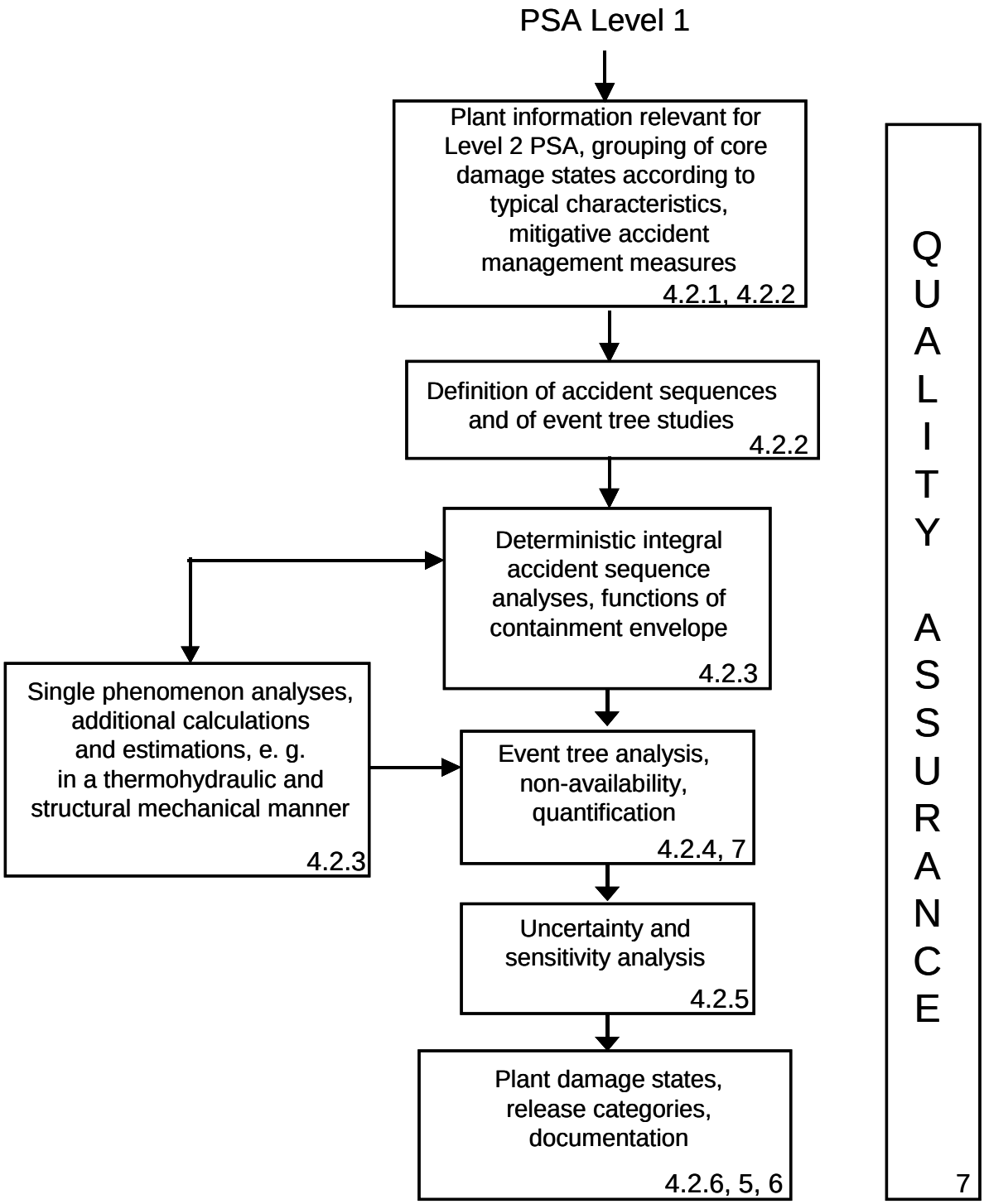

Fig. 3: Flow chart of the Probabilistic Safety Analysis Level 2 (including references to the repsective sections in the present guide)

3.2 PSA der Stufe 2 für den Leistungsbetrieb

Basis für Analysen der Stufe 2 sind die im Rahmen der PSA der Stufe 1 ermittelten Kernschadenszustände, deren charakteristische Merkmale übernommen werden. Untersucht wird, wie sich aus Kernschadenszuständen[6] verschiedene Unfallabläufe entwickeln und zu Freisetzungen radioaktiver Stoffe in die Umgebung führen können. Hierzu werden unter Berücksichtigung der physikalischen, chemischen, thermodynamischen und strukturmechanischen Phänomene Ereignisbaumanalysen durchgeführt. Sie sind durch Unsicherheits- und Sensitivitätsanalysen zu ergänzen. Die Endzustände (Anlagenschadenszustände[7]) der Unfallablaufanalysen werden in Freisetzungskategorien[8] zusammengefasst.

Zu untersuchen ist
- die Wirkung unfallbestimmender Phänomene auf das Verhalten der Anlage und mögliche Schwachstellen unter den Bedingungen auslegungsüberschreitender Ereignisabläufe mit Kernschmelzen einschließlich der Unsicherheiten und
- inwieweit Unfallabläufe mit den vorgeplanten Maßnahmen des anlageninternen Notfallschutzes in ihren Auswirkungen gemildert und unter Kontrolle gebracht werden können.

Die Analyse soll es ermöglichen, die ergebnisbestimmenden Unfallabläufe zu erkennen und unter Berücksichtigung von Beurteilungsunsicherheiten zu bewerten.

PSA der Stufe 2 können unter Vermeidung der Schnittstelle von Stufe 1 zu Stufe 2 auch integral erstellt werden. Hierbei ist sicher zu stellen, dass die für die Bewertung relevanten Zwischenergebnisse zur Stufe 1 – insbesondere die Häufigkeiten von Gefährdungszuständen – angegeben werden können.

4. Methoden der Analyse

4.1 PSA der Stufe 1 für den Leistungs- und Nichtleistungsbetrieb

4.1.1 Anlagenspezifische Eingangsinformationen

Zur Durchführung einer PSA sind detaillierte Informationen über Aufbau, Funktionen und Wirksamkeiten der zu berücksichtigenden Komponenten und Systeme einschließlich von Bedienungsmaßnahmen, Betriebsweisen, Instandhaltungsmaßnahmen, Wiederkehrenden Prüfungen und Notfallmaßnahmen erforderlich. In der Regel sind diese Informationen der vorhandenen anlagenbeschreibenden Dokumentation zu entnehmen. Diese enthält Systembeschreibungen, Schaltpläne, Betriebshandbücher, Prüfhandbücher, Notfallhandbücher und Analysen zu Störfällen, die der Auslegung der sicherheitstechnischen Einrichtungen der Anlage zugrunde liegen. Für den Nichtleistungsbetrieb sind u.a. zusätzlich Angaben zur Komponentenverfügbarkeit bei bestimmten Anlagenbetriebsphasen, Revisionsberichte, Anweisungen zu Arbeitsvorgängen, Freischaltungen etc. während der Revision erforderlich.

Der PSA ist der Anlagenzustand zur Zeit ihrer Erstellung zugrunde zu legen. Der Betreiber gibt den genauen Zeitpunkt an. Der Betreiber weist auch aus, welche Änderungen er während der Erstellung der PSA durchgeführt hat, die Einfluss auf die Ergebnisse der PSA haben. Vorgesehene Anlagenänderungen können zusätzlich in die PSA einbezogen werden, soweit prüffähige Unterlagen vorhanden sind. Der Einfluss vorgesehener Anlagenänderungen auf die Ergebnisse der PSA ist gesondert einzeln auszuweisen.

[6] Begriffserläuterungen im Anhang A
[7] Begriffserläuterungen im Anhang A
[8] Begriffserläuterungen im Anhang A

3.2 PSA Level 2 for full power operation

Level 2 Analyses are based on the core damage states determined within the PSA Level 1, whose characteristics are taken from the Level 1 analysis. Investigations focus on the question how core damage states[6] can lead to different accident sequences and to the release of radioactive material into the environment. To this end, event tree analyses are carried out, which take into account the physical, chemical, thermodynamic and structural mechanical phenomena. Uncertainty and sensitivity analyses are required as a supplement to event tree analyses. The final conditions (plant damage states[7]) of the accident sequence analyses are summarised in different release categories[8].

Investigations must include:
- the effects that phenomena determining influencing the accident progression have on the plant behaviour as well as potential vulnerabilities under the conditions of beyonddesign-basis event sequences with core meltdown including the uncertainties; and
- the question to what extent the consequences of accident sequences can be alleviated and brought under control with the help of the prearranged measures relating to on-site accident management.

