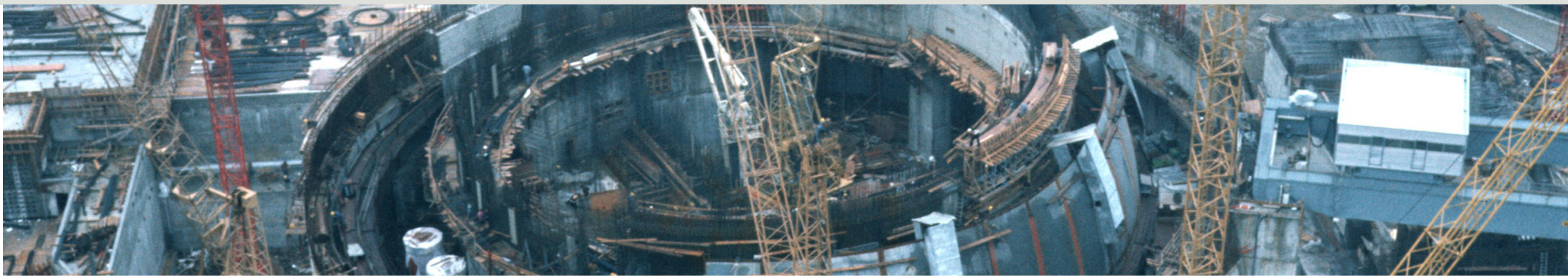
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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



Probabilistic Safety Analysis (PSA): Quality and Scope

Guideline for Swiss Nuclear Installations

ENSI-A05/e

Edition March 2009

Probabilistic Safety Analysis (PSA): Quality and Scope

Edition March 2009

Guideline for Swiss Nuclear Installations **ENSI-A05/e**

English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

Contents

Guideline for Swiss Nuclear Installations ENSI-05/e

1 Introduction

The Swiss Federal Nuclear Safety Inspectorate (ENSI) is the Regulatory Authority for nuclear safety and security of the nuclear installations in Switzerland. ENSI issues guidelines either in its capacity as a regulatory authority or based on a mandate in an ordinance. Guidelines are implementation support documents that formalize the implementation of legal requirements, and facilitate uniformity of the implementation practice. ENSI may allow deviations from the guidelines in individual cases provided that the suggested solution guarantees at least an equivalent level of nuclear safety or security.

2 Objective and Scope

The guideline ENSI-A05 defines the quality and scope requirements regarding the plant-specific level 1 and level 2 Probabilistic Safety Analysis (PSA) for both internal and external events and covering all operating modes of the nuclear power plants. In addition, this guideline establishes the PSA requirements for other nuclear installations.

The quality and scope requirements in this guideline shall ensure that in particular the following PSA applications are possible:

a. Assessment of overall plant safety

b. Assessment of the balance of the risk contributions

c. Assessment of the safety impact of plant modifications

d. Evaluation and rating of reportable events

e. Assessment of the safety importance of components

f. Probabilistic evaluation of operational experience

In accordance with international PSA practice, no requirements regarding the consideration of risks due to war, terror and sabotage are provided in this guideline.

3 Regulatory Basis

The regulatory basis for the implementation of PSA in the nuclear oversight process is defined in the Nuclear Energy Act (KEG, SR 732.1, 21 March 2003) and the corresponding Nuclear Energy Ordinance (KEV, SR 732.11, 10 December 2004).

Article 4 Paragraph 3 a KEG requires the applicant for a licence or the licensee of a nuclear installation to take all safety measures that are deemed necessary according to the experience and to the state of the art. PSA is an established method that shall be part of the decision basis for evaluation of the safety measures.

In addition, this guideline refers to following requirements of the Nuclear Energy Ordinance:

a. The PSA is a technical document according to Appendix 3 KEV that is required for obtaining a licence to operate a nuclear power plant (Article 28 Paragraph 1 KEV). The PSA shall be maintained throughout the lifetime of the plant (Article 41, Paragraph 1 KEV). Appendix 3 KEV defines the scope of the PSA.

b. According to Article 34 Paragraph 2 KEV, a PSA shall be submitted as part of the Periodic Safety Review.

c. Article 22 Paragraph 1 KEV requires the estimation of accident frequencies for the categorization of the potential hazard of nuclear installations. Paragraph 2 of the same article entrusts ENSI with defining in corresponding guidelines the methodology and the constraints for the analysis.

4 Technical Requirements for the Level 1 PSA of a Nuclear Power Plant

4.1 Scope of the Level 1 PSA

a. All the potential sources of significant radioactive releases in the nuclear power plant (NPP) shall be identified. If any of these sources are excluded from detailed consideration, the exclusion shall be justified.

b. The risk of radioactive release involving the spent fuel pool for the NPP at full-power operation shall be evaluated. If it can be shown based on conservative assumptions that the risk of radioactive release involving the spent fool pool is negligible (contribution to the Total Risk of Activity Release, *TRAR* less than 1%), no further analysis is necessary. Otherwise, a PSA shall be performed for the spent fuel pool, which follows the same requirements as set forth for NPPs.

c. The risk shall be analyzed for all operating modes of the plant. In case of non-full-power operation, both planned and unplanned shutdown shall be separately evaluated.

d. Internal events, internal plant hazards, and external plant hazards shall be accounted for and modelled within a single comprehensive PSA model. The PSA model can be subdivided into models for full-power, low-power and shutdown operation.

e. The plant-specific operational experience shall be reviewed in order to define the Plant Operating States (POS) for non-full-power operation.

f. The respective interfaces between the operating modes considered in the PSA shall be clearly defined and justified.

4.2 Component Reliability Data Analysis

4.2.1 Collection of Plant-Specific Raw Data

a. Consistent with the requirements of the systems analysis (see Chapter 4.4.3), the scope of the component types, the component boundaries, the component failure modes and a set of reliability parameters (e.g., failure rates per unit time or per demand) shall be defined and documented.

b. Components of the same type with similar design characteristics that are operated under similar conditions can be grouped together into a component group. For this grouping, attention shall be paid that the respective components have similar failure behaviour.

c. The evaluation of the plant documentation for determination of plant-specific raw data should be supported by the personnel in charge of the corresponding system at the plant.

d. It shall be verified that the component tests evaluated for data collection are representative for the demand.

e. In case of scarce (component-specific) operational experience, raw data from similar non-modelled components shall be considered.

f. If a component or a number of components have been replaced or significantly modified, it shall be discussed whether the operational data of the component group collected so far is appropriate for the modified component.

g. The documentation of component failures from operational experience shall comprise:

   - Component ID
   - Component group
   - Failure mode
   - Root cause of the failure
   - Date of failure
   - Plant operating mode
   - Reference to the plant documentation

h. The documentation of component unavailabilities due to repair, maintenance (or tests) shall comprise:

   - Component ID
   - Component group
   - Date of begin of the unavailability
   - Duration of the unavailability
   - Plant operating mode
   - Reference to the plant documentation

i. The number of demands and the number of operating hours shall be derived and documented from the plant documentation.

j. The collected component reliability data shall be stored electronically.

4.2.2 Generic Reliability Data

a. Generic reliability data from accepted international references shall be used together with the associated uncertainties in order to account for a broader range of operational experience.

b. The generic data shall be evaluated for their applicability to the subject plant equipment in consideration of the design, operational characteristics, grouping, boundaries, and failure modes of the equipment.

4.2.3 Development of Plant-Specific Reliability Parameters

a. The plant-specific reliability parameters shall be derived for each component group by combining the collected plant-specific raw data with the generic reliability data through a Bayesian update process.

b. For industrial mass products (e.g., electronic circuits), for which typically no plant-specific failure statistics are collected, generic data can be used directly.

c. Component data from the full-power PSA can be applied to the non-full-power PSA if they comply with the grouping requirements described in Chapter 4.2.1 b. Otherwise, shutdown-specific component data shall be provided.

d. The mean failure probability and a statistical representation of the associated uncertainty (5th, 50th, 95th percentile) shall be provided for each reliability parameter. The uncertainty distribution resulting from the Bayesian update shall be directly used or mapped by an appropriate distribution (e.g., β or γ distribution).

4.2.4 Development of Plant-Specific CCF Parameters

a. The minimum scope of components for which common cause failure (CCF) parameters shall be determined is listed in Chapter 4.4.3 i.

b. Components known to have significant coupling factors with regard to CCFs (i.e., design, operational and maintenance conditions, etc.) shall be grouped to CCF groups.

c. The accepted CCF parameter models are the Alpha Factor and the Multiple Greek Letter models. The determination of the CCF parameters shall be based on plant-specific evidence and generic data. The generic CCF data shall be evaluated for their applicability to the subject plant equipment and uncertainties in the CCF parameters shall be considered.

4.3 Human Reliability Analysis

4.3.1 Identification and Screening of Personnel Actions

a. Category A actions: For each system modelled in the PSA, human interactions that may degrade the system availability shall be identified. Alignment/configuration errors when equipment is restored to service following testing or maintenance, and miscalibration of equipment and systems for measurement data acquisition are of particular significance in this identification.

b. If a fault tree analysis is performed in order to quantify an initiating event frequency, potential human errors that may lead to the initiating event (errors in tests, maintenance, repair, and in the management of operational disturbances) shall be identified and modelled.

c. Category C personnel actions shall be identified in the context of the accident sequence analysis (see Chapter 4.4.2).

d. Whether personnel actions with negative impact on the accident sequence ("Errors of Commission" - EOCs) have been identified shall be stated. In the case that EOCs have been identified, their consequences and possible countermeasures shall be discussed.

e. Measures to restore system functions in accident sequences ("Recovery Actions") can be taken into account in the case of independent component failures if they are plausible and realizable in the considered accident scenario. The analysis of recovery actions shall in particular take into account the identification of the affected components, accessibility, availability of resources (e.g., qualified personnel), the support of procedures and the mean repair time derived from the operational experience. These measures shall be analyzed as category C actions.

f. Category A and B actions can be screened out based on qualitative criteria. For example, Category A actions can be screened out provided these actions affect components:

   - that are actuated automatically on demand,
   - in systems subject to a function test after a maintenance or repair, through which the error will be discovered,
   - whose status is displayed in the control room, periodically controlled and modifiable from the control room, or
   - for which there is a requirement to check their status at least once a shift.

   The criteria for screening out these personnel actions shall be documented.

4.3.2 Assessment of Human Error Probabilities

4.3.2.1 Category A Actions

a. The failure probabilities of Category A actions, also referred to as Human Error Probabilities (HEPs) shall be estimated in a systematic quantification process. Acceptable methods are the “statistical method” (i.e., quantify the errors solely on a statistical basis using generic and plant-specific experience), as well as THERP and ASEP.

b. For the detailed quantification, the following factors shall be considered:

- Quality of written procedures relating to the task execution and verification,
- Availability of instrumentation and indications for error detection, and
- Other factors that impact human performance (such as noise or time restrictions).

c. Each category A action credited in the PSA shall be documented in accordance with Appendix 4.

4.3.2.2 Category B Actions

a. Category B actions shall be quantified using the same methods as for Category A actions.

b. Personnel actions to prevent an initiating event shall be quantified as Category C actions.

4.3.2.3 Category C Actions

a. Category C actions can only be credited if relevant procedural guidance is available and/or the actions have been included as part of crew training. Crediting actions without procedural guidance shall be justified.

b. For the quantification of the failure probabilities of category C actions, acceptable quantification methods are THERP, ASEP, and SLIM variants accepted by ENSI, and the statistical method described in Chapter 4.3.2.1.

c. The assessment of HEPs shall consider both the diagnosis/decision aspect and the execution aspect of the human actions.

d. The following plant-specific and scenario-specific impacts on human performance shall be accounted for in estimating the HEPs:

- Characteristics and frequency of the operator training and experience,
- Quality of the written procedures,
- Availability of instrumentation and ergonomic quality of the human-machine interface,
- Clarity/unambiguousness of the cues and indications,
- Time available and time required to complete the task,

- Complexity of the response (e.g., coordination and communication requirements),
- Environment in which the operators are working, and
- Accessibility, availability, and adequacy of required tools and equipment.

