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 2019

Probabilistic Safety Analysis (PSA): Quality and Scope

Edition March 2019

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-A05/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 established by an ordinance. Guidelines are support documents that formalise the implementation of legal requirements and facilitate uniformity of implementation practices. Furthermore, they concretise the state of the art in science and technology. ENSI may allow deviations from the guidelines in individual cases, provided that the suggested solution ensures at least an equivalent level of nuclear safety or security.

2 Subject and scope

The guideline ENSI-A05 formalises the quality and scope requirements related to plant-specific Level 1 and Level 2 Probabilistic Safety Analysis (PSA) for both internal and external events and covering all operating modes of 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 plant-specific PSAs enable, at least the following PSA applications:

a. Probabilistic evaluation of the safety level

b. Evaluation of the balance of the risk contributions

c. Probabilistic evaluation of the technical specifications

d. Probabilistic evaluation of changes to structures and systems

e. Risk significance of components

f. Probabilistic evaluation of operational experience

In accordance with international PSA practices, this guideline does not include any requirements regarding consideration of risks due to war, terror and sabotage.

3 Legal basis

This guideline implements the legal requirements stated in:

a. Article 4, Paragraph 3 a of the Nuclear Energy Act (NEA; SR 732.1)

b. Article 22, Paragraphs 1 and 2 of the Nuclear Energy Ordinance (NEO; SR 732.11)

c. Article 28, Paragraph 1 of the Nuclear Energy Ordinance

d. Article 34, Paragraph 2 of the Nuclear Energy Ordinance

e. Article 41, Paragraph 1 of the Nuclear Energy Ordinance

f. Annex 3 of the Nuclear Energy Ordinance for the definition of the scope of a PSA

g. Articles 1, 5 and 12 of the DETEC Ordinance on the Hazard Assumptions and the Assessment of the Protection against Accidents in Nuclear Installations of 17 June 2009 (SR 732.112.2)

4 Technical requirements for the Level 1 PSA of a nuclear power plant

4.1 Scope of the Level 1 PSA

a. All 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 specific exclusions shall be justified.

b. A PSA shall be performed for the spent fuel pool for full-power operation of the nuclear power plant. This requirement can be waived if the expected total annual release of radioactive substances in case of fuel damage in the spent fuel pool is less than 1% of the risk parameter *TRAR*.

c. The risk shall be analysed for all operating modes of the plant. For 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 comprehensive PSA model. The PSA model can be subdivided into models for full-power and non-full-power 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

4.2.1 Collection of plant-specific reliability 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 of 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, it shall be considered that the respective components have similar failure behaviour.

c. The evaluation of the plant documentation for the determination of the plant-specific raw data shall be supported by the personnel in charge of the corresponding system at the plant or by other experts with the necessary knowledge of the system.

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

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

f. If a component or several components have been replaced or significantly modified, it shall be discussed whether the operational data of the component group collected since the date of replacement/modification is appropriate for the subject components.

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

    1. Component ID
    2. Component group
    3. Failure mode
    4. Root cause of the failure
    5. Date of failure
    6. Plant operating mode
    7. Reference to the plant documentation

h. The documentation of component unavailabilities due to repair or maintenance shall comprise:

    1. Component ID

2. Component group
3. Date of begin of the unavailability
4. Duration of the unavailability
5. Plant operating mode
6. Reference to the plant documentation

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

j. The collected component reliability data shall be maintained 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 considering the design, operational characteristics, grouping, boundaries, and failure modes of the specific 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 plant-specific raw data and the generic reliability data through a Bayesian updating process.

b. For commercial (non-nuclear grade) components (e.g. electronic circuits), for which typically plant-specific failure statistics are not collected, generic data can be used directly.

c. Component data used in 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 reliability data shall be utilized.

d. The mean failure probability and a statistical representation of the associated uncertainty (i.e. 5%, 50% and 95% fractiles) 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. Beta distribution or Gamma 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 regarding CCFs (i.e. design, operational and maintenance conditions, etc.) shall be grouped in the CCF groups.