The analysis is supposed to make it possible to identify the accident sequences determining influencing the event and to assess them while taking into account the relevant uncertainties of assessment.

PSAs Level 2 can also be conducted integrally thus avoiding the interface between Level 1 and Level 2. In this case it has to be ensured that the interim results from the Level 1 analysis relevant for the assessment – in particular the frequencies of hazard states – are available.

4. Methods of analysis

4.1 PSA Level 1 for full power and low-power and shutdown operation

4.1.1 Plant-specific initial information

To perform a PSA, detailed information on the structure, functions and efficiencies of components and systems to be considered is necessary, including operating measures, operating modes, maintenance measures, periodic testing and in-service inspections, and accident management measures. In general, this information is provided in the existing plant documentation. This documentation contains descriptions of the systems, circuit diagrams, operating and inspection manuals, emergency manuals as well as analyses of accidents on which the design of the engineered safety features of the plant is based. In the case of low-power or shutdown operation, additional information is required during the review with respect to the availability of components during different plant operating periods as well as review reports, instructions on operations, isolations etc.

The PSA must generally be based on the plant status at the time of analysis. The operator indicates the exact time. The operator also indicates what changes he has implemented while the analysis was conducted and which might influence the results of the PSA. Envisaged changes of the plant can be additionally incorporated into the PSA provided that verifiable documentation is available. The impact of envisaged changes of the plant on the results of the PSA have to be separately described.

[6] Explanation of terms see Appendix A
[7] Explanations of terms see Appendix A
[8] Explanation of terms see Appendix A

Wichtige und ergänzende Informationen sind aus Begehungen der Anlage, aus Betriebserfahrungen sowie aus Fachgesprächen mit dem Betriebspersonal (z.B. über spezifische Betriebsabläufe bei Personalhandlungen) heranzuziehen.

4.1.2 Auslösende Ereignisse

Auslösende Ereignisse, die Gegenstand anderer PSA und bisher vorliegender Untersuchungen waren, sind in den Anhängen B1, B2, B3 und B4 zusammengestellt. Bei B1 und B2 handelt es sich um Referenzspektren zu betrachtender auslösender Ereignisse im Leistungsbetrieb für DWR und SWR. B3 enthält beispielhaft Betriebsphasen des Nichtleistungsbetriebs für SWR und DWR.

Die Referenzspektren sind anlagenspezifisch auf Relevanz hin zu überprüfen und gegebenenfalls zu modifizieren (z.B. bezüglich der Leckgröße). Das bei der probabilistischen Analyse zu betrachtende Spektrum auslösender Ereignisse ist anlagenspezifisch hinsichtlich seiner Vollständigkeit unter Beachtung aller in deterministischen Analysen zu betrachtenden Ereignisse zu begründen.

Die Häufigkeit der auslösenden Ereignisse ist anlagenspezifisch zu bestimmen. Bei Verwendung generischer Werte ist die Übertragbarkeit zu bewerten. Wenn auslösende Ereignisse zusammengefasst werden, müssen für die einzelnen Systemfunktionen bzw. Notfall-Systemfunktionen[9] die jeweils ungünstigsten Mindestanforderungen berücksichtigt werden.

Für den Nichtleistungsbetrieb enthält der Anhang B3 eine Unterteilung in verschiedene Betriebsphasen. Für die Erfordernisse der Analyse sind diese Betriebsphasen weiter zu unterteilen, so dass während einer Betriebsphase annähernd konstante Randbedingungen vorliegen.

Auslösende Ereignisse brauchen nicht detailliert untersucht werden, wenn ihr Einfluss auf die Ergebnisse für die Häufigkeit eines Gefährdungs- und Kernschadenszustandes sowie für die Freisetzungshäufigkeiten gering ist. Hier ist eine Abschätzung ausreichend. Voraussetzung für eine Abschätzung zu nicht im Detailuntersuchten auslösenden Ereignissen ist die Erfüllung folgender Bedingungen:

1. Der Beitrag zur Gefährdungs- und Kernschadenshäufigkeit durch ein einzelnes auslösendes Ereignis liegt unter 10 % und der Gesamtbeitrag aller abgeschätzten auslösenden Ereignisse liegt unter 20% der Gesamthäufigkeit der Gefährdungs- und Kernschadenszustände.
2. Der Beitrag zur Häufigkeit früher großer Freisetzungen durch ein einzelnes auslösendes Ereignis liegt unter 10 % und die Gesamtbeiträge aller abgeschätzten auslösenden Ereignisse liegen unter 20 % der Gesamthäufigkeiten früher großer Freisetzungen. Im Hinblick auf die Häufigkeit anderer Freisetzungen kann analog verfahren werden.

Die abgeschätzten Beiträge der nicht im Detail analysierten Ereignisabläufe zu den genannten Ergebnisgrößen sind bei der Bewertung entsprechend zu berücksichtigen.

Important and supplementary information is to be derived from plant walk downs, operating experiences as well as from expert talks with the operating personnel (e.g. on specific operational processes during human actions).

4.1.2 Initiating events

Initiating events which were the subject of other PSAs and investigations available so far are comprised in Appendices B1, B2, B3 and B4. B1 and B2 are reference spectra of initiating events to be considered for the full power operation of PWR and BWR. B3 contains exemplary operating periods during low-power or shutdown operation of BWR and PWR.

The reference spectra have to be reviewed with respect to their relevance and, if necessary, modified (e.g. regarding the leak size). The spectrum of initiating events to be considered in a probabilistic analysis shall be justified plantspecifically with respect to completeness, considering all events to be examined in deterministic analyses.

The frequency of initiating events is to be determined plant-specifically. If generic values are used, it has to be assessed to what extent these values can be applied to the present case. If initiating events are considered conjointly, the relevant most unfavourable minimum requirements of the single system functions and/or emergency system functions[9] have to be taken into account.

In Appendix B3 the different operating periods during low-power or shutdown operation are considered separately. For the requirements of the analysis these operating periods have to be further divided so that almost constant boundary conditions exist for each operating period.

Initiating events which only have a small impact on the results for the frequency of a hazard and core damage state as well as for the frequencies of release do not need to be examined in detail. In this case an estimation would be sufficient. For an estimation of initiating events not to be examined in detail it is necessary precondition that the following requirements are complied with:

1. A single initiating event contributes less than 10 % to the frequency of hazard and core damage states and all initiating events estimated contribute less than a total of 20 % to the total frequency of hazard and core damage states.
2. A single initiating event contributes less than 10 % to the frequency of early large releases and all initiating events estimated contribute less than a total of 20 % to the total frequency of early large releases. The same requirements can be applied to the frequency of other types of releases.

The estimated contributions of the event sequences not analysed in detail to the resulting parameters mentioned have to be considered appropriately in the assessment.

[9] Begriffserläuterungen im Anhang A

[9] Explanations of terms see Appendix A

4.1.3 Ereignisablaufanalysen

In Abhängigkeit vom auslösenden Ereignis und dem jeweils vorliegenden Anlagenbetriebszustand bzw. der Betriebsphase sind diejenigen Sicherheitsfunktionen von Betriebs- und Sicherheitssystemen[10] sowie die Personalhandlungen zu ermitteln, die zur Beherrschung des Ereignisses vorgesehen sind und angefordert werden. Grundlage dieser Ermittlung sind vor allem die Anregekriterien für die Systeme zur Störfallbeherrschung. Daneben sind Handeingriffe des Betriebspersonals zu berücksichtigen. Die Wirksamkeitsbedingungen der einzelnen Systeme sind abhängig vom Ereignisablauf festzustellen. Anlagenzustände, die von den Sicherheitsfunktionen nicht auslegungsgemäß beherrscht werden, sind den Gefährdungszuständen zuzuordnen und auszuweisen.

Vorhandene anlageninterne Notfallschutzmaßnahmen einschließlich Reparaturmaßnahmen sind im auslegungsüberschreitenden Bereich zu berücksichtigen. Ereignisabläufe, die auch nach Berücksichtigung des realistischen Verhaltens der Systeme, Strukturen und Komponenten und anlageninterner Notfallschutzmaßnahmen nicht beherrscht werden und zu Kernschäden führen, werden als Kernschadenszustände ausgewiesen.

Die Analysen werden in Form von Ereignisablaufdiagrammen dargestellt, wesentliche Ergebnisse sind die Endzustände und deren Häufigkeiten. Die Endzustände sind in geeigneter Weise in Kategorien einzuteilen, die den zeitlichen Abläufen und möglichen Auswirkungen auf die Anlage Rechnung tragen, z.B. infolge unterschiedlicher Drücke im Primärkreis.