The assessment of these performance shaping factors (PSF) shall be documented for each personnel action. In addition, the documentation shall state which factors influence only the diagnosis/decision or the execution aspect of action, or both aspects.

e. In particular, actions outside the control room should be discussed with operators in order to identify possible problems with access or other factors limiting the feasibility of the considered action. Particular attention should be placed on the potential performance conditions that could exist in the post-initiator phase.

f. The quantification of Category C personnel actions shall be primarily scenario-specific. If an action is used in multiple scenarios, it shall be ensured that the quantification considers the worst case.

g. The available time window for personnel actions shall be based on plant-specific thermal-hydraulic analyses. The required time for completion of the task shall be derived from operator interviews or based on simulator observations.

h. If the statistical method is used for the quantification of failure probabilities of Category C actions, the requirements c, d, and g do not apply.

i. HEPs lower than 10^{-5} (mean) are not accepted by ENSI. For the assessment of actions that are based on the decision of the emergency response team, a lower limit of $5 \cdot 10^{-3}$ (mean) for the failure probability shall be applied.

j. Each Category C action credited in the PSA shall be documented in accordance with Appendix 3.

4.3.2.4 Dependencies

a. The following types of dependencies shall be systematically considered:
   - Dependencies within a task, where a task is defined as a group of actions that relate to a specific goal or system function,
   - Dependencies among Category A actions, and
   - Dependencies among Category C actions, and among Category B and C actions within the same accident sequence.

b. For each sequence with multiple post-initiator human errors (HEs), maximum levels of credit shall be applied. A maximum number of credited human post-initiator interactions per sequence shall be defined and justified. The minimum joint failure probability for Cat. C actions within an accident sequence is 10^{-5}. For sequences that include actions that are supported by the emergency response team, the applicable minimum joint failure probability can be reduced to 10^{-6}.

4.3.2.5 Uncertainties

a. Uncertainties shall be estimated for all HEPs. The uncertainty analysis shall include the variabilities in individual human performance as well as in the scenario-specific influences on the action under consideration.

4.3.3 Specific HRA Issues Related to Internal and External Plant Hazards

a. In general, the HRA for internal and external plant hazard scenarios shall consider the potential for:

- Increased stress and confusion,
- Reduced availability of personnel,
- Limited accessibility and habitability of relevant areas (e.g., rooms)
- Failed or erroneous instrument indications,
- Additional workload on personnel,
- Additional difficulties in the detection/diagnosis of certain hazards, and
- Limited accessibility to areas of the plant.

b. The impact of fires on the human error probabilities shall be evaluated, taking into account the adverse environment caused by fires (e.g., propagation of smoke or other by-products of combustion, unavailability of alarms and lighting, hindered access due to the actuation of fire suppression systems) and their negative influence on performance shaping factors.

c. The impact of internal floods on the human error probabilities shall be evaluated, taking into account the adverse environment caused by floods (e.g., high temperatures and poor visibility conditions due to steam, flooding of rooms, loss of lighting equipment) and their negative influence on performance shaping factors.

d. The impact of earthquakes on the failure probabilities of personnel actions shall be analyzed using the following procedure:

- The choice of parameters (e.g., earthquake acceleration, earthquake duration) that characterize an earthquake and their assumed effect on the error probabilities shall be defined and justified.
- The approach applied and the numerical values (such as increase factors) used to define the failure probabilities shall be justified.
- The psychological and possibly physical effects of the earthquake on the installation personnel shall be taken into account in the modelling of failure probabilities. In particular, the uncertainty about the installation state associated with stronger earthquakes shall be taken into account in determining the failure probabilities.

A model accepted by ENSI to adjust the failure probabilities of personnel actions to the earthquake intensity can be found in Appendix 5.

4.4 Internal Events

4.4.1 Initiating Events

4.4.1.1 Identification of Initiating Events

a. A comprehensive list of potential initiating events shall be identified with the involvement of plant personnel. To ensure that the list is as complete as possible, the following methods shall be applied:

- System Analysis – This consists of a systematic review of the systems and components, and of the test and maintenance practice at the plant.
- Use of Analytical Methods – “Master Logic Diagrams”, Failure Modes and Effects Analysis (FMEA), or other pertinent analytical methods.
- Evaluation of the operational experience – Those initiating events that have actually occurred, as well as precursor events that due to the intervention of operators and/or due to limiting systems did not lead to a reactor trip, shall be considered. For each of these events, at least the date and a brief description of the event group (see Chapter 4.4.1.2) shall be provided.
- Evaluation of generic operational experience – internationally recognized and available lists of initiating events for similar types of plant shall be evaluated.

b. The initiating event category “transient” shall include:

- Total or partial failures of front-line systems or support systems,
- Inadvertent actuation of safeguards, and
- Manual reactor trips.

c. The “Loss of Coolant Accident” (LOCA) event category covers breaks in water or steam carrying pipes. The subdivision into different leakage sizes and locations complies with the individual success criteria (necessary for the prevention of core or fuel damage).

d. Regardless of the subdivision made under letter c, the following specific LOCAs shall be explicitly considered:

- Interfacing Systems LOCA, i.e., LOCA caused by failure of a high/low pressure system boundary
- Excessive LOCA, i.e., catastrophic rupture of the reactor pressure vessel that exceeds the capacity of the ECCS
- Steam Generator Tube Rupture (SGTR – for PWR only)
- Non-isolable LOCAs outside the containment

e. In case of a non-full-power PSA, specific types of LOCA events shall be also considered (e.g., draindown events due to misalignment or loss of coolant from shutdown cooling systems).

f. Fuel mishandling, heavy load drops and events affecting reactivity control (e.g., boron dilution, control rod ejection) shall be discussed and if necessary taken into account in the non-full-power PSA.

4.4.1.2 Grouping and Screening of Initiating Events

a. In the case where initiating events are grouped, the licensee shall ensure that:

- All initiating events belonging to the same group have similar direct consequences and mitigation requirements in terms of plant response and success criteria for prevention of core or fuel damage.
- Those initiating events that have the potential for a large radionuclide release (e.g., steam generator tube rupture, catastrophic rupture of the reactor pressure vessel, interfacing systems LOCA, and unisolated breaks outside containment, etc.) shall be modelled independently in separate groups.
- The mitigation requirements for each individual event in the group are less restrictive than the requirements defined for the group.

b. With the exception of the LOCA class defined in 4.4.1.1 d., an event group with a frequency less than 10^{-8} per year can be screened out, provided that it does not lead directly to a core or fuel damage.

4.4.1.3 Quantification of Initiating Event Frequencies

a. The quantification of initiating event[1] frequencies shall be based on plant-specific raw data.

b. In order to account for broader experience of nuclear power plant operations, generic frequencies of initiating events (including uncertainties) from internationally recognized sources shall be compiled and their applicability to the subject plant shall be evaluated.

c. Generic data shall be appropriately combined with the plant-specific data using a Bayesian approach.

d. It is recommended to use fault tree modelling to derive initiating event frequencies resulting from the loss of support or other systems. Consistency of the fault tree results with plant-specific operating experience shall be demonstrated.

e. For LOCAs, the frequencies shall be estimated using generic data from international databases such as the OECD Piping Failure Data Exchange Project (OPDE) or from the results of expert interviews, as described in

[1] For simplicity, the term “Initiating Event” also refers to event groups as introduced in Chapter 4.4.1.2.

NUREG-1829. In order to assess the applicability to the subject plant, plant-specific characteristics and additional information such as insights from the in-service inspection program, "Leak before Break" (LBB) analysis or probabilistic fracture mechanics shall be taken into account. In substantiated cases, fracture frequencies can be based on probabilistic fracture mechanics analysis.

f. The frequencies of Interfacing Systems LOCAs shall be evaluated with due consideration of the possible failure locations, the type of barrier, the protective interlocks and the surveillance strategies.

g. Independent of a specific operating mode, the initiating event frequencies shall be expressed by the number of events per calendar year.

h. The mean frequency and a statistical representation of the associated uncertainty shall be provided for each initiating event of the PSA model. The uncertainty distribution resulting from the Bayesian update shall be directly used or mapped by an appropriate distribution.

4.4.2 Accident Sequence Analysis

4.4.2.1 Identification of Safety Functions

a. Safety functions of the subject plant necessary to prevent core or fuel damage following an initiating event shall be identified consistent with the existing plant response analysis and the plant-specific procedures.

b. The front-line systems that are required for successful performance of each safety function shall be identified.

4.4.2.2 Event Sequence Modelling

a. For each initiating event, potential event progression paths shall be developed by employing event sequence diagrams. This graphical representation shall be complemented by a description of each accident sequence in which, in particular, relevant design and operational characteristics as well as the requirements in the regulations shall be addressed.

b. Event sequences shall be represented in the PSA model by a linked fault tree or a linked event tree method. The modelling of event sequences shall reflect the chronological event progression to the extent possible.

c. Each event sequence shall be modelled until either a successful (i.e., safe and stable) end state, or a core or fuel damage state is reached.

d. A mission time of 24 hours shall be assumed in general for the performance of safety functions that are required to prevent core or fuel damage for each event sequence. In those special cases where an event sequence does not result in core or fuel damage state, nor a safe end state during the mission time, core or fuel damage shall be assumed unless it can be demonstrated that sufficient measures to reach a safe end state are available.

e. In case of a non-isolable LOCA outside the containment, it shall be assumed that a stable end state can only be achieved if the plant is cooled down to residual heat removal (RHR) entry conditions and RHR cooling is successfully put into operation.

f. For each modelled safety function, its dependence on the initiating event and on the success or failure of the preceding functions shall be identified.

g. In developing event sequences, the secondary effects caused by the initiating event or other subsequent events during the accident progression shall be properly taken into account. For example, in the case of a (large) LOCA, the phenomenological impacts or resulting harsh environments such as plugging of screens/filters due to debris or elevated temperature and humidity shall be accounted for, particularly with respect to their effect on the availability of systems and components.

4.4.2.3 Success Criteria Analysis

a. Success criteria in terms of the required systems and components (including the corresponding auxiliary systems) shall be identified and documented for each initiating event and specific event sequence.

b. Realistic and conservative thermal hydraulic analyses shall be performed to validate the success criteria.

c. For numerical analyses, validated computer codes shall be used.

4.4.3 Systems Analysis

a. For each front-line system, all support systems necessary for the function shall be identified. The front-line-to-support and support-to-support system dependencies shall be represented by a set of dependency matrices.

b. If unit-to-unit crossties are credited for some systems (e.g., diesel generators), the component dependencies across unit boundaries shall be taken into account.

c. Fault trees shall be employed to model the unavailabilities of the system functions. The system models shall be consistent with the as-built and as-operated state of the plant systems.

d. The system models shall include:

- Unavailabilities of active and passive components due to independent and dependent failures or test/maintenance activities
- Special failure modes (if applicable), such as flow diversion or spurious actuation
- Operational restrictions imposed by the plant Technical Specifications
- Functional dependencies including electrical power, cooling water, instrument air, actuation, etc.
- System operational alignments or configurations
- Impact of initiating events on system operability

- Human errors

e. The component models shall take into account:
   - Mission times, maintenance durations and frequencies, test intervals, detection times, number of demands, and number of failures,
   - Component failure modes (e.g., failure to start, failure during operation).

f. Modelling of both maintenance unavailability and an active failure mode within a single basic event shall be avoided.

g. Flow diversion as a failure mode for fluid systems may be ignored if the flow loss through the diversion path is negligible or unlikely to occur (e.g., in the case where more than two manual valves in the diversion path would have to be in the wrong position).

h. In order to circumvent the circular logic loops that may occur (due to reciprocal system dependencies), the logic loops shall be cut in such a way that they do not unduly distort the risk results.

i. CCFs shall be modelled for at least the following components:
   - Pumps
   - Diesel generators
   - Fans
   - Control rods
   - Motor-operated, pneumatic and check valves
   - Heat exchangers
   - Transmitters
   - Safety and pressure relief valves
   - MSIV
   - Batteries, chargers, inverters, relays
   - Circuit breakers, switches
   - Strainers

   International experience shall be used in order to check the completeness of the component types considered susceptible to CCFs.

j. The potential for inter-system CCFs shall be discussed taking into account coupling factors such as component type, manufacturer, common design characteristics, maintenance strategy, etc. If deemed necessary, these CCFs shall be modelled.

k. A systematic format (e.g., with a specific designator for systems, components, and component failure modes or human errors) shall be employed for coding basic events.

l. Combining several components into a common component (super-component) should take place only in isolated cases. Attention shall be paid to verifying that the failure of any single component has the same effect on the function of the super-component. The composition of super-components shall be documented in a comprehensible way

m. For each system modelled in the PSA, the plausibility of the main minimal failure combinations shall be verified and the total unavailability shall be documented.