c. The accepted CCF parameter models are the Alpha Factor and the Multiple Greek Letter schemes. 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 affecting potential degradations of the availability of the systems modelled in the PSA 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 process.

b. If a fault tree analysis is performed in order to quantify the frequency of an initiating event, potential human errors associated to Category B actions (actions during tests, maintenance, repair, and in the management of operational disturbances that may lead to the initiating event) 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. In the full power PSA a search for potential Errors of Commission (EOCs) shall be conducted. For the identified EOCs, their consequences and possible countermeasures shall be discussed qualitatively.

e. Recovery actions can be considered in the case of independent component failures if they are plausible and realisable in the considered accident scenario, and if they are not repairs (e.g. reassembly of disassembled components). The analysis of recovery actions shall in particular consider the identification and accessibility of the affected components, the availability of resources (e.g. qualified personnel), and the procedural support. These measures shall be analysed as Category C actions.

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

    1. that are actuated automatically on demand,

2. in systems subject to a function test after a maintenance or repair, through which the error is discovered,

3. whose status is displayed in the control room, periodically controlled and modifiable from the control room, or

4. for which there is a requirement to check their status at least once per shift.

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

g. A failure in Category A or Category B actions shall not be screened out, if

1. failure leads simultaneously to the unavailability of multiple trains of a redundant system, or

2. failure has been observed in the plant-specific or applicable generic operating experience.

4.3.2 Assessment of human error probabilities

4.3.2.1 Category A actions

a. Human Error Probabilities (HEPs) of Category A actions, shall be estimated in a systematic quantification process. Methods considered acceptable are the statistical method (i.e. quantification of the errors solely based on a statistics using generic and plant-specific experience), THERP, and ASEP.

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

1. Quality of written procedures relating to the task execution and verification,

2. Availability of instrumentation and indications for error detection, and

3. Other factors that impact human performance (e.g. noise or time restrictions).

c. Each Category A action modelled in the PSA shall be documented in accordance with Appendix 3.

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 be credited if relevant procedural guidance is available and 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 methods are THERP, ASEP, and SLIM variants as well as the statistical method described in Chapter 4.3.2.1 a.

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

d. The following Performance Shaping Factors (PSFs) shall be accounted for in the quantification of HEPs:

   1. Characteristics and frequency of the operator training and experience,
   2. Quality of the written procedures,
   3. Availability of instrumentation and ergonomic quality of the human-machine interface,
   4. Clarity and unambiguousness of the cues and indications,
   5. Time available and time required to complete the task,
   6. Complexity of the response (e.g. coordination and communication requirements),
   7. Environment in which the operators are working, and
   8. Accessibility, availability, and adequacy of required tools and equipment.

   The assessment of these PSFs shall be documented for each modelled personnel action. In addition, the documentation shall state which factors influence only the diagnosis and decision aspect or the execution aspect of the action, and which factors influence both aspects.

e. In particular, actions outside the control room shall be discussed with operators in order to identify possible problems with access or other factors limiting the feasibility of the considered action. Aggravating conditions during post-initiator phase shall be considered.

f. The quantification of Category C personnel actions shall be primarily scenario-specific. If an action is used in multiple scenarios, the quantification process shall consider 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 described in Chapter 4.3.2.1 a is used for the quantification of failure probabilities of Category C actions, the requirements of Paragraphs c, d, g and i as well as of Chapter 4.3.2.4 b do not apply.

i. For HEPs of actions of the shift personnel, a lower limit of 10^{-5} (mean) shall be used. For HEPs of actions requiring the involvement of the emergency response team, a lower limit of $5 \cdot 10^{-3}$ (mean) shall be used.

j. Each Category C action modelled in the PSA shall be documented in accordance with Appendix 4.