4.1.4 Analysen zu Wirksamkeitsbedingungen

Die Wirksamkeitsbedingungen beschreiben die Mindestanforderungen an die angeforderten Sicherheitsfunktionen derjenigen Systeme, die diese Funktionen im Anforderungsfall gewährleisten sollen, zusätzlich werden die zugehörigen verfahrenstechnischen Einsatzzeiten benötigt. Die Ermittlung der Wirksamkeitsbedingungen sollte vorzugsweise auf der Grundlage von Rechnungen mit realistischen Randbedingungen erfolgen, damit die vorhandenen Sicherheitsreserven der Anlage in der Analyse berücksichtigt werden und eine möglichst realitätsnahe Beurteilung der Ausgewogenheit des Sicherheitskonzepts ermöglicht wird. Zur Reduzierung des Untersuchungsaufwandes können vorliegende Rechnungen übernommen werden, falls diese hinsichtlich Ausgangs- und Randbedingungen auf den zu betrachtenden Ereignisablauf übertragbar sind.

4.1.5 Fehlerbaumanalysen

In den Diagrammen zu den Ereignisablaufanalysen (vgl. Abschnitt 4.1.3) wird aufgezeigt, wie sich die einzelnen Ereignisabläufe abhängig von der Verfügbarkeit der angeforderten Sicherheitsfunktion verzweigen können. Die möglichen Ausfälle der Sicherheitsfunktionen werden mit Hilfe der Fehlerbaumanalyse untersucht.

Die Quantifizierung der Fehlerbäume erfolgt mit den in den Abschnitten 4.1.6 bis 4.1.8 genannten Eingangsdaten.

[10] Begriffserläuterungen im Anhang A

4.1.3 Event sequence analysis

Depending on the initiating event and the respective operational condition and/or operating period of the plant, such safety functions of operational and safety systems[10] as well as the human actions shall be determined which are designed and required for controlling the event. The activation criteria for the systems controlling accidents represent the main basis of this determination. In addition, manual actions of the operating personnel have to be taken into account. The success criteria of the individual systems shall be determined depending on the event sequence. Plant conditions which are not controlled according to the design by the safety systems shall be regarded as hazard states and shall be characterised accordingly.

Existing on-site accident management measures including repair measures have to be taken into account in the beyond-design-basis area. Event sequences which cannot be controlled even after taking into account the realistic behaviour of systems, structures and components, and on-site accident management measures and which lead to core damage are characterised as core damage states.

The analyses shall be illustrated in the form of event sequence diagrams, the final conditions and their frequencies are considered to be essential results. The final conditions have to be appropriately divided into categories which allow for the time sequences and potential consequences on the plant, e.g. following different pressures in the primary circuit.

4.1.4 Analyses relating to success criteria

The success criteria describe the minimum requirements to be met by the required safety functions of such systems which are supposed to ensure these functions in case of demand. In addition, the relevant mission times with respect to procedures are needed. The determination of the success criteria should preferably be carried out on the basis of computations with realistic boundary conditions so that the existing safety margins of the plant can be considered in the analysis and the balance of the safety concept can be assessed as realistically as possible. Existing results of analyses can be used to reduce investigation efforts provided that they can be applied to the event sequence under consideration with regard to initial and boundary conditions.

4.1.5 Fault tree analyses

The diagrams relating to the event sequence analyses (cf. section 4.1.3) show how the single event sequences can branch out depending on the availability of the safety functions required. Potential failures of safety functions are investigated with the help of a fault tree analysis.

The quantification of fault trees is based on the input data defined in the sections 4.1.6 and 4.1.8.

[10] Explanations of terms see Appendix A

4.1.6 Zuverlässigkeitskenngrößen für unabhängige Komponentenausfälle

Grundsätzlich sind für die PSA anlagenspezifische Zuverlässigkeitskenngrößen[11] zu verwenden. Für deren Ermittlung sind die notwendigen Informationen aus den Betriebsunterlagen der Anlage zu entnehmen. Im Datenband ist ausgeführt, wie die Kenngrößen bestimmt werden können.

Steht keine hinreichende anlagenspezifische Datenbasis zur Verfügung, können generische Daten verwendet werden. Bei Verwendung von generischen Daten ist jedoch unter Berücksichtigung anlagenspezifischer Gegebenheiten die Anwendbarkeit zu prüfen und zu dokumentieren. Wenn Komponenten, für die generische Daten verwendet wurden, wesentliche Beiträge zur Gesamthäufigkeit der Gefährdungszustände liefern, ist eine anlagenspezifische Auswertung der Übertragbarkeit der zugehörigen generischen Zuverlässigkeitskenngrößen durchzuführen und nachvollziehbar zu begründen.

4.1.7 Personalhandlungen

Die im Zuge eines Ereignisablaufes angeforderten Funktionen können auf verschiedene Weise von Personalhandlungen abhängen. Die Analyse von Personalhandlungen beinhaltet die Identifizierung, Modellierung und probabilistische Bewertung von Handlungen des Betriebspersonals, die Auswirkungen auf Ereignisabläufe haben. Zur Bestimmung des Beitrags von Personalhandlungen in den Ereignisabläufen ist eine Analyse mit eigenständiger Methodik erforderlich. Für die Durchführung einer derartigen Analyse stehen zahlreiche Methoden zur Verfügung. Grundsätzlich sind Methoden zu bevorzugen, die bereits in atomrechtlichen Verfahren eingesetzt und begutachtet wurden, sofern diese dem geltenden Stand von Wissenschaft und Technik genügen. Die Wahl der jeweiligen Methodik ist nachvollziehbar zu begründen. Dies gilt insbesondere für die Personalhandlungen, die sich in der Importanz- und Sensitivitätsanalyse als ergebnisbestimmend erwiesen haben.

4.1.8 Abhängige Ausfälle

Abhängige Ausfälle sind in der Fehlerbaumanalyse zu berücksichtigen. Folgeausfälle und funktionelle Abhängigkeiten (z.B. gemeinsame Abhängigkeit von einem Hilfssystem) werden explizit modelliert, die verbleibenden abhängigen Ausfälle (GVA) können über parametrische Modelle in die Fehlerbäume eingebracht werden.

Entscheidende Bedingung für die Anwendung der Modelle zur Quantifizierung von GVA ist eine ausreichende Abstützung der Modellparameter auf Betriebserfahrung. Dies gilt insbesondere für die Komponentengruppen, die sich in der Importanz- und Sensitivitätsanalyse als ergebnisbestimmend erwiesen haben. Grundsätzlich sind Modelle zu bevorzugen, die bereits in atomrechtlichen Verfahren eingesetzt und begutachtet wurden, sofern diese dem geltenden Stand von Wissenschaft und Technik genügen. Die Wahl der jeweiligen Methodik ist nachvollziehbar zu begründen.

[11] Begriffserläuterungen im Anhang A

4.1.6 Reliability parameters for independent component failures

A PSA should generally make use of plantspecific reliability parameters[11]. The necessary information for a collection of such parameters can be found in the operational records of the plant. The technical documents on PSA (datavolume) explains in detail how to establish the parameters.

In the case that a sufficient plant-specific data base is not available, generic data can be used. If generic data is used, however, the applicability of such data has to be assessed and documented under consideration of plant-specific conditions. If components for which generic data are used contribute an essential part to the total frequency of hazard states, the applicability of the relevant generic reliability parameters has to be assessed plant-specifically and the assessment has to be substantiated in a comprehensible way.

4.1.7 Human actions

The functions required in the course of an event sequence can depend on human actions in different respects. The analysis of human actions comprises the identification, modelling and probabilistic assessment of actions by the operating personnel having an impact on event sequences. An analysis with an independent methodology is necessary in order to determine to what extent human actions contribute to event sequences. Numerous methods are available which can be used to carry out such an analysis. Methods which have already been used and peerreviewed in procedures relating to nuclear law should generally be preferred provided that these methods comply with the state-of-the-art of science and technology. The choice of the relevant method has to be substantiated in a comprehensible way. This is in particular valid for such human actions for which the importance and sensitivity analyses have shown that they have a decisive impact on the outcome.

4.1.8 Dependent failures

Dependent failures shall be considered in the fault tree analysis. Subsequent failures and functional dependencies (e.g. joint dependency on an auxiliary system) shall be modelled explicitly, the remaining dependent failures (CCF) can be incorporate

A decisive precondition for the application of models quantifying CCF is that the model parameters must be sufficiently based on operating experience. This is in particular valid for component groups for which the importance and sensitivity analyses have shown that they had a decisive impact on the outcome. Methods which have already been used and peer-reviewed in procedures relating to nuclear law should generally be preferred provided that these methods comply with the state-of-the-art of science and technology. The choice of the relevant method has to be substantiated in a comprehensible way.