4.5 Internal Plant Hazards

4.5.1 Selection Process and Selection Criteria

a. Internal fires and internal floods shall be analyzed in accordance with the requirements in Chapters 4.5.2 and 4.5.3 and included in the PSA model.

b. In addition, the following events shall be analyzed:

- Explosion
- Release of toxic gas
- Turbine missile

c. The events mentioned in b do not need to be included in the PSA model, when one of the following conditions is met:

- It can be shown with qualitative arguments that the hazard has a negligible contribution to the *CDF/FDF* (for example, if the impact on the plant does not lead to a demand of safety systems or the effects are already covered by events that have a significantly higher frequency of occurrence).
- A quantitative evaluation shows that the contribution to the *CDF/FDF* is less than 10^{-9} per year.

4.5.2 Internal Fires

4.5.2.1 Identification and Screening of Relevant Fire Compartments

a. The plant documentation shall be used to identify the following information:

- Fire compartments (according to the fire protection concept, “Brandschutzkonzept”)
- Fire loads (i.e., permanent, temporary and transient combustibles)
- Potential ignition sources (e.g., transformers, electrical cabinets, or welding activities) and vulnerable PSA components
- Routing of cables
- Fire protection equipment for fire detection and fighting and fire barriers and duration of their resistance to fire

b. A comprehensive and systematic plant walkdown shall be conducted in order to:

- verify the information collected from the plant documentation,

- investigate the physical distribution/separation of the potential ignition sources and the fire loads,
- identify and document potential fire propagation paths and fire scenarios,
- analyze vulnerability of PSA components to fire effects (heat and smoke) and to fire suppression actuation.

c. For all the operating states modelled in the non-full-power PSA, the differences with the full-power PSA regarding potential ignition sources, fire loads, fire propagation and fire suppression shall be identified.

d. All the information needed for the fire analysis shall be collected in a structured "Spatial Interaction Database".

e. Qualitative screening: A fire compartment can be screened out if the compartment does not contain any PSA equipment, and a fire occurring within the compartment does not cause an initiating event.

f. Quantitative screening: Fire compartments can be screened out to the extent that their cumulative *CDF/FDF* contribution is less than 10^{-8} per year. The *CDF/FDF* calculation shall be based on the following conservative assumptions:

   - All vulnerable equipment in the fire compartment where a fire can propagate shall be set as failed as a result of the fire, and
   - The failure of cables in the considered fire compartment leads to the worst conceivable impacts (failure or spurious actuation) for the corresponding equipment.

   The estimation of the fire event frequencies shall be performed according to the requirements in Chapter 4.5.2.2.

g. The results of the screening procedure (relevant and screened out fire compartments) shall be documented in a comprehensible way.

4.5.2.2 Determination of the Fire Event Frequencies

a. For each fire scenario identified in the relevant fire compartments, the frequency shall be determined. The types and quantity of ignition sources shall be considered.

b. The fire event frequencies shall be quantified by combining plant-specific data with generic data by means of a Bayesian technique. In particular, fire events caused by ignition sources that can typically be found in PSA-relevant areas of the installation shall be considered.

c. Each identified plant-specific fire event shall be described by providing at least the following information:

   - Plant operating state
   - Ignition source location
   - Root cause of the fire

- Actuation of fire detection and suppression systems
- Fire propagation and consequences (e.g., damaged equipment and fire barriers)

d. The applicability of the generic experience shall be verified.

4.5.2.3 Identification and Screening of Relevant Fire Scenarios

a. A fire propagation event tree shall be used to estimate the frequency of each fire scenario. The fire propagation event tree shall consider the fire event frequency and the availability of fire detection and suppression systems and of fire barriers in the fire compartment.

b. The HEPs of actions that are required for manual detection and suppression of a fire shall be quantified based on the methods referred to in Chapter 4.3.2.

c. The failure probabilities of the devices for automatic fire detection and fire suppression and the probability of open doors and fire dampers shall be directly estimated based on generic and plant-specific experience or through fault tree analysis.

d. The extent of damage (in terms of failed PSA components) of each fire scenario shall be estimated and documented as a function of the failure of the modelled fire detection and fire suppression systems, as well as the effectiveness of fire barriers (e.g., walls, doors, fire dampers, penetration seals).

e. It is recommended that the consequences of cable fires on their related components be assessed in a detailed manner ("Circuit Analysis"). In case such an analysis is not conducted, the conservative boundary conditions described in Chapter 4.5.2.1 f shall be applied.

f. The assumptions regarding the spatial separation and the effectiveness of the fire barriers shall be verified for selected fire compartments by means of a recognized fire simulation code or by hand calculation.

g. The frequencies of fire scenarios with similar consequences can be combined.

h. Fire scenarios can be screened out to the extent that the cumulative *CDF/FDF* contribution of all quantitatively screened out scenarios (including quantitatively screened out compartments) is less than 10^{-8} per year.

4.5.2.4 Estimation of the fire *CDF/FDF*

a. The fire *CDF/FDF* shall be calculated with the PSA model for internal events taking into account the frequencies of the relevant fire scenarios and the scenario-specific consequences and assuming that all the PSA components affected by the fire are failed.

b. The extent to which the HEPs considered in the PSA model for internal events need to be modified according to the requirements in Chapter 4.3.3 shall be checked.

c. For each building that contains PSA components, the total *CDF/FDF* contribution as well as the *CDF/FDF* contributions of the most important rooms/sectors shall be presented in table form.

d. For the quantification of the fire *CDF/FDF*, the uncertainties associated with the fire event frequencies and the failure probabilities of the manual and automatic fire detection and fire suppression shall be taken into account.

4.5.3 Internal Floods

4.5.3.1 Identification and Screening of Relevant Flood Areas

a. The plant documentation shall be used to identify the following information:

- Flood sources (e.g., water tanks and piping)
- Flood areas
- Potential flood causes (e.g., pipe breaks, spurious actuation of systems, or human-induced events such as overfilling tanks)
- Characteristics of the flood sources (e.g., location, capacity, type of flow medium, flow rate)
- PSA equipment that might be affected by the flood
- Design features for protection against flooding (e.g., drains, sump pumps, watertight doors, flood detection and suppression systems)

b. A comprehensive and systematic plant walkdown shall be conducted in order to:

- verify the information collected from the plant documentation,
- investigate the spatial distribution of potential flood sources,
- determine potential flooding propagation paths and identify flood scenarios,
- analyze vulnerability of the PSA equipment to flooding (e.g., critical flood level) and indirect flooding effects (e.g., spray, blast forces, elevated ambient temperatures).

c. For all the operating states modelled in the non-full-power PSA, the differences with the full-power PSA regarding potential flood sources, flooding propagation routes, flood detection and suppression shall be identified.

d. All the information needed for the flood analysis shall be collected in a structured “Spatial Interaction Database”.

e. Qualitative screening: a flood area can be qualitatively screened out if one of the following criteria is met:

- The flood area does not contain any PSA equipment, and a flood in that area does not cause an initiating event.

- It can be demonstrated under conservative assumptions (e.g., drains assumed to be blocked) that any PSA equipment within the flood area will not be affected by the floods (e.g., the expected maximum flood level is too low to fail equipment, the maximum consequential temperatures and humidities are below the equipment design values).

f. Quantitative screening: Flood scenarios can be quantitatively screened out to the extent that their cumulative *CDF/FDF* contribution is less than 10^{-8} per year. The *CDF/FDF* calculation shall be based on the following assumptions:

   - All equipment susceptible to effects of flooding in the flood area shall be assumed to be failed, and
   - The flood leads to the worst conceivable impacts (failure or spurious actuation) for the corresponding equipment.

   The estimation of the flood event frequencies shall be performed according to the requirements in Chapter 4.5.3.2.

g. The results of the screening procedure (relevant and screened out flood areas) shall be documented in a comprehensible way.

4.5.3.2 Determination of the Flood Event Frequencies

a. For each flood scenario identified in the relevant flood areas the frequency shall be determined. The types and quantity of flood sources shall be considered.

b. The flood event frequencies shall be quantified by combining plant-specific data with generic data by means of a Bayesian technique. In particular, flood events caused by flood sources that can typically be found in PSA-relevant areas of the installation shall be considered. It is recommended that the OPDE database be used for the generic data.

c. Each identified plant-specific flood event shall be described by providing at least the following information:

   - Plant operating state
   - Flood source location
   - Root cause of the flood
   - Propagation of the flood and consequences (e.g., damaged equipment)

d. The applicability of the generic data shall be justified and documented.

4.5.3.3 Identification and Screening of Relevant Flood Scenarios

a. The frequency of each flood scenario shall be determined based on the flood event frequency and the availability of flood detection and suppression systems in the flood area.

b. The time window until PSA-relevant equipment is affected by the flood shall be estimated. Flow rates, drainage rates, and critical volumes of the flood areas shall be considered.

c. The failure probability of personnel actions for flood detection and manual suppression of the flood sources shall be determined based on the methods referred to in Chapter 4.3.2.

d. The failure probabilities of the systems for automatic detection and suppression of the flood sources shall be estimated on the basis of statistical evaluations.

e. For each flood scenario, the consequences (in terms of failed PSA components) shall be estimated and documented. For this estimation, the failure of the flood detection and suppression capabilities shall be considered.

f. The frequencies of flood scenarios with similar consequences can be combined.

g. Flood scenarios can be screened out to the extent that the cumulative *CDF/FDF* contribution of all screened out scenarios (including the contribution of the flood areas that were quantitatively screened out) is less than 10^{-8} per year.

4.5.3.4 Estimation of the flood *CDF/FDF*

a. The flood *CDF/FDF* shall be calculated with the PSA model for internal events taking into account the frequencies of the relevant flood scenarios and the scenario-specific consequences and assuming that all the PSA components affected by the flood are failed.

b. The extent to which the HEPs considered in the PSA model for internal events need to be modified according to the requirements in Chapter 4.3.3 shall be checked.

c. For each building that contains PSA equipment, the total *CDF/FDF* contribution as well as the *CDF/FDF* contributions of the most important flood areas shall be presented in table form.

d. For the quantification of the flood *CDF/FDF*, the uncertainties associated with the flood event frequencies and the failure probabilities of the flood detection and suppression capabilities shall be taken into account.

4.5.4 Turbine Missiles

a. For the frequency of turbine missile generation, the following generic prior data shall be used: $1.1 \cdot 10^{-4}$ per year (5th percentile), $1.8 \cdot 10^{-4}$ per year (mean), $2.9 \cdot 10^{-4}$ per year (95th percentile).

b. Plant-specific and generic data for turbine missiles shall be combined using a Bayesian method.

c. Potential trajectories of the parts ejected from the turbine shall be determined. The following factors shall be considered: the speed of the projectiles (derived from the maximum rotation speed of the turbine shaft), the variation of the flight angle (the range between -25° and +25° measured from the rotational plane shall be considered) as well as potential obstacles (such as building or room walls).

d. Targets that, if hit, have the potential to lead directly or indirectly (e.g., by wall failure, flooding, or fire) to damage of a PSA component shall be identified.

e. Given a turbine missile event, the conditional probability of a missile strike shall be determined for each of the identified targets assuming that 4 missiles with independent trajectories are generated simultaneously.

f. Given a missile strike on an identified target, the conditional failure probability shall be evaluated for each of the affected PSA components. If a PSA component is hit directly, guaranteed failure shall be assumed.

g. The consequences of the four most adverse independent turbine missiles shall be analyzed. At the same time the PSA component unavailabilities caused by an induced turbine fire (e.g., due to ignition of hydrogen or seal and lube oil) shall be considered in the PSA model. In addition, the effects of hydrogen explosion and smoke shall be discussed.