[11] Explanations of terms see Appendix A

4.1.9 Unsicherheits-, Sensitivitäts- und Importanzanalysen

Die Häufigkeiten auslösender Ereignisse und die Zuverlässigkeit für die Systemkomponenten und die Personalhandlungen werden in der PSA durch Wahrscheinlichkeitsverteilungen beschrieben, aus denen sich der Erwartungswert[12] berechnen lässt und die darüber hinaus Informationen über die Abweichungen dieser Größen vom Erwartungswert beinhalten, so dass die Unsicherheiten zu den Erwartungswerten der Häufigkeiten von Gefährdungs- und Kernschadenszuständen quantifiziert werden können (Unsicherheitsanalyse). Bei der Quantifizierung des Ereignisbaumes sind daher Streubreiten der Zuverlässigkeitskenngrößen, z.B. in der Form von Intervallen zu verwenden, um ein Maß für die Ergebnisunsicherheiten zu erhalten.

Neben der Unsicherheitsanalyse ist auch eine Sensitivitätsanalyse durchzuführen. Mit der Sensitivitätsanalyse ist zu ermitteln, welche der in der Unsicherheitsanalyse berücksichtigten unsicheren Eingabedaten in besonders hohem Maße zur Ergebnisunsicherheit beitragen.

Der Einfluss von Komponenten, Systemen und Personalhandlungen auf die wesentlichen Ergebnisgrößen ist über die entsprechenden Importanzen, insbesondere die diagnostische Importanz[13], zu bewerten.

4.1.10 Durchführung der Auswertung und Ermittlung der Ergebnisse der Stufe 1 - Analysen

Die quantitative Auswertung der Ereignisablauf- und Fehlerbaumanalyse erfolgt im Hinblick der in Kapitel 2 formulierten Ziele der probabilistischen Sicherheitsanalyse. Als Ergebnis der Analyse sind Eintrittshäufigkeiten für Ereignisabläufe zu ermitteln, die zu Gefährdungs- bzw. Kernschadenszuständen führen und ihre Unsicherheiten sowie relevante Einflüsse auf diese Häufigkeiten aufzuzeigen. Hierbei sind Gefährdungs- und Kernschadenszustände getrennt auszuweisen. Des Weiteren sind die Nichtverfügbarkeiten von Systemfunktionen zu ermitteln.

4.2 PSA der Stufe 2 für den Leistungsbetrieb

4.2.1 Anlagenspezifische Eingangsinformationen der PSA der Stufe 2

Relevante Ereignisabläufe und die ermittelten Kernschadenszustände der PSA der Stufe 1 sowie der Anlagenzustand und die Systemverfügbarkeiten dienen als Eingangsinformation und sind damit Ausgangszustände für die PSA der Stufe 2.

Merkmale und Eigenschaften der Anlagentechnik, die für das Anlagenverhalten unter Unfallbedingungen wichtig sind, sind bei der Modellierung des Anlagenverhaltens zu berücksichtigen. Maßnahmen des anlageninternen Notfallschutzes sind entsprechend den Regelungen des Notfallhandbuchs zu berücksichtigen. Unter sorgfältiger Prüfung ihrer Durchführbarkeit können Reparaturmaßnahmen in einer Unfallsituation in den Analysen berücksichtigt werden, wenn der schwierige Entscheidungsprozess für ihre Durchführung berücksichtigt wird. Der Beitrag ist gesondert auszuweisen.

[12] Begriffserläuterungen im Anhang A
[13] Definition der Importanzmaße siehe Methodenband, Anhang C

4.1.9 Uncertainty, sensitivity and importance analyses

The frequencies of initiating events and the reliability of the system components and human actions are described in the PSA by probability distributions from which the expectation value[12] can be calculated. The probability distributions further comprise information on the deviations of these parameters from the expectation value so that the uncertainties of the expectation values of frequencies of hazard states and core damage states can be quantified (uncertainty analysis). In quantifying the event tree, variations of reliability parameters, e.g. in the form of intervals, shall be used in order to have a measure for the result uncertainties.

A sensitivity analysis shall be carried out in addition to the uncertainty analysis. The sensitivity analysis is supposed to determine which of the uncertain input data considered in the uncertainty analysis contribute to a particularly large extent to the uncertainty of the result.

The impact of components, systems and human actions on the key result parameters is to be assessed with the help of the relevant importances, in particular the diagnostic importance[13].

4.1.10 Performance of the analysis ad determination of the results of the Level 1 analyses

The quantitative analysis of the event sequence and fault tree analyses is carried out under consideration of the objectives of the probabilistic safety analysis defined in section 2. Occurrence frequencies for event sequences which lead to hazard and/or core damage states shall be determined as results of the analysis and their uncertainties as well as relevant impacts on these requencies shall be indicated. In the results, hazard states and core damage states shall be listed separately. Furthermore, non-availabilities of system functions shall be determined.

4.2 PSA Level 2 for full power operation

4.2.1 Palnt-specific initial information of PSA Level 2

Relevant event sequences and the determined core damage states from the PSA Level 1 as well as the plant status and system availabilities serve as initial information and are therefore considered as initial conditions for the PSA Level 2.

Features and characteristics of the plant technology which are important for the plant behaviour under accident conditions have to be considered in the modelling of the plant behaviour. Measures relating to on-site accident management have to be considered according to the regulations set out in the emergency manual. Repair measures in an accident situation may be incorporated in the analyses provided that their operability is carefully verified, as long as the difficult decision process for their implementation is taken into account. Their contribution must be separately indicated.

[12] Explanations of terms see Appendix A
[13] For a definition of the importance measures see the technical documents on PSA, methods-volume, Appendix C

4.2.2 Festlegung repräsentativer Kernschadenszustände und Unfallabläufe

Auf der Basis der in der PSA der Stufe 1 analysierten auslösenden Ereignisse und deren ermittelten Kernschadenszuständen sind repräsentative Kernschadenszustände, für die jeweils eine gemeinsame Analyse durchführbar ist, auszuwählen und für die Ereignisbaumanalyse aufzubereiten. Unabhängig vom gewählten Verfahren (gestuft oder integral, s. Abschnitt 3.2) ist bei der Zusammenfassung der Kernschadenszustände sicherzustellen, dass die möglichen Anlagenzustände und Systemverfügbarkeiten hinreichend vollständig, z.B. anhand eines definierten Spektrums charakteristischer Merkmale, berücksichtigt werden. Weiterhin sind hier Ereignisabläufe, die für die Belange der Stufe 1 unberücksichtigt bleiben könnten, im Falle einer Ergebnisrelevanz für die Stufe 2 zu berücksichtigen (vgl. Abschnitt 4.1.2).

Die Festlegung der zu untersuchenden Unfallabläufe soll vorrangig hinsichtlich des Integritätsverlusts der druckführenden Umschließung und des Sicherheitseinschlusses unter Berücksichtigung der wesentlichen möglichen unfallbestimmenden Phänomene und der möglichen Freisetzung radioaktiver Stoffe in die Anlagenumgebung erfolgen und im Ergebnis anlagenspezifische Freisetzungspfade ausweisen.

4.2.3 Deterministische Unfallablaufanalysen

Ausgehend von den repräsentativen Kernschadenszuständen werden für die wichtigsten Ereignisabläufe möglichst realistische Szenarien entwickelt, um die unfallbestimmenden Phänomene und Einflussgrößen, die Wirksamkeit von Notfallmaßnahmen, die zeitlichen Abläufe und das Verhalten des Sicherheitseinschlusses unter Einbeziehung seiner aktiven und passiven Funktionen möglichst realistisch abbilden zu können.

Es sind umfassende deterministische Analysen, d.h. Analysen mit festgelegten Rand- und Anfangsbedingungen, durchzuführen, die vom auslösenden Ereignis bis zur Freisetzung reichen. Dabei sind integrale Rechenprogramme zu verwenden, in denen thermohydraulische, physikalische und struktur-mechanische Modelle miteinander gekoppelt sind. Zusätzlich sind erforderlichenfalls Detailanalysen zu wesentlichen Phänomenen und Vorgängen durchzuführen, um die Ergebnisse der integralen Rechenprogramme zu ergänzen und abzusichern.

Die in den deterministischen Unfallablaufanalysen ermittelten physikalischen Parameter und Charakteristika von Anlagenzuständen und Anlagenverhalten in den einzelnen Unfallphasen fließen in die Ereignisbaum-analyse ein.

Anhang B4 enthält beispielhaft auslösende Ereignisse für deterministische Unfallabläufe bei DWR und SWR.

4.2.4 Ereignisbaumanalyse

Die probabilistische Ereignisbaumanalyse behandelt die Ereignisse vom Beginn der Kernzerstörung bis zu den Anlagenschadenszuständen, bei denen die Freisetzung von Radionukliden in die Anlagenumgebung im Wesentlichen abgeschlossen ist. Dabei werden die aufgrund der phänomenologischen Komplexität möglichen Variationen im Unfallablauf erfasst. Die Ereignisbaumanalyse ist dabei so zu strukturieren (zu verzweigen), dass die einzelnen Unfallphasen in Verbindung mit den unfallbestimmenden Phänomenen (z.B. Dampfexplosion, Strukturversagen, Wasserstoffverbrennung im Sicherheitsbehälter) und den Notfall-Systemfunktionen, wie z.B. den Funktionen zur Kühlung des teilzerstörten Kerns, sowie den Funktionen

4.2.2 Determination of representative core damage states and accident sequences

On the basis of the initiating events analysed in the PSA Level 1 and the core damage states determined, representative core damage states which can be jointly analysed have to be chosen and prepared for the event tree analysis. Independently of the procedure chosen (staged or integral procedure, see section 3.2), it must be ensured that while summarising the core damage states the potential plant conditions and system availabilities are taken into account in a sufficiently complete manner, e.g. with the help of a defined spectrum of characteristics. Furthermore, event sequences which may remain unconsidered for the purposes of the Level 1 analysis have to be taken into account for the Level 2 analysis if they are relevant for the result (cf. section 4.1.2).

The accident sequences to be investigated shall be determined principally with respect to the loss of integrity of the pressure boundary and the containment envelope, while taking into account the significant potential phenomena influencing the accident and the potential release of radioactive material into the environment of the plant. Plant-specific release paths shall be indicated in the result.

4.2.3 Deterministic accident sequence analysis

On the basis of the representative core damage states, scenarios as realistic as possible are developed for the most important event sequences in order that the phenomena influencing the accident and the parameters, the efficacy of accident management measures, the time sequences and the behaviour of the containment envelope under consideration of its active and passive functions can be represented as realistically as possible.

Comprehensive deterministic analyses, i.e. analyses with defined boundary and initial conditions, are to be conducted, reaching from the initiating event to the release. These analyses must make use of integral computation codes, in which thermohydraulic, physical and structural mechanical models are interlinked. Additional detailed analyses of significant phenomena and processes may also be necessary in order to supplement and support the results from the integral computation codes.

The physical parameters and characteristics of plant conditions and plant behaviour in the different stages of the accident, which have been determined in the deterministic accident sequence analyses, are used for the event tree analysis.

Appendix B4 contains exemplary initiating events for deterministic accident sequences in PWR and BWR.

4.2.4 Event tree analysis

The probabilistic event tree analysis deals with the events from the beginning of the core destruction to the plant damage states for which the release of radionuclides into the environment of the plant is mostly completed. This analysis establishes the possible variations in the accident sequence which are possible due to the complexity of the phenomena. The event tree analysis must be structured (branched) in such a way that the single stages of the accident are represented in relation to the phenomena influencing the accident (e.g. vapour explosion, structural failures, hydrogen combustion in the reactor containment) and the emergency system functions, such as the functions for cooling the partlydestroyed core and the functions for preventing large releases. The necessary

zur Verhinderung großer Freisetzungen abgebildet werden. Die Ermittlung der benötigten Verzweigungswahrscheinlichkeiten ist durch ergänzende Berechnungen und Abschätzungen vorzunehmen und nachvollziehbar zu dokumentieren. Hierbei können auch Modelle und Ergebnisse aus vergleichbaren Analysen verwendet werden, sofern die Übertragbarkeit überprüft und bewertet wird.

branching probabilities shall be determined through supplementary computations and estimations and shall be documented in a comprehensible way. Models and results from comparable analyses can also be used to this end if it is assessed and proved that these models and results can be applied to the present analysis.

4.2.5 Unsicherheits- und Sensitivitätsanalysen

Sofern Eingabedaten für die Ereignisbaumanalyse unsicher sind, sind sie nicht als Punktwert, sondern als entsprechende Verteilung einzugeben. Die übliche Technik zur Berücksichtigung der unsicheren Eingabedaten sind Monte-Carlo-Simulationen. Damit sind folgende Analysen durchzuführen:

- In einer Unsicherheitsanalyse ist zu ermitteln, mit welcher Bandbreite die Resultate der Ereignisbaumanalyse (also z.B. die Häufigkeit für Sicherheitsbehälter-Versagen oder für Freisetzungskategorien) versehen sind. Zur Kennzeichnung der Ergebnisunsicherheiten sind für die Kategorien von Anlagen-schadenszuständen und den Freisetzungskategorien neben den Erwartungswerten die 5 %-, 50 %- und 95 %-Fraktile anzugeben.
- In einer Sensitivitätsanalyse ist festzustellen, welche der unsicheren Eingabedaten (z.B. Phänomene, Zustände) besonders großen Einfluss auf die Bandbreite der Resultate haben.
-

4.2.5 Uncertainty and sensitivity analyses

In the event that input data for the event tree analysis are uncertain, they shall not be entered as point values but as the relevant distribution. Monte Carlo simulations are used as the standard method for taking into account uncertain input data. The following analyses must be conducted with the help of this method:

- An uncertainty analysis determines the range of the results from the event tree analysis (e.g. the frequency of failures in the reactor containment or the frequencies associated with release categories). For marking the result uncertainties, the 5 %, 50 % and 95 % quantiles have to be indicated, in addition to the expectation values, for the categories of plant damage states and the release categories.
- A sensitivity analysis shall be conducted to determine which of the uncertain input data (e.g. phenomena, conditions) have a particularly large influence on the range of the results.

4.2.6 Durchführung der Auswertung und Ermittlung der Ergebnisse der Stufe 2 - Analysen

Es sind die Häufigkeiten der Anlagenschadenszustände mit den zugehörigen Freisetzungen sowie ihre Unsicherheiten zu ermitteln. Die im Ereignisbaum auftretenden Abläufe sind in zweckmäßiger Weise zu kategorisieren (z.B. nach Kernzustand, Zustand Sicherheitseinschluss, unfallbestimmende Einzelphänomene) und jeweils mit dem auslösenden Ereignis anzugeben. Insbesondere sind die möglichen Freisetzungen zweckmäßig in Kategorien einzuteilen (Freisetzungskategorien) und ihre jeweilige Häufigkeit zu bestimmen.

Der Einfluss der berücksichtigten mitigativen Notfall-Systemfunktionen auf die Häufigkeiten von Anlagen-schadenszuständen ist quantitativ zu ermitteln und auszuweisen.

4.2.6 Performance of the analysis and determination of the results of the Level 2 analyses

The frequencies of different plant conditions shall be determined as well as the associated releases and uncertainties. The sequences appearing in the event tree shall be categorised in an appropriate manner (e.g. according to the core condition, condition of the containment envelope, single phenomena influencing the accident) and shall be indicated together with the relevant initiating event. In particular the potential releases shall be categorised in an appropriate manner (release categories) and their relevant frequencies shall be determined.

The impact of the mitigative emergency system functions on the frequencies of plant conditions shall be quantitatively determined and indicated.

5. Dokumentation

Die Dokumentation der Erstellung und Durchführung der Analysen, der Maßnahmen zur Qualitätssicherung und der Ergebnisse ist nachvollziehbar zu gestalten. Insbesondere müssen Voraussetzungen, Annahmen, Zwischenschritte, Erhebung und Verwendung von Expertenurteilen, Schlussfolgerungen der Analysen und ggf. nachvollziehbare Begründungen für die Übertragbarkeit aus Referenzanalysen ersichtlich werden.

Die Dokumentation umfasst:

- verwendete Unterlagen und wesentliche Eigenschaften der Anlage,
- verwendete Rechenprogramme, -modelle und Datenbanken,
- Dokumentation der programmtechnischen Auswertung,
- Qualitätssicherung sowie
- Ergebnisse, Angaben zu deren Unsicherheiten und Ergebnisbewertung.

Für die PSA der Stufe 1 sind auszuweisen:

- analysierte auslösende Ereignisse und

5. Documentation

The preparation and performance of the analyses, the measures used for quality assurance and the results must be comprehensibly documented. The documentation shall include In particular postulates, assumptions, intermediate steps, requests for and use of expert judgements, conclusions of the analyses and, if appropriate, comprehensible justification for the application of reference analyses.

The documentation shall comprise:

- documents used and essential characteristics of the plant;
- computation codes, computation models and data bases used;
- documentation of the computer analysis;
- quality assurance; and
- results, data on the uncertainties associated with the results and evaluation of the results.