4.6 External Plant Hazards

4.6.1 Screening Analysis and Screening Criteria

a. Earthquakes, extreme winds, tornadoes, external flooding and aircraft crashes shall be analysed and modelled in the PSA in accordance with the requirements in Chapters 4.6.2 - 4.6.6.

b. In addition, the following external hazards shall be considered in the screening analysis:

- Drought
- Erosion
- Forest fire
- High summer temperature
- Ice cover
- Industrial or military facility accident
- Landslide
- Lightning
- Low river water level
- Low winter temperature
- Pipeline accident
- On-site release of chemicals
- River diversion

- River transported material leading to water-intake plugging (e.g., logs, leaves, mussels, algae)[2]
- Snow (drift)
- Soil shrink-swell consolidation
- Ground transportation accidents

c. In addition, the following combinations of hazards shall be considered:

- Harsh winter conditions including snow (drift), low temperatures, and ice cover
- Harsh summer conditions including high temperatures, drought, forest fire, and low river water level

d. Events due to the hazards reported in b and c do not need to be modelled in the PSA, provided that one of the following conditions is met:

- It can be shown based on qualitative arguments that the hazard has a negligible impact on the *CDF/FDF* (e.g., if the consequences on the plant do not require the actuation of front-line systems or the consequences are already covered by events having a significantly higher frequency of occurrence).
- A bounding analysis of the *CDF/FDF* due to the hazard yields a result less than 10^{-9} per year.

4.6.2 Earthquakes

a. The seismic PSA shall include a probabilistic evaluation of earthquake hazards, a probabilistic evaluation of seismic fragilities, and an analysis of earthquake accident sequences. For vibratory ground motions caused by earthquakes, a detailed probabilistic assessment is required. In addition, the possibility of other seismic hazards and their relevance shall be assessed.

4.6.2.1 Vibratory Ground Motion

<u>Hazard Analysis</u>

a. A site-specific probabilistic seismic hazard analysis (PSHA) shall be performed to determine the annual frequencies of exceedance of vibratory ground motions at the nuclear installation site, including the uncertainties associated with such an estimate.

b. The PSHA shall meet the following methodological requirements:

- The PSHA shall comply with the SSHAC Level 4 methodology[3].
- The approach to analyse the effects of the site-specific soil conditions shall be equivalent to the SSHAC Level 4 methodology.

[2] Water intake plugging by the effects of external flooding shall be considered in the external flooding analysis (see Chapter 4.6.5).

[3] R. J. Budnitz, D. M. Boore, G. Apostolakis, L. S. Cluff, K. J. Coppersmith, C. A. Cornell, and P.A. Morris, “Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts”, Report NUREG/CR-6372, US NRC (1997)

- A comprehensive up-to-date database (containing, for example, geological, seismological, and geophysical data) shall be compiled. The database shall be maintained throughout the project.
- The hazard shall be quantified for earthquakes having moment magnitudes $M \geq 4.5$.
- Critical processes having a direct impact either on project results or on the reproducibility of these results shall be subjected to project-specific quality assurance procedures.
- The PSHA shall be comprehensively documented in a manner that allows for reviewing, applying, and updating the PSHA.
- The peer review process shall include a participatory review by ENSI.
- After completion of the PSHA project, the PSHA databases and software shall be maintained and the capability to provide presentations of PSHA data and results shall be kept.

c. The PSHA shall provide the following results:

- Ground motion results shall be provided for a reference subsurface rock outcrop condition, for the reactor building foundation level, and for the local ground surface, all for free-field conditions.
- The hazard shall be computed for the geometric mean of the two horizontal ground motion components and for the vertical component.
- Hazard curves for rock and soil shall be provided for spectral frequencies from 0.5 Hz to 50 Hz, and for the peak ground acceleration (PGA). For soil, the site-specific soil resonances shall be adequately represented.
- The hazard results shall be provided for ground motion levels from 0.025 g to at least the ground motion level corresponding to an annual exceedance frequency of 10^{-7} per year.
- The epistemic uncertainty (of the hazard) shall be represented by at least 25 curves aggregated and weighted based on similar characteristics (e.g., slope and level) or at least 25 equally weighted curves that have been developed, on statistical grounds, to accurately capture the epistemic variation in hazard.
- Uniform Hazard Spectra at 5% damping shall be provided for each order-of-magnitude change in annual exceedance frequencies from 10^{-2} per year to 10^{-7} per year inclusive.
- The PSHA documentation shall provide direct results, guidance, or a combination thereof, to facilitate the estimation of peak velocity, average spectral acceleration, and spectra at any damping value, as well as the selection of time histories.
- The horizontal components of the hazard results shall be deaggregated in terms of magnitude, distance, and epsilon (number of standard deviations).
- Sensitivity results (including a discussion) for the following items:

    - Hazard contributions by seismic source
    - Principal contributors to uncertainty
    - Upper limit ground motion estimates
    - Foundation/depth levels
    - Expert-to-expert comparisons
    - Comparison with previous hazard studies for Swiss NPPs

Fragility Analysis

d. For the fragility analysis, information related to the seismic capacity of structures and components shall be collected, e.g.,
    - List of PSA equipment including their locations
    - Layout drawings of piping
    - Preliminary list of structures and components potentially compromising PSA equipment, piping or other structures, or components relevant for PSA, e.g., based on the list of components ("Komponentenliste"), the Safety Analysis Report, or plant layout drawings
    - Seismic design documents of the components and structures (providing information related to, e.g., layout, dimension, material properties, anchorage, failure modes, design methods, and qualification test reports and results)
    - Generic information about seismic design and fragilities

e. A comprehensive and systematic walkdown of the plant and plant vicinity shall be performed according to international standards (e.g., EPRI-NP-6041-SL) in order to:
    - assess and verify the plant configuration,
    - evaluate the adequacy of seismic design documents in relation to the as-built plant configuration,
    - evaluate the potential for seismically induced LOCA, and the potential for seismically induced containment failure,
    - identify components and structures potentially compromising PSA equipment in case of earthquake (e.g., due to mechanical interaction, seismically induced fires, floods, and explosions),
    - identify and evaluate the dominant failure modes of components and structures compromising PSA equipment,
    - identify equipment known to be vulnerable to earthquakes such as tanks, masonry/block walls, raised floors, spring-mounted/supported equipment, and chatter-sensitive relays, contacts and switches,
    - identify anomalies (improperly installed components, corroded anchorage/connections, etc.),
    - identify issues related to seismic housekeeping,
    - complete the collection of data necessary for the fragility computation.

f. Based on the insights gained from the plant documentation review and walkdown, for each structure or component identified as being relevant, the seismic fragility due to the direct effects of vibratory ground motion shall be evaluated using a screening analysis as follows:

   - A ground motion value shall be selected as a screening level. For ground motions higher than the screening level, seismic failure of all structures and components and, consequently, guaranteed core damage/fuel damage shall be assumed. The risk contribution resulting from ground motions higher than the screening level should be less than 10% of the seismic *CDF* or *FDF*.
   - High seismic capacity structures or components can be screened out from a refined fragility investigation if the structure or component is shown to have a seismic High Confidence, Low Probability of Failure (*HCLPF*) capacity higher than the screening level and failure of the structure or component will not directly lead to a containment bypass. For the screened out structures and components, no structure or component-specific seismic failures need to be considered in the PSA model. The high seismic capacity can be demonstrated by conservative expert judgment.
   - For each structure or component that is not screened out and that has a significant importance value to *CDF/FDF* or the failure of which leads directly to a containment bypass, realistic fragility parameters shall be assessed.
   - For the remaining structures and components, conservative fragility parameters can be assessed by means of expert judgement.

g. For each structure or component vulnerable to the indirect effects of vibratory ground motion, the fragility parameters shall be determined as follows:

   - For mechanical interactions, the probability of the interaction and the conditional probability of failure (given the interaction) shall be estimated as a function of ground motion.
   - The conditional failure probability of structures or components affected by seismic-induced fires, explosions and floods shall be estimated as a function of ground motion or assumed to be 1.0 (guaranteed failure).

h. A comprehensive seismic equipment list shall be developed including the following information:

   - Component identification number
   - Location
   - Failure mode
   - Fragility parameters
   - *HCLPF*
   - Equipment affected by the failure and their failure mode and conditional failure probability

i. For the external power supply (grid and hydro plants), realistic fragility parameters shall be estimated.

j. With respect to a LOCA that may result from the effect of individual or cumulative leakage of small piping within the reactor coolant system pressure boundary, an equivalent LOCA shall be assumed. The size of the equivalent LOCA shall be determined based primarily on the insights gained from the plant walkdown.

k. In the case of non-full-power operation, differences in the potential for mechanical interactions, and fire and flood-relevant characteristics as compared with full-power operation shall be identified. The shutdown-specific plant conditions related to earthquake risk evaluation shall be assessed by analyzing outage schedules and activities, and conducting interviews with outage management personnel.

Analysis of Earthquake Accident Sequences

Earthquake accident sequences due to the effects of vibratory ground motions shall be comprehensively modelled and the associated risk shall be quantified.

l. Initiating events shall be defined as follows:

 - The ground motion range between the lowest *HCLPF* value and the screening value shall be covered by at least 7 initiating events.
 - For ground motions exceeding the screening value, one initiating event shall be defined.

m. The seismic initiating events together with the insights from the fragility analysis shall be incorporated into the PSA model taking into account the following requirements:

 - For ground motions exceeding the screening level, guaranteed core/fuel damage shall be assumed.
 - The HEPs used in the internal events PSA shall be reviewed and adjusted according to the requirements given in the HRA Chapter 4.3.3.
 - The PSA model shall explicitly reflect all seismically induced failures identified that were not screened out in the fragility analysis, i.e., not only the seismically weakest component or structure shall be modelled.
 - Direct and indirect failures of a component shall be modelled separately.

n. For the quantification of the seismic *CDF* and *FDF*, the uncertainties of initiating event frequencies and failure probabilities of components and structures as well as of human actions shall be considered. Possible correlations among seismic failures shall be identified and considered in the uncertainty analysis.

4.6.2.2 Other Seismic Hazards

a. In addition to the failures caused by the direct effects of the earthquake vibratory ground motions, other seismic hazards, such as fault displacement, landslide, soil liquefaction, soil settlement, seismically induced industrial hazards, and dam breaks shall be identified and their consequences discussed. It shall be evaluated whether the hazards lead to additional seismic failures that need to be included in the PSA model.

4.6.3 Extreme Winds

a. The analysis of extreme (translational) winds shall include a probabilistic evaluation of wind hazards and of wind-induced failures, and a quantification of *CDF/FDF* including uncertainties.

b. A comprehensive and up-to-date database on wind occurrences and peak wind velocities shall be developed consisting of:

- Site-specific historical wind velocity data (short-term)
- Wind data from long-term measurement for at least one other location (e.g., from a fixed weather station or an airport near the plant)

c. Long-term site-specific wind data shall be developed by considering the short-term site-specific and the wind data from the other locations.

d. If measured wind speeds have to be mapped to specific heights of interest, the Thom equation[4] shall be used:

$$v_1 = v_2\ (h_1/h_2)^{1/n}$$

with:

v_1 wind velocity at height h_1

v_2 wind velocity at height h_2

n constant depending on the surface roughness

e. A maximum wind speed exceedance frequency curve (yearly exceedance frequency versus maximum wind speed) shall be developed based on the long-term site-specific wind data using a Gumbel probability distribution for the data fit and extrapolation.

f. A plant walkdown shall be conducted. The walkdown shall include identification of vulnerable SSCs (including windows and appurtenances such as exhaust stacks for diesel generators and air intakes), and potential missile sources.

g. Realistic wind fragilities shall be estimated for the relevant SSCs. Uncertainties shall be taken into account.

[4] H.C.S Thom, “New Distributions of extreme Winds in the United States,” Journal of the Structural Division, Proceedings of the American Society of Civil Engineers, July 1968

h. The load case “extreme wind” shall be represented by an adequate number of initiating events.

i. For each wind category, a loss of offsite power shall be assumed.

j. For wind speeds greater than 180 km/h, failure of glass (windows) shall be assumed. The corresponding damage (e.g., due to water ingress, pressurization) in the affected building or room shall be considered in the PSA.

k. It shall be assumed that wind-induced failure of a structure causes failure of all equipment within the structure.

l. In addition to the direct wind effects, the potential and effects of indirect wind threats such as wind-induced missiles, and increased wind speeds between structures caused by channelling effects shall be identified and their consequences discussed.