The following documentation is required for a PSA Level1:

- initiating events and event sequences analysed as well as a justification of the spectrum of events

Ereignisabläufe sowie Begründung des Ereignisspektrums,
- Ereignisablauf- und Fehlerbaumanalysen,
- Wirksamkeitsanalysen,
- verwendete Zuverlässigkeitskenngrößen,
- verwendete Komponentenmodelle für unabhängige und gemeinsam verursachte Ausfälle,
- Einbeziehung von Personalhandlungen in die Analysen.

Für die PSA der Stufe 2 soll die Darstellung insbesondere umfassen:
- ausgewählte repräsentative Ereignisabläufe mit charakteristischen Kernschadenszuständen (sofern die Stufe 2 nicht integral modelliert wird),
- deterministische Unfallablaufanalysen, Ergebnisse der Integralcoderechnungen und ggf. zusätzliche Einzelphänomenanalysen,
- Aufbau und Quantifizierung des Ereignisbaumes einschließlich der Verzweigungswahrscheinlichkeiten,
- relevante Ereignisabläufe sowie Freisetzungskategorien und deren Häufigkeiten.

Es ist ein zusammenfassender Bericht zur PSA zu erstellen, der die Annahmen, Begründungen, Modelle, Daten sowie die Ergebnisse und Folgerungen umfasst.

analysed;
- event sequence and fault tree analyses;
- analyses of efficiency;
- reliability parameters used;
- component models used for independent and common cause failures;
- incorporation of human actions into the analyses.

The documentation for a PSA Level 2 shall comprise in particular:
- selected representative event sequences with characteristic core damage states (provided that Level 2 is not modelled integrally);
- deterministic accident sequence analyses, results of the integral code computations and, if appropriate, additional analyses of single phenomena;
- development and quantification of the event tree including the branching probabilities;
- relevant event sequences as well as release categories and the associated frequencies.

A summary report for the PSA must be prepared which comprises the assumptions, justifications, models, data as well as the results and conclusions.

6. Rechenprogramme

Die Analysen der Stufe 1 (für Leistungs- und Nichtleistungsbetrieb) und für die Stufe 2 sind mit Programmen und Analysetools durchzuführen, deren Qualifizierung nachgewiesen ist.

Insbesondere gilt dies für die quantitative Auswertung von Ereignisablaufdiagrammen und Fehlerbäumen sowie für die Unsicherheits-, Importanz- und Sensitivitätsanalysen.

6. Computation codes

It has to be proven that the codes and analysing tools used for the Level 1 analyses (for full power operation and low-power and shutdown operation) and Level 2 analyses are qualified for this task.

This is in particular valid for the quantitative evaluation of event sequence diagrams and fault trees as well as for uncertainty, importance and sensitivity analyses.

7. Qualitätssicherung

Bei der Durchführung und Auswertung der PSA soll vom Ersteller ein Qualitätssicherungssystem angewendet werden, welches die „Allgemeinen Forderungen an die Qualitätssicherung“ der geltenden KTA-Regel 1401 erfüllt oder dieser Regel äquivalent ist. Die qualitätssichernden Maßnahmen und Arbeitsschritte sowie die diesbezüglich erreichten Ergebnisse sind nachvollziehbar und prüffähig zu dokumentieren.

7. Quality assurance

The person or persons responsible for performing and evaluating the PSA shall use a quality assurance system which complies with the “General requirements for quality assurance” set out in the applicable German KTA rule 1401 (safety standard set by the Nuclear Standards Committee) or is equivalent to this regulation. Quality assurance measures and work steps as well as the results reached in this context have to be documented in a comprehensible and verifiable manner.

8. Anhänge

Anhang A: Begriffserläuterungen für verwendete Begriffe

Anlagenspezifische Zuverlässigkeitskenngröße
Zuverlässigkeitskenngrößen sind Größen, die zur Quantifizierung der Zuverlässigkeit von Komponenten oder Systemen herangezogen werden (Ausfallraten, Ausfallwahrscheinlichkeiten). Anlagenspezifische Zuverlässigkeitskenngrößen sind Kenngrößen, die auf Daten und Informationen aus der Anlage basieren.

Ausgewogenheit
Die sicherheitstechnische Auslegung ist in Verbindung mit dem Betriebsreglement als ausgewogen anzusehen, wenn einzelne auslösende Ereignisse, Komponenten ausfälle oder Personalhandlungen das jeweilige Ergebnis nicht übermäßig dominieren.

Auslösendes Ereignis
Für den Leistungsbetrieb werden Störungen und Schäden an Komponenten und Anlagenteilen, die eine Anforderung von Sicherheitssystemen auslösen, als "auslösende Ereignisse" bezeichnet. Im Nichtleistungsbetrieb werden solche Ereignisse als „auslösend“ bezeichnet, bei denen

8. Appendices

Appendix A: Explanations of trems used

Plant-specific reliability parameters
Reliability parameters are parameters which are used to quantify the reliability of components or systems (failure rates, failure probabilities). Plant-specific reliability parameters are parameters based on data and information derived from the plant.

Balance
The safety-related design shall be considered well balanced in connection with the operating regulations if single initiating events, component failures or human actions do not dominate excessively the respective result.

Initiating event
During full power operation, disturbances and damage to components and parts of the plant initiating an actuation of the safety systems are called "initiating events". During low-power or shutdown operation, the term “initiating events” describes events for which the system functions

die Systemfunktionen zur Brennelementkühlung nicht im erforderlichen Umfang verfügbar bzw. bei denen die Systemfunktionen zur Reaktivitätskontrolle nicht ausreichend wirksam sind.

Leistungsbetrieb (LB)
LB, i.S. der für diesen PSA-Bereich zu berücksichtigenden Betriebszustände für auslösende Ereignisse, umfasst alle Betriebszustände im stationären Leistungsbetrieb.

I.A. wird der Leistungsbetrieb bei Nennleistung mit einer - je nach Analyseziel für PSA der Stufe 1 und Stufe 2 – zyklus-repräsentativen Kernbeladung angesetzt.

Nichtleistungsbetrieb (NLB)
NLB umfasst alle Betriebsphasen beim Abfahren aus dem stationären Leistungsbetrieb (Nennleistung oder Teilleistung), BE-Wechsel und Wiederanfahren in einen stationären Leistungsbetrieb.

Notfall-Systemfunktion
Als Notfall-Systemfunktionen (präventive, mitigative) werden diejenigen in einer Ereignisbaumanalyse eingebundenen Funktionen bezeichnet, die entsprechend dem jeweils vorliegenden Anlagenzustand gemäß Notfallhandbuch (einschließlich schutzzielorientierten Teil des BHB) zur Überführung in einen sicheren (d.h. Kern unterkritisch und langfristig ausreichend gekühlt) Anlagenzustand vorgesehen sind und ergriffen werden können. Hierzu können neben technischen Auslegungsreserven zusätzliche Einrichtungen und Personalhandlungen sowie Reparaturmaßnahmen zur Wieder-herstellung ausgefallener Systeme und Komponenten gehören. Präventive N.-S. werden während eines Ereignisablaufs zur Vermeidung eines Kernschadenszustandes (s.o.) einbezogen, mitigative N.-S. werden nach Eintritt eines Kernschadenszustandes zur Verminderung der Folgen einbezogen.

Freisetzungskategorien
Die Freisetzungskategorien sind mit den Häufigkeiten ihres Eintretens ein wesentliches Ergebnis der PSA der Stufe 2. Die Freisetzungskategorien fassen Abläufe aus den Unfallanalysen mit ähnlichen Radionuklidzusammensetzungen unter Berücksichtigung weiterer Charakteristika der Freisetzung (z.B. Nuklideigenschaften, wie insbesondere Radiotoxizität und Flüchtigkeit, Zeit des Ereignisses nach dem Beginn des Unfalls, Dauer, Höhe, Energieinhalt) zusammen.

Erwartungswert
Der Erwartungswert einer Zufallsgröße ist die Summe (Integral) über alle Werte, welche diese Zufallsgröße annehmen kann, gewichtet mit der jeweiligen Wahrscheinlichkeit.

Freisetzung, früh
Als „früh“ bezeichnet man eine Freisetzung, wenn wegen des raschen Ereignisablaufes schadenseindämmende Maßnahmen des Katastrophenschutzes erst nach der Freisetzung und daher mit verminderter Wirkung zum Einsatz kommen können.

Eine Freisetzung innerhalb von wenigen Stunden nach Eintreten des auslösenden Ereignisses wird in der Regel als „früh“ anzusehen sein.

Hinweis: Das Merkmal „früh“ ist anlagen- und standortspezifisch zu konkretisieren. International werden beispielsweise 10 Stunden als Konkretisierung diskutiert.

Freisetzung, große
Eine Freisetzung wird dann als „groß“ bezeichnet, wenn sie Wirkungen in der Umgebung der Anlage zur Folge haben kann, die einschneidende Maßnahmen des Katastrophenschutzes erfordern.

for the cooling of fuel elements are not available to the appropriate extent and/or for which the system functions for reactivity

Full power operation
Full power operation in the sense of the operating conditions to be considered for initiating events in the context of this PSA comprises all operating conditions in steady-state full power operation.

In general, full power operation is assumed at the rated output with a core load representative for the cycle - depending on the analysis targets for a PSA Level 1 and Level 2.

Low-power and shutdown operation
Low-power and shutdown operation comprises all operating periods during shutdown from steady-state full power operation (rated output or partial output), change of fuel elements and restart-up aiming at steady-state full power operation.

Emergency system functions
Emergency system functions (preventive, mitigative) are such functions incorporated in an event tree analysis which are designed, and can be implemented, to transform the current plant condition in a safe plant condition (i.e. core is subcritical and sufficient long-term cooling is provided) according to the emergency manual (including protection goal oriented part of the operating manual) based on the present plant condition. This may include technical design resources as well as additional installations, human actions and repair measures in order to restore systems and components which have failed. Preventive emergency system functions are used during an event sequence in order to avoid a core damage state (see above), while mitigative emergency system functions are used once a core damage state has occurred in order to minimise the consequences.

Release categories
The release categories together with the frequencies of their occurrence are a key result of a PSA Level 2. Release categories summarise sequences from the accident analyses with similar radionuclide combinations with respect to further release characteristics (e.g. nuclide properties, in particular radiotoxicity and volatility, time of the event after the beginning of the accident, duration, level, energy content).

Expectation values
The expectation value of a random variable is the sum (integral) of all values this variable can assume, weighted with the respective probability.

Release, early
A release is considered an “early” release if, due to the rapid event sequence, disaster control measures to confine the damage can only be implemented after the release so that their efficiency is reduced.

A release within a few hours from the occurrence of the initiating event is generally regarded as an “early” release.

Note: The property “early” has to be concretised plant-specifically and site-specifically. A concretisation of, e.g., 10 hours is discussed on the international level.

Release, large
A release is considered a “large” release, if it can lead to consequences in the environment of the plant which require drastic disaster control measures.

Note: The property “large” has to be concretised plant-

Hinweis: Das Merkmal „groß“ ist anlagen- und standortspezifisch zu konkretisieren. International werden beispielsweise 10^{16} Bq für I und Cs diskutiert.

Gefährdungszustand
Anlagenzustand, bei dem die Kühlung der Brennelemente, nicht mehr von dafür auslegungsgemäß vorgesehenen Systemen beherrscht wird. Ohne weitere Maßnahmen tritt ein Kernschadenszustand ein. Ein Gefährdungszustand kann u.U. mittels anlageninterner Notfallmaßnahmen in einen sicheren Zustand (unterkritisch, langfristige Kernkühlung) überführt und der Eintritt eines Kernschadenszustands verhindert werden.

Kernschadenszustand
Anlagenzustand, der eintritt, wenn ein auslösendes Ereignis von den auslegungsgemäß vorgesehenen Systemen und von präventiven Notfallmaßnahmen nicht beherrscht wird und Kernmaterial (i.d.R. Steuerstabmaterial) im Reaktor oder im Brennelement-Lagerbecken zu schmelzen beginnt.

Ohne weitere Maßnahmen kann ein Anlagenschadenszustand eintreten.

Anlagenschadenszustand
Endzustand einer Anlage nach einem Kernschmelzablauf, zu einem Zeitpunkt, ab dem keine wesentlichen weiteren Freisetzungen radioaktiver Stoffe in die Umgebung mehr geschehen.

Sicherheitseinschluss
Der Sicherheitseinschluss ist das System aus Sicherheitsbehälter und umgebendem Gebäude sowie den Hilfssystemen zur Rückhaltung und Filterung etwaiger Leckagen aus dem Sicherheitsbehälter.

Sicherheitssystem
Das Sicherheitssystem ist die Gesamtheit aller Einrichtungen einer Reaktoranlage, die die Aufgabe haben, die Anlage vor unzulässigen Beanspruchungen zu schützen und bei auftretenden Störfällen deren Auswirkungen auf das Betriebspersonal, die Anlage und die Umgebung in vorgegebenen Grenzen zu halten.

PSA Stufe 1
Bei einer Analyse der Stufe 1 werden Ereignisabläufe ermittelt und quantifiziert, die zur Gefährdung der Brennelementkühlung führen können; Analyseergebnisse sind Eintrittshäufigkeiten der auslösenden Ereignisse solcher Ereignisabläufe sowie die Häufigkeiten von Gefährdungs- bzw. Kernschadenszuständen.

PSA Stufe 2
Bei einer Analyse der Stufe 2 werden, ausgehend von den Kernschadenszuständen, die möglichen weiteren Ereignisabläufe mit Kernschmelzen bis zur Freisetzung radioaktiver Stoffe in die Anlagenumgebung analysiert. Ergebnisse sind Art und Zeitbereiche des Barriereversagens sowie die Häufigkeiten von Anlagenschadenszuständen in Verbindung mit dem jeweiligen Ort und der Menge freigesetzter radioaktiver Stoffe.

PSA Stufe 3
Stufe 3 umfasst zusätzlich eine Untersuchung des Transports von radioaktiven Stoffen in der Umgebung der Anlage sowie die daraus folgenden Schäden und ihre zu erwartenden Eintrittshäufigkeiten.

specifically and site-specifically. On the international level, e.g., 10^{16} Bq is discussed for I and Cs.

Hazard state
Plant condition where the cooling of fuel elements is no longer under the control of the systems designed for this purpose. If no further measures are taken, a core damage state may arise. It is possible that a hazard state can be transformed into a safe plant condition (subcritical, long-term core cooling) by means of on-site accident management measures and that a core damage state can thus be prevented.

Core damage state
Plant condition which occurs if an initiating event is not controlled by the systems designed for this purpose and by preventive accident management measures, and if core material (generally control rod material) in the reactor or in the spent fuel pool starts to melt.

If no further measures are taken, a plant damage state may arise.

Plant damage state
Final condition of a plant after a core meltdown sequence at a time from which no essential further releases of radioactive material in the environment will occur.

Containment envelope
The containment envelope is the system consisting of containment vessel and the surrounding building as well as auxiliary systems to retain and filter possible leakages from the containment vessel.

Safety system
The safety system is the entirety of all systems of a reactor plant having the task of protecting the plant against unpermissible stress and, in the event that accidents occur, of keeping their effects on the operating personnel, the plant and its environment within the defined limits.

PSA Level 1
In a Level 1 analysis event sequences are determined and quantified which can be a hazard to the fuel element cooling; analysis results include frequencies of occurrence of the initiating events of such event sequences as well as frequencies of hazard states and/or core damage states.

PSA Level 2
In a Level 2 analysis, the potential further event sequences with core meltdowns up to the release of radioactive material into the environment of the plant are analysed on the basis of the relevant core damage states. Analysis results include the type and periods of barrier failures as well as frequencies of plant damage states in combination with the relevant place and amount of radioactive material released.

PSA Level 3
Level 3 comprises an additional investigation of the transport of radioactive material into the environment of the plant as well as the resulting damage and the frequencies of occurrence to be expected.

Anhang B
Referenzspektrum auslösender Ereignisse

Anhang B1
Referenzspektrum auslösender Ereignisse für einen Druckwasserreaktor im Leistungsbetrieb