4.6.4 Tornadoes

a. The analysis of tornadoes (i.e., extreme rotational winds) shall include a probabilistic evaluation of tornado hazards and of tornado-induced failures, and a quantification of the core and fuel damage risks including uncertainties.

b. The occurrence of tornadoes shall be assumed to be uniformly distributed within a rectangular area of 12,500 km^2 around the plants (lower baseline extending from Geneva to Schaffhausen). The mean annual frequencies of tornadoes shall be assumed as follows:

-	F0 and F1:	$2.3 \cdot 10^{0}$ per year
-	F2:	$2.2 \cdot 10^{-1}$ per year
-	F3 and higher:	$6.3 \cdot 10^{-2}$ per year

A lognormal distribution of the frequencies with an error factor of 10 shall be assumed.

c. The strike areas for tornadoes with various intensities shall be assumed as follows:

-	F0 and F1:	length = 3.8 km, width = 70 m
-	F2:	length = 5.1 km, width = 150 m
-	F3 and higher:	length = 19 km, width = 320 m

d. A plant walkdown shall be conducted. The walkdown shall include identification of vulnerable SSCs (including windows and appurtenances such as exhaust stacks for diesel generators and air intakes) and potential missile sources.

e. Realistic fragilities shall be estimated for the relevant SSCs. Uncertainties shall be taken into account.

f. The load case “tornado” shall be represented by an adequate number of initiating events.

g. For each tornado velocity category, a loss of offsite power shall be assumed.

h. For each tornado velocity category, failure of glass (windows) shall be assumed. The corresponding damage (e.g., due to water ingress, pressurization, pressure drop) in the affected building or room shall be considered in the PSA.

i. It shall be assumed that tornado-induced failure of a structure causes failure of all equipment within the structure.

j. In addition to the direct tornado effects (e.g., tornado-induced collapses), the potential and effects of indirect tornado threats such as tornado-induced missiles shall be identified and discussed.

4.6.5 External Floods

a. The analysis of external floods shall include a probabilistic evaluation of flood hazards and of flood-induced failures, and a *CDF/FDF* quantification including uncertainties.

b. The following categories of flooding events shall be considered:

   - Heavy rainstorms or sudden large snowmelt events causing a high river water level at the plant
   - Failures of water flow control structures (e.g., dams, weirs, levees) both up and downstream as well as on-site, including potential domino failures and simultaneous failures of remote water flow control structures (e.g., due to earthquakes)
   - Intense precipitation events at the plant and in the local vicinity

c. A plant walkdown shall be conducted. The walkdown shall include examination of:

   - The grades and drainage characteristics at the plant,
   - Local water flow control facilities including operational and maintenance requirements and procedures,
   - Pathways for water ingress,
   - Flood-exposed SSCs,
   - The potential for roof ponding (i.e., examination of roofs, roof drainage systems, maintenance procedures), and
   - Potential local factors that can exacerbate a flood (e.g., drain plugging or damming of a river by means of landslide).

d. A maximum river water level exceedance frequency curve shall be developed based on the site-specific measured data. If deemed appropriate, a Pearson-III probability distribution shall be used for the data fit and extrapolation. Topographical and hydrological characteristics (of the catchment basin and the local area) shall be taken into account. The resulting hazard curve shall be discussed in the light of national historical flooding events.

e. It shall be assumed that a dam or weir fails with a mean frequency of $6.4 \cdot 10^{-5}$ per year (lognormal distribution with error factor 10) with the following consequences:

- 100% reservoir inventory loss in 10% of the dam/weir failures
- 50% reservoir inventory loss in 80% of the dam/weir failures
- 20% reservoir inventory loss in 10% of the dam/weir failures

f. Hazards due to extreme rainfall in the local vicinity of the plant can be screened out in the PSA if associated threats such as roof ponding, water ingress, and electrical short-circuiting are not found to be a possibility or cannot lead to an initiating event. Otherwise, the initiating event frequency shall be estimated.

g. Hazard mitigation measures (e.g., opening of weir gates) shall only be credited in cases with sufficient warning time.

h. The response of relevant structures to hydrostatic and hydrodynamic loads (including short-term erosion and flood/debris impact) shall be analyzed. In the case of collapse of a building, guaranteed failure of all components within the building shall be assumed. In the case of water intrusion into a building, the flooding propagation paths and the PSA equipment affected shall be identified.

i. Water-intake plugging due to debris and sediments shall be considered.

j. For flooding events leading to flood levels above plant grade or above the elevation of offsite transformers or associated electrical equipment, a loss of offsite power shall be assumed.

k. Each category of flooding events not screened out shall be separately considered in the PSA model and the risk contribution quantified.

4.6.6 Aircraft Crashes

a. The aircraft crash analysis shall include an evaluation of aircraft crash frequencies, an evaluation of failures due to effects of aircraft crashes, and a *CDF/FDF* quantification including uncertainties.

b. For the risk analysis, the following three aircraft categories shall be considered in the PSA:

- Commercial aircraft (i.e., weight > 5.7 tons)
- Military aircraft
- Light aircraft (i.e., weight < 5.7 tons)

4.6.6.1 Commercial Aircraft

a. The risk contribution of the following initiating events shall be quantified:

- Commercial aircraft crash on the reactor building
- Commercial aircraft crash on the bunkered emergency building
- Commercial aircraft crash on other buildings, if relevant
- Commercial aircraft crash on the remaining plant area

<u>Determination of Crash Frequency</u>

b. Aircraft crash frequencies shall be estimated using a four-factor formula which considers a) the number of aircraft operations, b) the probability that an aircraft will crash, c) given a crash, the probability that the aircraft crashes into a 1-square-kilometer area where the plant is located and d) the virtual impact area.

$$F = \sum_{i,j} N_{i,j} \cdot C_i \cdot \rho_{i,j} \cdot A_{virt}$$

with:

F estimated annual aircraft crash impact frequency

$N_{i,j}$ estimated annual number of site-specific aircraft operations for each applicable summation parameter *i, j*

C_i aircraft crash rate per operation in the vicinity of the airport or per kilometre for the in-flight phase

$\rho_{i,j}$ aircraft crash conditional probability per square kilometre in the vicinity of the airport or per kilometre for the in-flight phase

A_{virt} virtual impact area (for a specific building or a plant area)

i index for flight phases

j index for airport or air corridor

c. Depending on the plant location, the analysis of the commercial aircraft crash frequency shall distinguish between the following flight phases:

- Operation in the vicinity of the airport (i.e., takeoff and landing), and
- In-flight operation.

d. The number of commercial aircraft operations $N_{i,j}$ shall be assessed realistically taking into account the past and the expected future variations.

e. Each airport within a radius of 50 km around the plant shall be considered.

f. For the crash rate in the vicinity of the airport, a lognormal distribution with mean value $C = 7.8 \cdot 10^{-7}$ and an error factor = 3 shall be assumed.

g. For the vicinity of the airport, the conditional aircraft crash probability per square kilometre $\rho_{AV,j}$ shall be calculated as follows:

$$\rho_{AV,j} = \frac{1}{\pi \cdot g^2 \cdot h_j^2} \left[km^{-2}\right]$$

with:

g no-power glide ratio (g = 17)

h_j mean flight altitude in the vicinity of the airport

h. For the estimation of the in-flight aircraft operations N, all air corridors within a radius of 100 km from the plant shall be considered. N and ρ shall be calculated for each air corridor separately.

i. For the crash rate for in-flight operation, a lognormal distribution with mean value $C = 5.8 \cdot 10^{-11}$ (per operation and per kilometre) and an error factor of 3 shall be assumed.

j. For in-flight operation the conditional aircraft crash probability per kilometre $\rho_{T,j}$ shall be calculated as follows:

$$\rho_{T,j} = \frac{d_j}{A_j} \left[km^{-1}\right]$$

with:

$$d_j = 2\sqrt{g^2 h_j^2 - b_j^2}$$

$$A_j = \pi\, g^2 h_j^2$$

and:

j index of air corridor

d_j flight distance in corridor j from which the NPP can be reached [km]

A_j crash exposure area for aircrafts coming from specific air corridor j [km^2]

g no-power glide ratio (g = 17)

h_j mean flight altitude for air corridor j

b_j horizontal component of the minimum distance between the air corridor j and the plant

k. The virtual impact area of a building shall be averaged from the virtual areas corresponding to four perpendicular aircraft approach directions:

$$A_{virt,building} = \frac{1}{4}\sum_{k=1}^{4} f_k \left(A_{gr} + \frac{A_{fr,k}}{\tan\varphi_k} \right)$$

with:

$A_{virt,building}$ virtual impact area of the building

A_{gr} ground area of the building (= [length of the building + ½ outer distance between aircraft engines] × [width of the building + outer distance between aircraft engines]), outer distance between aircraft engines assumed to be 25 m for commercial aircraft and 4 m for military aircrafts

$A_{fr,\,k}$ front area of the building for direction k (= [width of the building + outer distance between aircraft engines] × height of the building)

k aircraft approach direction

φ_k crash impact angle (assumed to be 30°)

f_k Topographical protection factor. If the minimum approach angle given by the (natural) topography around the plant is larger than 10°, f_k can be assumed $1/\sqrt{3}$, otherwise f_k = 1)

For the calculation of the virtual crash area shielding by adjacent buildings can be considered, taking into account φ_k and the real dimensions of the shielding buildings. Round buildings shall be treated as enveloping rectangular buildings.

l. The virtual impact area of the remaining plant area $A_{virt,plant\ area}$ is given by:

$$A_{virt,\,plant\,area} = A_{site} - \sum_m A_{virt,building,m}$$

with:

A_{site} circular area around reactor building with radius r = 100 m

m index of building

Direct Effects of an Aircraft Crash (Mechanical Impact)

m. For the reactor building and the bunkered emergency building, the conditional failure probability (given that the plane hits the building) shall be assessed taking into account the variability in aircraft type (e.g., dimensions, weights) and velocities. Local (i.e., wall penetration) and global (e.g., overturn, displacement) structural responses relative to the aircraft impact shall be considered.

n. The impact of crash-induced vibrations and accelerations on components within the reactor building and the bunkered emergency building shall be assessed.

o. For accident sequences involving penetration of the building wall, guaranteed failure of all equipment within the building shall be assumed.

p. For any building for which no conditional failure probability was assessed, guaranteed failure of all equipment located within the building shall be assumed if the aircraft hits the building. Furthermore, no actions of personnel present in the building shall be credited.

Indirect Effects of an Aircraft Crash (Missiles and Fire/Explosion Effects)

q. The effects of collateral mechanical loads and of fire/explosion resulting from a crash either on a building or on the remaining plant area shall be analysed and the failure probabilities of the buildings shall be assessed taking into account the variability in aircraft type.

r. For buildings designed against missile impact, only fire effects shall be assessed taking into account fire and explosion sources (e.g., amount of fuel from the aircraft, gas and oil storage in the plant area), pathways for smoke and hot gas (e.g., air intakes of emergency diesel generators) and pathways for fuel run-off on and into plant structures and along plant grades.

s. Guaranteed failure of all equipment located within the building shall be assumed if the protection against the indirect effects is assumed to be failed.

t. All outdoor equipment shall be assumed to be failed. In particular, a LOOP shall be assumed.

4.6.6.2 Military Aircraft

a. The risk contribution of the following initiating events shall be quantified:

- Military aircraft crash on the reactor building
- Military aircraft crash on the bunkered emergency building

b. The annual crash rate of military jet aircrafts per unit area shall be directly calculated from the number of crash occurrences in Switzerland. The time interval to be considered shall be at least 20 years. The uncertainty shall be described by a lognormal distribution with a mean value and standard deviation resulting from the data.

c. The effects of military aircraft crashes shall be assessed in the same manner as for commercial aircraft crashes.

4.6.6.3 Light Aircraft

a. The *CDF/FDF* contribution of light-aircraft (including helicopter) crashes on buildings that are not designed against missile impact shall be quantified.

b. The annual crash rate of light aircrafts per unit area shall be directly quantified from the number of crash occurrences in Switzerland. The time interval to be considered shall be at least 5 years. The uncertainty shall be described by a lognormal distribution with a mean value and standard deviation resulting from the data.

c. Guaranteed failure of all equipment located within the building (for buildings that are not designed to resist to the impact of missiles) shall be assumed if the aircraft hits the building.

d. The plant risk due to light-aircraft crash can be screened out if a bounding analysis of the *CDF/FDF* due to light-aircraft crash yields a result less than 10^{-9} per year.

4.6.7 Other External Hazards

a. For each external event (listed in Chapter 4.6.1) that is not screened out based on the criteria provided, the *CDF/FDF* contributions including uncertainties shall be calculated. The assessment shall include: (a) a detailed review of the relevant available information, (b) a plant walkdown (if necessary), (c) an identification of possible hazard scenarios, (d) a determination of the conditional probabilities of SSC failures (fragilities) and human errors, and (e) implementation of the event in the PSA model.

4.7 Quantification and Presentation of Level 1 PSA Results

4.7.1 Quantification

a. For the computation of the PSA results, a validated computer code shall be used. Limitations of the code or of the quantification method (e.g., missing capability to consider success probabilities in accident sequences) shall be discussed.

b. The selected truncation value for the sequence quantification shall be justified by a sensitivity analysis or by demonstrating a low contribution from unaccounted cutsets under conservative conditions (i.e., lower than 1% of the *CDF/FDF*).

c. The complete spectrum of hazards (internal and external) considered in the PSA shall be quantified based on a single integrated model.

d. Minimal cutsets/sequences with mutual exclusive basic events/split fractions shall be identified and eliminated.

e. All basic event and initiating event uncertainties shall be considered and propagated through the model.

f. The uncertainty analysis within the PSA shall consider the “correlation effect[5]”.

g. A plausibility check of the most important minimal cutsets leading to a core or fuel damage shall be performed.

4.7.2 Presentation of Level 1 PSA Results

4.7.2.1 Risk Profile

a. The *CDF/FDF* contributions categorized by groups of initiating events shall be provided as part of the PSA hardcopy documentation and in addition electronically:

[5] G. Apostolakis and S. Kaplan, “Pitfalls in Risk Calculations”, Rel. Eng. 2, 1981

Table 1: CDF/FDF contributions categorized by groups of initiating events

Group	**Initiating Event Category**	***CDF/FDF***				**% of Grand Total (Mean)**
		Mean	**5 %**	**50 %**	**95 %**	
	Transient					
	LOCA					
Internal Events (Total)						
	Fires					
	Internal floods					
	Other internal hazards					
Internal Plant Hazards (Total)						
	Earthquakes					
	Extreme winds & tornadoes					
	External floods					
	Aircraft crash					
	Other external hazards					
External Plant Hazards (Total)						
***CDF/FDF* (Grand Total)**						

b. The *CDF/FDF* contributions of all individual initiating events shall be provided as part of the PSA hardcopy documentation and in addition electronically.

Table 2: CDF/FDF contributions of all initiating events

Initiating Event			
ID	**Description**	**Frequency**	**Mean *CDF/FDF***
Seismic1			
Fire1			
…			

c. The *FDF* contribution of each plant outage state shall be provided as part of the PSA hardcopy documentation and in addition electronically.

Table 3: FDF contribution of each plant outage state

Operating State		**Reactor Cooling System**				**Contain-ment**	**Initiation of Safety Systems**	**Dura-tion [h]**	***FDF* [%]**
Abbr.	**Description**	***P*$_{abs.}$ [bar]**	***T* [°C]**	**Level Pressurizer (PWR), [%]**	**Cond. RPV**				
A1	*Cooling down*	*150-20*	*300-150*	*60*	*closed*	*closed*	*automatic*	*20*	*6.3*
A2	*Remove fuel*								
…									

d. In addition to the results listed above, the total contribution of ATWS sequences to the *CDF* shall be provided.

4.7.2.2 Importance Analysis

a. For each operating mode modelled (i.e., full power, low power and shutdown), the most important basic events, sorted by Fussell-Vesely (FV) and Risk Achievement Worth (RAW) values shall be provided (top 100 as hardcopy and top 1,000 electronically).

Table 4: Importance of basic events

	Basic Event ID	Description	Mean	*RAW/FV*
1				
2				

b. For each operating mode modelled, the most important components, sorted by *FV* and *RAW* values shall be provided. The lists shall contain at least all components with *RAW* > 2 or *FV* > $1 \cdot 10^{-3}$ and shall be provided as a hardcopy and electronically.

Table 5: Importance of components

	Component ID	Description	Mean	*RAW/FV*
1				
2				

c. For each operating mode modelled, the most important personnel actions, sorted by *FV* and *RAW* values shall be provided (top 30 as hardcopy and electronically).

Table 6: Importance of personnel actions

	Personnel Action ID	Description	Mean	*RAW/FV*
1				
2				

d. For each operating mode modelled, the *FV* and *RAW* values of all systems considered in the PSA shall be provided (as hardcopy and electronically).

Table 7: Importance of systems

	System ID	Description	*RAW/FV*
1	*TH*	*TH system with all safety functions*	
2	*TH Recirculation*	*TH system, safety function recirculation*	
3	*TH Injection*	*TH system, safety function injection*	

e. For each operating mode modelled, a list of about 10,000 most important minimal cutsets/sequences (where possible) shall be provided according to following table (electronically):

Table 8: Most important minimal cutsets

	CDF (FDF)	%	Minimal Cutset	
			Name	Description
1	*1.63E-06*	*6.00*	*IEXZ1*	*Initiating Event XZ1*
			XY111ABC	*Diesel 111 fails to start*
			AXYZNCC	*CCF of components XYZ*
2				

f. For each operating mode modelled, a ranking of the 30 most important accident sequences of the model according to following table shall be provided (hardcopy):

Table 9: Most important accident sequences

Sequence Number	
Sequence Frequency	
Percent of Total *CDF*	
Initiating Event	
Unavailability due to Initiating Event – **Direct, Guaranteed Failure** – **Dependent Failure (e.g., Fragility)**	
Support Systems Failed	
Front-Line Systems Failed	
Personnel Action Failed	
Description	

4.7.2.3 Assessment of Plant Modifications

The following sensitivity study shall be performed with the current PSA model and documented:

a. The influence of significant, PSA-relevant hardware changes performed in the past on the *CDF/FDF* (e.g., backfit bunkered emergency system) shall be determined.

Table 10: Risk impact of plant modifications

Date	Description of Plant Modification	Total *CDF*	Total *FDF*

4.7.2.4 Insights

a. Any (potential) plant improvements (backfits) or improvements of the procedural guidance identified during the development of the PSA shall be reviewed and documented. In particular, the insights gained from the plant walkdowns and the analysis of plant procedures shall be considered.

b. The plant's safety level in terms of *CDF/FDF* and the balance of the risk profile shall be discussed based on the criteria given in the guideline ENSI-A06.

c. Components having a high failure rate as compared to the international experience shall be identified and the reason for the increased failure rate shall be evaluated. The same process shall be applied to initiating events with high frequencies.

d. It shall be investigated whether a historical trend (improvement or deterioration) in the component reliability data or the initiating event frequencies can be observed.

e. The risk insights of the updated PSA shall be compared with the risk insights from the previous PSA performed for the same plant. Differences in the PSA results shall be discussed.

5 Technical Requirements for the Level 2 PSA of a Nuclear Power Plant

5.1 Definition and Quantification of Plant Damage States

a. Accident sequences of the Level 1 PSA with similar severe accident progression shall be grouped into plant damage states (PDS). The PDS shall be characterized by at least:

- The initiating event type (i.e., transient, LOCA, etc.)[6],
- The reactor coolant system pressure at the time of core or fuel damage (if the core is inside the vessel),
- The status of front-line systems,
- The containment isolation status[7],
- The accident sequences that result in containment bypass (i.e., steam generator tube rupture (SGTR) for PWR, and interfacing system LOCA), and
- The status of containment systems for heat removal or pressure reduction and of the systems for reduction of fission products.

b. For the grouping of the low-power and shutdown accident sequences, POS-specific characteristics such as the location of the fuel and the isolation status of the reactor vessel (e.g., vessel open/closed) shall also be considered additionally.

c. The number of PDS can be reduced by combining and/or screening of the PDS. The total frequency of the screened PDS shall be no higher than 1% of the *CDF*. Those PDS known beforehand to result in a high risk consequence (e.g., due to pre-existing containment failure or ATWS) shall not be screened out.

d. The uncertainties in the frequency for each PDS shall be derived from the Level 1 PSA.

e. The characteristics and mean frequencies of the PDS should be preferentially presented in terms of a PDS matrix.

5.2 Containment Performance

a. In order to determine the containment response to accident conditions, a structural response analysis shall be performed.

b. All relevant containment design information with regard to the structural response analysis shall be considered, such as:

- Properties of construction materials and reinforcement

[6] Only for separated Level 1/Level 2 models

[7] The containment isolation system and the containment heat removal systems credited in the Level 2 PSA shall be modelled explicitly using fault tree techniques.

- Sizes and locations of containment penetrations
- Penetration seal configuration and materials
- Local discontinuities, e.g., shape transitions, changes in steel shell or concrete reinforcement
- Potential interaction between the containment structure and neighbouring structures

c. The potential containment failure locations (e.g., failure of steel shell or failure of hatches and penetrations) to be considered in the structural analysis shall be identified.

d. A plant walkdown shall be conducted in order to verify the collected information.

e. Relevant plant-specific operational experience such as results from containment leakage tests and insights from the ageing surveillance program shall be considered in the structural response analysis.

f. The structural analysis shall consider quasi-static and dynamic over-pressure conditions. Additionally, over-temperature impact on containment performance shall be taken into account for quasi-static conditions.

g. Structure analyses using well-documented and peer-reviewed state-of-the-art techniques shall be performed for the identified containment failure locations. These analyses shall provide the best-estimate failure pressure at a given temperature for each location (ultimate pressure capacity) and the best-estimate failure modes (e.g., leakage, cracks, gross rupture, etc.).

h. The structure analyses shall provide an assessment of parametric and modelling uncertainties to arrive at the failure location fragilities. These fragilities shall be combined to an enveloping fragility curve (pressure and temperature dependent) for the whole containment.

i. In addition to the containment fragility for over-pressure conditions, the fragility for under-pressure conditions shall be estimated.

j. The containment fragility shall be compared to the available results in the literature for similar design.

5.3 Containment Loads

a. For the determination of the containment loads, the knowledge basis of the international nuclear safety community as related to the key severe accident phenomena shall be taken into account. The following severe accident phenomena shall be considered:

- In-vessel metal oxidation and hydrogen generation, and implications of any applicable modes of hydrogen combustion in the containment (including global deflagration, detonation, deflagration-to-detonation transition, and diffusion flames)

- In-vessel melt-coolant interactions (including energetic steam explosions)
- Interaction of core debris with the RPV lower head and lower head failure modes (including the impact of external lower head cooling, if applicable)
- Loss of primary coolant system integrity
- High pressure melt ejection
- Vessel failure
- Containment pressurization due to steam and non-condensable gas blowdown from the primary coolant system
- Vessel thrust forces (in case of failure at high pressure)
- Direct Containment Heating (DCH)
- Melt-dispersal and spreading
- Ex-vessel melt-coolant interactions (including energetic steam explosions)
- Molten Core Concrete Interactions (MCCI), considering
  - ▪ Debris coolability
  - ▪ Basemat and side wall attack by core debris
  - ▪ Hydrogen and carbon monoxide generation
  - ▪ Generation of other non-condensable gases (e.g., carbon dioxid)
- Quasistatic pressurization as the result of long-term addition of heat, steam, and non-condensable gases to the containment atmosphere

b. Specific severe accident phenomena relevant for low-power and shutdown accident scenarios shall be considered (e.g., air ingression to the fuel assembly or potential for increased oxidation and zirconium fire).

c. For various dominant severe accident scenarios, analyses shall be performed to establish the technical basis for assessment of severe accident loads on the containment. Uncertainties in the containment loads that arise due to the incomplete knowledge in the phenomena shall be estimated.