	Lecks in einer Hauptkühlmittelleitung	Leckquerschnitt (cm²)
1	großes und mittleres Leck	> 200
2	kleines Leck 1	80 - 200
3	kleines Leck 2	50 - 80
4	kleines Leck 3	25 - 50
5	kleines Leck 4	25 - 50
6	kleines Leck 5	2 - 12
	Lecks am Druckhalter	Leckquerschnitt (cm²)
	kleines Leck am Drcukhalter durch Transienten:	
7	bei Ausfall Hauptspeisewasser	20
8	bei Ausfall Hauptwärmesenke	20
9	bei anderen Transienten	20
10	kleines Leck am Druckhalter bei Fehlöffnen eines Sicherheitsventils	40
	Leck in einer Anschlussleitung im Ringraum	Leckquerschnitt (cm²)
11	Leck	2 - 500
	Dampferzeuger-Heizrohrlecks	Leckquerschnitt (cm²)
12	kleines Leck 1	6 - 12
13	kleines Leck 2	1 - 6
	Betriebstransienten	
14	Notstromfall	
15	Ausfall Hauptspeisewasser ohne Ausfall Hauptwärmesenke (langfristig)	
16	Ausfall Hauptspeisewasser und Ausfall Hauptwärmesenke	
17	Ausfal Hauptwärmesenke ohne Ausfall Hauptspeisewasser	
18	Dampferzeuger-Überspeisung	
	Transienten durch Frischdampf-Leitungslecks	
	großes Leck:	
19	innerhalb des SHB (Sicherheitsbehälters)	
22	außerhalb des SHB	
	mittleres Leck:	
21	innerhalb des SHB	
22	außerhalb des SHB	
	Transienten durch Speisewasser-Leitungslecks	
	großes Leck:	
23	innerhalb des SHB	
24	außerhalb des SHB	
	mittleres Leck:	
25	innerhalb des SHB	
26	außerhalb des SHB	
	Betriebstransienten mit Ausfall der Reaktorschnellabschaltung (ATWS)	
27	ATWS bei Ausfall Hauptspeisewasser	
28	ATWS beim Notstromfall	
29	ATWS beim Ausfall Hauptwärmesenke und Hauptspeisewasser	
30	ATWS bei sonstigen Transienten	
	Analgenübergreifende Ereignsse	
	Interne	
31	Überflutung sicherheitstechnisch wichtiger Gebäudeteile auf Grund interen Ursachen	
32	Brand	
	Externe	
33	Flugzeugabsturz	
34	Explosionsdruckwelle	
35	Hochwasser	
36	Erdbeben	

Appendix B
Reference spectrum of initiating events

Appendix B1
Reference spectrum of initiating events for pressurised water reactor at full power operation

	Leaks in a main coolant line	leak cross-section (cm²)
1	large and medium-sized leak	> 200
2	small leak 1	80 - 200
3	small leak 2	50 - 80
4	small leak 3	25 - 50
5	small leak 4	25 - 50
6	small leak 5	2 - 12
	Pressuriser leaks	leak cross-section (cm²)
	small leak at the pressuriser caused by transients:	
7	due to loss of main feedwater supply	20
8	due to loss of main heat sink	20
9	due to other transients	20
10	small pressuriser leak due to inadvertent opening of a safety valve	40
	Leak in a connecting line in the annulus	leak cross-section (cm²)
11	leak	2 - 500
	Steam generator tube leak	leak cross-section (cm²)
12	small leak 1	6 - 12
13	small leak 2	1 - 6
	Operational transients	
14	loss of off-site power	
15	loss of main feedwater supply without loss of main heat sink (long-term)	
16	loss of main feedwater supply and loss of main heat sink	
17	loss of main heat sink without failure of main feedwater supply	
18	overfeeding of steam generator	
	Transients caused by leaks in the main-steam lines	
	large leak:	
19	inside the containment vessel	
22	outside the containment vessel	
	medium-sized leak:	
21	inside the containment vessel	
22	outside the containment vessel	
	Transients caused by leaks in the feedwater lines	
	large leak:	
23	inside the containment vessel	
24	outside the containment vessel	
	medium-sized leak:	
25	inside the containment vessel	
26	outside the containment vessel	
	Anticipated transients without scram (ATWS)	
27	ATWS due to loss of main feedwater supply	
28	ATWS due to loss of off-site power	
29	ATWS due to loss of main heat sink and main feedwater supply	
30	ATWS due to other transients	
	Plant-interfacing impacts	
	internal	
31	flooding of safety relevant parts of the building due to plant-internal causes	
32	fire	
	external	
33	aircraft crash	
34	explosion	
35	flooding	
36	earthquake	

Anhang B2

Referenzspektrum auslösender Ereignisse für einen Siedewasserreaktor im Leistungsbetrieb

	Leckstörfälle innerhalb SHB
1	Frischdampfleitungslecks unterschiedlicher Größe
2	Speisewasserlecks unterschiedlicher Größe
3	Leck im RDB-Boden
4	Lecks im Reaktorwasserreinigungssystem
	Leckstörfälle außerhalb SHB
5	Frischdampfleitungslecks unterschiedlicher Größe
6	Hilfsdampfleitungslecks unterschiedlicher Größe
7	Speisewasserlecks unterschiedlicher Größe
8	Lecks im Reaktorwasserreinigungssystem
	Sonstige Lecks
9	Lecks unterschieldicher Größe an der Kondensationskammer (z.B. Bruch einer Anschlussleitung außerhalb SHB)
10	Leck in einer Nebenkühlwasserleitung
11	Bruch einer flusswasserführenden Leitung im Maschinenhaus
	Transienten
12	Ausfall der Hauptwärmesenke
13	Ausfall des Speisewassersystems
14	Notstromfall
15	Betreibstransienten mit Ausfall der Reaktorschnellabschaltung (ATWS)
16	Fehlöffnen oder Offenbleiben eines S+E Ventils
17	Fehlöffnene von Turbinen- und Umleitstellventilen
18	Überspeisungs-Transiente
	Anlagenübergreifende Ereigniss
	Interne
19	Überflutung sicherheitstechnisch wichtiger Gebäudeteile auf Grund interen Ursachen
20	Brand
	Externe
21	Flugzeugabsturz
22	Explosionsdruckwelle
23	Hochwasser
24	Erdbeben

Appendix B2

Reference spectrum of initiating events for a boiling water reactor at full power operation

	Leak accidents inside the containment vessel
1	leaks in main-steam lines having different sizes
2	feedwater line leaks having different sizes
3	leak in the RPV bottom
4	leak in the reactor water purification system
	Leak accidents outside the containment vessel
5	leaks in the main-steam lines having different sizes
6	leaks in the auxiliary steam lines having different sizes
7	leaks in the feedwater lines having different sizes
8	leaks in the reactor water purification system
	Other leaks
9	leaks having different sizes in the pressure suppression pool, e.g. outside the containment vessel (break of a connecting pipe)
10	leak in a service water line
11	break of a line carrying river water into the turbine hall
	Transients
12	loss of the main heat sink
13	loss of the feedwater supply system
14	loss of off-site power
15	anticipated transients without scram (ATWS)
16	inadvertent opening or remaining open of a S&R valve
17	inadvertent opening of turbine and by-pass control valves
18	overfeeding transient
	Plant-interfacing impacts
	internal
19	flooding of safety relevant parts of the buildings due to plant-internal cause
20	fire
	external
21	aircraft crash
2	explosion
23	flooding
24	earthquake

Anhang B3: Beispiel für eine Liste der Betriebsphasen für den Druck- und Siedewasserreaktor im Nichtleistungsbetrieb

Betriebsphasen:

- Heiß unterkritisch,
- Abfahren über die Hauptwärmesenke,
- Abfahren mit dem Nachwärmeabfuhrsystem,
- Stillstand der Anlage, kalt unterkritisch,
- Anfahren der Anlage.

Appendix B 3: Example of a list of operating periods for pressurized and boiling water reactors in lowpower or shutdown operation

Operating periods:

- Hot Subcritical;
- shutdown via the main heat sink;
- shutdown via the residual heat removal system,
- plant outage period, cold subcritical;
- plant startup.

Anhang B4: Beispiel für das Spektrum auslösender Ereignisse für deterministische Unfallabläufe für Druck- und Siedewasserreaktoren im Leistungsbetrieb für PSA der Stufe 2

Anlagen mit DWR:

- Kleines Leck am kalten Strang einer Hauptkühlmittelleitung,
- Kleines Leck am heißen Strang einer Hauptkühlmittelleitung,
- Mittleres Leck an einer Hauptkühlmittelleitung,
- Leck über ein Druckhalter-Abblaseventil,
- Dampferzeuger-Heizrohrleck,
- Transiente nach Ausfall der sekundärseitigen Wärmeabfuhr,
- Transiente beim Ausfall der Notstromversorgung.

Anlagen mit SWR:

- nicht abgesperrtes Leck innerhalb des SHB,
- nicht abgesperrtes Leck außerhalb des SHB,
- Leck am Druckabbausystem,
- Transiente mit Ausfall aller Bespeisungssysteme,
- Transiente mit Ausfall der RDB-Füllstandsmessung und daraus folgenden Systemausfällen.

Appendix B 4: Example of the spectrum of initiating events for deterministic accident sequences for pressurized and boiling water reactors during full power operation for PSA Level 2

PWR plants:

- small leak in the cold leg of a main coolant line;
- small leak in the hot leg of a main coolant line;
- medium-sized leak in a main coolant line;
- steam generator tube leak;
- transients after failure of secondary side heat removal;
- transients due to failure of the Emergency Power Supply.

BWR plants:

- unisolated leak inside the containment envelope;
- unisolated leak outside the containment envelope;
- leak in the pressure suppression system;
- transients with failure of all injection systems;
- transients with failure of the RPV level measuring
- and the resulting system failures.