5.4 Severe Accident Progression

a. For each PDS or accident sequence, the severe accident progression from core or fuel damage to the release of radioactive material shall be modelled using an Accident Progression Event Tree (APET).

b. The nodal questions in the APET shall, if possible, follow the chronology of the accident progression. In the case that the fuel is in the RPV, at least the following time frames shall be taken into account:

- From core or fuel damage to vessel breach
- Immediately after vessel breach

- Longer term following vessel breach

c. For each time frame, the nodal questions in the APET should address:

    - Severe accident phenomena
    - The availability of systems required for severe accident management (e.g., containment venting system, circulating air cooler, hydrogen recombiners)
    - Actions related to severe accident management including recovery of power and/or system functions (e.g., actuation of containment heat removal)
    - Status of the containment

d. The quantification of the nodal probabilities shall be supported in general by state-of-the-art computer codes (e.g., MELCOR or MAAP) and engineering calculations. If it is not possible to use analytical methods, justified expert judgement can be applied. If the nodal probabilities are based on decomposition of the nodal branches (depending on accident boundary conditions)[8], the decomposition rationale shall be clearly developed and documented.

e. Uncertainties in the APET nodal probabilities shall be determined as follows:

    - The assessment of uncertainties in the APET nodal probabilities shall be supported by experimental evidence, documented analyses, expert judgement, or results of other studies that are publicly available and have been subjected to a peer review (e.g., NUREG-1150, NUREG/CR-6109.). Alternatively, the quantification of the APET nodal probabilities that potentially involve significant uncertainties should be supported by sensitivity cases that cover the expected range of uncertainties. If a computer code is used to support these sensitivity cases, the range of parameters should be clearly justified and documented.
    - The limitations of the computer code shall be taken into consideration when addressing the uncertainties in the phenomenological issues.

f. A minimum mission time of 48 hours after the start of core damage shall be assumed for the assessment of containment performance and radiological releases into the environment. In situations where containment failure (due to overpressure or basemat penetration) is considered imminent, this mission time shall be extended beyond 48 hours.

g. The end states of the APET shall be grouped into release categories, which are characterized by similarities in accident progression and source term, considering at least the following attributes:

[8] Example: a branch in the APET may deal with probability of combustion-induced containment failure. This could be decomposed into several subissues (not necessarily within the tree) as likelihood of ignition source present, likelihood of DDT, etc.

- Containment status, for instance open due to shutdown activities, vented, isolated[9], non-isolated, bypassed, ruptured, basemat penetrated
- Time of release (e.g., early or late)
- Mode of ex-vessel releases (i.e., dry or submerged core concrete interaction)
- Containment fission product removal mechanisms (e.g., scrubbing by containment sprays or by an overlying water pool)

h. The APET shall be quantified to determine the distributions and mean values of the frequencies of the various release categories.

5.5 Source Term Analysis

a. For each release category, a source term shall be calculated including both the magnitude and the timing of radiological release.

b. The source terms shall be represented by radiological groups that characterize the core radiological inventory of the reactor. These groups shall be based on similarities in thermodynamic and chemical properties of the various radionuclides. As a minimum the following radiological groups shall be considered:

Table 11: Radiological groups for the source term analysis

No.	Acronym	Group Name	Elements
1	Xe	Noble Gases	Xe, Kr, Ne, Ar, Rn, H, N
2	I	Halogens[10]	I, Br, Cl, F, At
3	Cs	Alkali Metals[11]	Cs, Rb, Li, Na, K, Fr, Cu
4	Te	Chalkogens	Te, Se, S, O, Po
5	Ba	Alkaline Earth Metals	Ba, Sr, Be, Mg, Ca, Ra, Es, Fm, Ga, Ge, In, Sn, Ag, B, Si, P
6	Mo	Transition Metals	Mo, V, Cr, Fe, Co, Mn, Nb, Tc, Ta, W
7	Ru	Platinoids	Ru, Rh, Pd, Re, Os, Ir, Pt, Au, Ni
8	Ce	Tetravalents	Ce, Ti, Zr, Hf, Th, Pa, Np, Pu, C
9	La	Trivalents	La, Al, Sc, Y, Ac, Pr, Nd, Pm, Sm, Eu, Gd, Tb, Dy, Ho, Er, Tm, Yb, Lu, Am, Cm, Bk, Cf, U

c. The source term calculations shall be based on a plant-specific model taking into account the radiological inventory of the core, the RCS and secondary coolant system, the containment building and systems, etc. A state-of-the art, fully integrated computer code shall be used that couples the thermohydraulics with fission product release, transport and retention.

d. Implication of the calculated source term results in recognition of any modelling limitations shall be discussed.

[9] With respect to the expected leakage

[10] CsI shall be grouped to the halogenes.

[11] CsOH shall be grouped to the alkali metals.

5.6 Quantification and Presentation of Level 2 PSA Results

5.6.1 Quantification

a. For the quantification of the APET, a validated computer code shall be applied. Limitations of the code or of the quantification method shall be discussed.

b. Uncertainties in the PDS frequencies and in the APET nodal probabilities shall be propagated through the model.

c. A combined Level 1/Level 2 PSA model or separate Level 1 and Level 2 PSA models can be used for the quantification.

d. The results shall be checked for plausibility taking into account the plant characteristics (plant design and operational features).

5.6.2 Presentation of Level 2 PSA Results

5.6.2.1 Risk Profile

a. A PDS matrix shall be provided as part of the PSA both as hardcopy documentation and electronically.

Table 12: PDS matrix (simplified example)

Event Category	RPV Pressure	Safety Injection	Containment Isolated?	
			Yes	No
Transient	*High*	*Ok*	*PDS1 (Mean, Error Factor)*	--
		No	*PDS2 (Mean, Error Factor)*	*PDS3 (Mean, Error Factor)*
	Low	*Ok*	--	--
		No	*PDS4 (Mean, Error Factor)*	*PDS5 (Mean, Error Factor)*
Large LOCA	…..	…..	…..	…..
	…..	…..	…..	…..

b. The contribution of the PDS (or the initiating events) to each release category shall be provided as part of the PSA hardcopy documentation.

Table 13: Contribution of PDS (IEs) to the release categories

Release Category	Mean Frequency [yr^{-1}]	Description	Plant Damage States	Relative Contribution to Release Category
RC-1	*6.2E-08*	*Early containment failure*	*PDS-3*	*50.1 %*
			PDS-6	*45.6 %*
			PDS-4	*4.3 %*
…				

c. The frequency of each release category and other release parameters according to Table 14 shall be provided as part of the PSA hardcopy documentation and in addition electronically.

Table 14: Release categories

Release Category		Frequency [yr^{-1}]	Time of Release[12] [h]	Release Duration [h]	Xe [Bq]	I [Bq]	Cs [Bq]	Te [Bq]	Ba [Bq]	Mo [Bq]	Ru [Bq]	Ce [Bq]	La [Bq]	Simulation
RC-1	*Mean*													*Run7, early venting*
	5 %													
	50 %													
	95 %													
RC-2	*Mean*													*Run2, bypass*
	5 %													
	50 %													
	95 %													

d. The contribution of the release categories to the *LERF* and *LRF* shall be provided as part of the PSA hardcopy documentation and in addition electronically.

Table 15: Contribution of release categories to the LERF and LRF

	Frequency [yr^{-1}]					
Risk Measure	**Mean**	**5 %**	**50 %**	**95 %**	**Release Category**	**Contribution**
LERF					*RC-3*	*47.1 %*
					RC-6	*43.6 %*
					RC-4	*7.2 %*
					RC-1	*2.1 %*
LRF					*RC-6*	*85.1 %*
					RC-1	*10.6 %*
					RC-2	*4.3 %*

e. The contribution of the initiating events to the *LERF* shall be provided as part of the PSA hardcopy documentation and in addition electronically.

Table 16: Contribution of initiating events to the LERF

Groups	**Initiating Event Category**	***LERF* [yr^{-1}]**				**% of Grand Total (Mean)**
		Mean	**5 %**	**50 %**	**95 %**	
	Transient					
	LOCA					
Internal Events (Total)						
	Fire					
	Internal floods					
	Other internal hazards					
Internal Plant Hazards (Total)						
	Earthquakes					
	Extreme winds and tornadoes					
	External floods					
	Aircraft crash					
	Other external hazards					
External Plant Hazards (Total)						
Important Events						
	ATWS					
	ISLOCA					
	SGTR (PWR only)					
***LERF* (Grand Total)**						

f. For each release category, the parameters according to Table 17 shall be provided as part of the PSA hardcopy documentation and in addition electronically.

[12] Time of the (first) release of noble gases

Table 17: Main parameters for each release category

Release Category	Frequency of Release [yr^{-1}]	Activity of Aerosol Release [Bq]	Risk of Aerosol Release [Bq/yr]	Contri-bution to Aerosol Risk [%]	Total Release (incl. Noble Gases) [Bq]	*TRAR* [Bq/yr]	Contri-bution to the *TRAR* (%)
RC-1	*1.07E-08*	*6.32E+16*	*6.76E+08*	*25.4*	*5.3E+18*	*5.67E+10*	*12.2*
…							
Total	***5.11E-06***		***2.81E+11***	**100**		***6.22E+12***	**100**

5.6.2.2 Importance Analysis

a. The basic event Fussell-Vesely (*FV*) and Risk Achievement Worth (*RAW*) importance values with regard to the *LERF* shall be provided electronically. If an integrated Level 1/Level 2 model is used, the importance values shall be calculated directly from the model. Otherwise, an approximation is acceptable.

Table 18: Importance values of basic events with regard to the LERF

	Basic Event ID	Description	Mean	*FV (RAW)*
1				
2				

b. The component *FV* and *RAW* importance values with regard to the *LERF* shall be provided electronically. If an integrated Level 1/Level 2 model is used, the importance values shall be calculated directly from the model. Otherwise, an approximation is acceptable.

Table 19: Importance values of components with regard to the LERF

	Component ID	Description	Mean	*FV (RAW)*
1				
2				

5.6.2.3 Sensitivity Analysis

a. Sensitivity analyses shall address three sets of issues related to the total risk of activity release *TRAR*, and to the *LERF*:

- Determination of the impact of various potential plant hardware and procedural modifications
- Determination of the impact of assumptions related to severe accident phenomenological issues
- Other significant modelling assumptions that were employed in the Level 2 analysis

5.6.2.4 Assessment of Plant Modifications

a. The influence of significant PSA-relevant hardware changes performed in the past on the *LERF* and *LRF* (e.g., drywell spray and flooding system or H_2 recombiners) shall be determined.

Table 20: Risk impact of plant modifications

Date	Description of Plant Modification	*LERF*

5.6.2.5 Insights

a. Any potential plant improvements (backfits) identified during the development of the Level 2 PSA shall be documented and discussed.

b. Based on the insights gained from the Level 2 PSA, it shall be discussed whether

- any modifications are required for the plant-specific SAMG (Severe Accident Management Guidance),
- there are any issues to be investigated in future severe accident research programs.

c. The plant's safety level in terms of the *TRAR/LERF* and the balance of the risk profile shall be discussed. A criterion in terms of the *LERF* is given in the guideline ENSI-A06.

d. The risk insights shall be compared with the insights from the previous PSA performed for the same plant. Differences in the PSA results shall be discussed.

6 Quality Assurance

6.1 QA Process and Peer Review

a. The development, update and application of the PSA shall be performed within the overall QA program of the licensee (respectively of the applicant for a licence), which shall define specific QA requirements for PSA issues.

b. The team conducting a new PSA or an update of a PSA shall consist of members having a profound knowledge of PSA techniques and of the characteristics of the installation.

c. The licensee (respectively the applicant for a licence) shall be strongly involved in the development, update and application of the PSA and shall review and approve (sign-off) the PSA documents.

d. The PSA shall be continuously improved.

e. A newly developed PSA or a comprehensive update of the PSA should be subjected to a peer review by a team of PSA practitioners who are independent of the PSA team. The peer reviewer's comments shall be made an integral part of the PSA documentation.

6.2 Documentation

a. The PSA documentation shall be complete and traceable. The PSA methods, models, data and analyses used as well as the results obtained shall be documented.

b. The PSA documentation shall be a stand-alone documentation system with the same high-level table of contents in each volume.

c. The PSA documentation system shall by structured such that updates to the PSA can be performed by replacing pages or chapters (to the extent possible). Changes in the documentation shall be marked and the change history of the updates shall be listed.

d. The PSA documentation including the PSA model (i.e., fault trees and event trees) shall be provided electronically (except for the Level 2 PSA model) and as a hardcopy (2 copies).

e. All important details of the methods and data used in the PSA performance shall be clearly described. The level of detail shall be sufficient to enable the reader to independently reproduce and scrutinize all aspects of the analyses and the results with a reasonable effort.

f. The assumptions used in the PSA models and analyses shall be identified and substantiated.

g. All PSA information and data sources shall be cited. The referenced documents should be freely available.

h. The results of the analyses performed in the context of the PSA shall be provided in SI units.

7 PSA for Other Nuclear Installations

The PSA requirements for other nuclear installations such as research reactors and intermediate storage facilities are dependent on the classification of the installation according to Article 22 KEV.

a. For all accidents referred to in Article 8 KEV with a resulting dose larger than 1 mSv for persons not exposed to radiation in the context of their profession, the initiating event frequencies and the probabilities of single failures shall be determined according to the requirements given in Chapter 4 (as far as applicable).

b. If the sum of all accident frequencies with a dose rate larger than 1 mSv is less than $1 \cdot 10^{-6}$ per year (installation with a low risk potential), no further probabilistic analysis is required.

c. If the sum of all accident frequencies with a dose rate larger than 1 mSv is larger than $1 \cdot 10^{-6}$ per year, the PSA requirements are defined on a case-by-case basis by the regulatory authority.

This guideline was approved by ENSI on 14 January 2009.

Director of ENSI: signed U. Schmocker

Appendix 1 Definition of Terms

Terms used in this guideline are defined below:

Category A actions

Actions in routine testing and in maintenance and repair of systems that are performed prior to the initiating event. In the PSA, the errors associated with these actions are modelled as contributors to system unavailability.

Category B actions

Actions or errors that cause (or contribute) to an initiating event, i.e., initiate an accident sequence.

Category C actions

Actions taken to prevent or mitigate accidents according to the instructions in operating and emergency operating procedures, and accident management measures. In the PSA, these actions are modelled in the response to initiating events.

CCF – Common Cause Failure

A failure of two or more components within a defined time window (usually two test intervals) as a result of a single shared cause.

***CDF* – Core Damage Frequency (Full-power operation)**

The Core Damage Frequency (*CDF*) is the expected number of events per calendar year that occur during power operation resulting in uncovery and heatup of the reactor core and leading to a significant release of radioactive material from the core.

***FDF* – Fuel Damage Frequency (Non-full-power operation)**

The Fuel Damage Frequency (*FDF*) is the expected number of events per calendar year that occur during non-full-power operation resulting in heatup of the fuel or in severe physical impact on the fuel so that a significant release of radioactive material from the core fuel is anticipated, regardless of whether the fuel is in the reactor vessel or in the spent fuel pool.

Fire compartment

Plant area completely surrounded by fire barriers.

Flood area

Area that can be affected by flooding or flooding effects.

Fragility

Conditional probability of failure of a component or structure as the result of an initiating event. The earthquake fragility is defined through a double logarithmic model with three parameters, A_m, β_R, and β_U.

Full-power operation

Comprises the operating states during the commercial plant operation at power and comparable low-power states.

Full-power PSA

A PSA that assesses the risk caused during full-power operation by initiating events.

FV of a basic event

Fussell-Vesely importance measure. FV_i = (CDF – CDF_S) / CDF, CDF_S : CDF with guaranteed success of basic event *i*, *CDF* : mean *CDF*.

HCLPF – High Confidence, Low Probability of Failure

Earthquake motion level at which there is a high (95 percent) confidence of a low (at most 5 percent) probability of failure (of a component or structure).

Initiating events

In full-power operation, disturbances and damage to plant components and parts that cause a reactor trip are called “initiating events”. Manual reactor trips (e.g., due to an earthquake or a fire) are also counted among the initiating events.

In non-full-power operation, “initiating events” are defined as events in which the system functions for fuel cooling are not available to the extent necessary, or where the system functions for reactivity control are not sufficiently effective.

Integrated PSA model

A PSA model that is capable of calculating an accident scenario from the initiating event to the release category without the need for grouping core damage states in the transition from Level 1 to Level 2 PSA.

Level 1 PSA

Probabilistic analysis to identify and quantify the accident sequences leading to the onset of core damage.

Level 2 PSA

Probabilistic analysis of the processes taking place after core damage and quantification of the frequency and quantity of radioactive releases.

LERF – Large Early Release Frequency

The Large Early Release Frequency is the expected number of events per calendar year with a release of more than $2 \cdot 10^{15}$ Bq of Iodine-131 per calendar year within the first 10 hours after core damage.

LRF – Large Release Frequency

The Large Release Frequency is the expected number of events per calendar year with a release of more than $2 \cdot 10^{14}$ Bq of Caesium-137 per calendar year.

Non-full-power operation

All operating modes other than full-power operation (i.e., low power and shutdown).

Non-full-power PSA

A PSA that assesses the risk caused during non-full-power operation by initiating events.

Permanent combustibles

Permanently installed or stored combustibles.

Plant-specific raw data (for the determination of the components reliability data)

The raw data to be analyzed based on the plant-specific operating experience include independent single failures and multiple failures of components with a common cause (CCF), the frequency and duration of component tests, and of repairs and maintenance activities as well as the number of demands and operating hours.

PSA equipment/components

All equipment that is modelled in the PSA.

PSA-relevant components

Components whose failure has an influence on the plant risk.

RAW of a basic event

Risk Achievement Worth – importance measure. $RAW_i = CDF_F / CDF$, CDF_F : *CDF* with guaranteed failure of basic event *i*, *CDF* : mean *CDF*.

Temporary combustibles

Combustibles that are temporarily stored in dedicated areas (in particular during outages).

Transient combustibles

Combustibles that can appear at different locations.

TRAR – Total Risk of Activity Release

The Total Risk of Activity Release is defined as the total radioactive release [Bq] per year.

Appendix 2 Abbreviations

APET	Accident Progression Event Tree
ASEP	Accident Sequence Evaluation Procedure
ATWS	Anticipated Transient Without Scram
CCF	Common Cause Failure
CDF	Core Damage Frequency
DCH	Direct Containment Heating
DDT	Deflagration-to-Detonation Transition
ECCS	Emergency Core Cooling System
EOC	Error of Commission
EPRI	Electric Power Research Institute
FDF	Fuel Damage Frequency
FMEA	Failure Mode and Effect Analysis
FV	Fussell-Vesely (Importance)
HCLPF	High Confidence, Low Probability of Failure
HE	Human Error
HEP	Human Error Probability
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
KEG	Kernenergiegesetz
KEV	Kernenergieverordnung
LBB	Leak Before Break
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LRF	Large Release Frequency
MCCI	Molten Core Concrete Interaction
MCR	Main Control Room
MOV	Motor-operated valve
NPP	Nuclear Power Plant
OECD	Organisation for Economic Cooperation and Development)
OPDE	OECD Piping failure data exchange project

PDS	Plant Damage State
PGA	Peak Ground Acceleration
POS	Plant Operating State
PSA	Probabilistic Safety Analysis
PSHA	Probabilistic Seismic Hazard Analysis
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
QA	Quality Assurance
RAW	Risk Achievement Worth
RC	Release Category
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RPV	Reactor Pressure Vessel
SAMG	Severe Accident Management Guidance
SGTR	Steam Generator Tube Rupture
SI	Système international d’unités
SLIM	Success Likelihood Index Methodology
SSHAC	Senior Seismic Hazard Analysis Committee
SSC	Structures, Systems, and Components
THERP	Technique for Human Error Rate Prediction
TRAR	Total Risk of Activity Release
US NRC	US Nuclear Regulatory Commission

Appendix 3 Description Sheet for Category C Personnel Actions

Basic Event Designator	*Designator of the PSA model event (e.g., basic event) that represents the failure of a Category C personnel action*
Initiating Event	*Designator and description of the initiating event(s) of the scenario(s) in which the Category C action is modelled*
Indications	*List of plant parameters, based on which the action is initiated*
Description of Action	
Diagnosis/Decision Part	*Short description of the diagnosis/decision (cognitive) part of the action including the relevant PSFs*
Execution Part	*Short description of the execution part of the action including the relevant PSFs*
Written Procedures	*Designator of the written procedure and of the corresponding steps in the procedure*
Preceding Events	*List or short description of failed top events as used in the PSA model*
Time Constraints	*Short description with specification of the required time and the time available*
Human Error Probability	*Mean value and error factor as used in the PSA model (split up into diagnosis part and execution part if available)*
Remarks/Special Notes	

Appendix 4 Description Sheet for Category A Personnel Actions

Basic Event Designator	*Designator of the PSA model event (basic event) that represents the failure of a Category A personnel action*
Brief Description of the Action	*Brief description of the required operation (e.g., close back valve or adjust limit switches), for which the potential error was identified*
Written Procedure	*Designator of the procedure describing and guiding the required task*
Affected Component and System or Function	*Identification of the component affected by the human error and of the affected system or function*
Failure Mode/Component Status	*Status of the component following the human error (e.g., misalignment in position XY, false calibration, false set point, initiation signal blocked)*
Opportunities for Error and Frequency	*Identification of routine activities or other activities during which the human error may occur, and determination of the frequencies of these opportunities. Examples: Functional testing, maintenance work in power operation or during shutdown*
Possibilities of Failure Detection and Correction and their Frequency	*Identification of the possibilities (and their frequency) for detecting and resolving the error. Examples: Periodic inspections (checklists and frequency shall be indicated), tests (test procedures shall be listed). Note: These tests are not identical with those by which the error can be caused.*
Human Error Probability	*Failure probability of the action, including uncertainty distribution*
Remarks/Special Notes	*Characteristics of the quantification, for example, dependence on previous errors*

Appendix 5 Model for the Adjustment of Human Error Probabilities in Case of Earthquake

As an acceptable option and in the interest of harmonization, ENSI presents below a model for the adjustment of the HEPs.

In case of earthquake, the HEPs can be adjusted as follows:

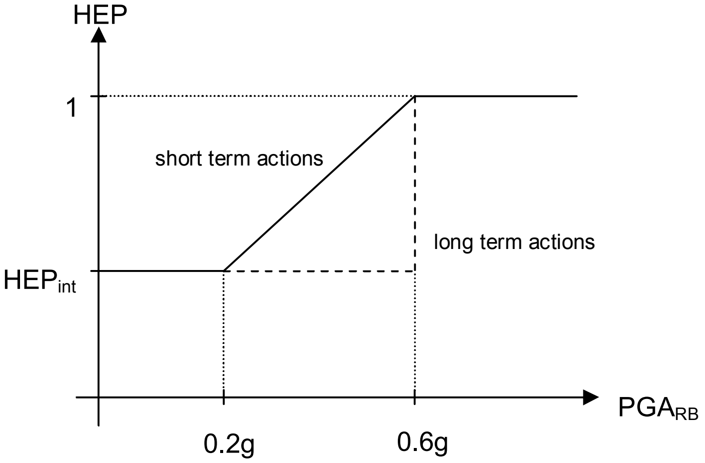
a. Up to an earthquake intensity of 0.2 g (maximum horizontal ground acceleration at the foundation level of the reactor building), the failure probabilities for personnel actions can be taken over without modification from the model for internal events (transients and LOCAs).

b. In the case of an earthquake with intensity from 0.2 g to 0.6 g, a linear interpolation between the values for 0.2 g and 0.6 g (guaranteed failure) shall be performed. Special case: for actions that must not be carried out within an hour after the earthquake, the failure probabilities up to an earthquake of magnitude 0.6 g can be taken over without modification from the model for internal events.

c. From 0.6 g, all personnel actions shall be considered as guaranteed failed.

The model is described graphically in Figure 1 below.

Figure 1: Dependence of HEPs on the earthquake intensity



Published by: Swiss Federal Nuclear Safety Inspectorate ENSI, CH-5232 Villigen-ENSI
Telephone +41(0)56 310 38 11, fax +41(0)56 310 39 95 and +41(0)56 310 39 07

Can be ordered from: Swiss Federal Nuclear Safety Inspectorate ENSI, Information Service, CH-5232 Villigen-ENSI
or by e-mail Info@ensi.ch
Electronic copies are available at ENSI's web page: www.ensi.ch