4.3.2.4 Dependencies

a. The following types of dependencies shall be systematically considered:

   1. Dependencies within a task, where a task is defined as a group of actions that relate to a specific goal or system function,

   2. Dependencies among Category A actions, and

   3. Dependencies among Category C actions, and among Category B and C actions within the same accident sequence.

   The available time, the existence of common factors (e.g. instrumentation, procedures or stress) and the availability of resources (e.g. personnel) shall be considered.

b. The minimum joint failure probability of 10^{-5} for an accident sequence shall be used. Given the availability of support personnel from the emergency response team, the applicable minimum joint failure probability may be reduced to 10^{-6}. A lower overall error probability may be used if it is statistically demonstrated.

4.3.2.5 Uncertainties

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:

   1. Increased stress and confusion,

2. Reduced availability of personnel,
3. Limited accessibility and habitability of relevant areas (e.g. rooms),
4. Failed or erroneous instrument indications,
5. Additional workload on personnel,
6. Additional difficulties in the detection/diagnosis of certain hazards, and
7. Limited accessibility to areas of the plant.

b. The impact of fires on the human error probabilities shall be evaluated, considering 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, considering 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 analysed using the following procedure:

1. The choice of parameters (e.g. earthquake ground acceleration, earthquake duration) that characterize an earthquake and their assumed effect on the error probabilities shall be defined and justified.
2. The approach applied and the numerical values (such as factors used to increase the failure probabilities determined for internal events) used to determine the failure probabilities for earthquakes shall be justified.
3. The psychological and possibly physical effects of the earthquake on the personnel shall be considered in representing the failure probabilities. In particular, the uncertainty about the state of the installation associated with severe earthquakes shall be taken into account in determining the failure probabilities.

Models to adjust the failure probabilities of personnel actions and their dependence on the earthquake severity/intensity considered acceptable are listed 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 developed with the involvement of plant personnel. To ensure that it is as complete as possible, the following methods shall be applied:

   1. System analysis (see Chapter 4.4.3) for the systematic review of the systems and components, and of the test and maintenance practice

   2. Master Logic Diagrams (MLDs), Failure Modes and Effects Analysis (FMEA), or other pertinent analytical methods

   3. Evaluation of the operational experience including initiating events as well as precursor events which did not lead to a reactor trip, either due to the intervention of operators or plant mitigating systems

      For each event, at least the date, a brief description, and the event group (see Chapter 4.4.1.2) shall be provided.

   4. Evaluation of generic operational experience

      Internationally accepted and available lists of initiating events for plants of similar types and vintages shall be evaluated.

b. The initiating event category “transient” includes:

   1. Total or partial failures of front-line systems or support systems

   2. Inadvertent actuation of safety systems

   3. Manual reactor trips

c. The “Loss of Coolant Accident” (LOCA) event category covers breaks in water or steam carrying pipes and faulty states or operation of valves in these pipes resulting in the failure of the integrity of the reactor coolant system. The subdivision according to leakage sizes and locations is based upon the success criteria for the prevention of core or fuel damage.

d. Regardless of the subdivision according to Paragraph c above, the following LOCAs shall be explicitly considered:

   1. Interfacing Systems LOCA, i.e., LOCA caused by failure of a boundary between high- and low-pressure systems

   2. Excessive LOCA (i.e. catastrophic rupture of the reactor pressure vessel that exceeds the capacity of the ECCS)

3. Steam Generator Tube Rupture (SGTR – for PWR only)

4. Non-isolable LOCA outside the containment

e. In a PSA for non-full-power operation, specific types of LOCA events shall be also considered (e.g. omission of securing the system while removing components, loss of coolant from shutdown cooling systems, leakages on the gate between pools).

f. Fuel mishandling, heavy load drops and events affecting reactivity control (e.g. boron dilution, control rod ejection) shall be discussed and if necessary included as part of the PSA model for non-full-power operation.

4.4.1.2 Grouping and screening of initiating events

a. In the case where initiating events are grouped, it shall be ensured that

1. all initiating events belonging to the same group have similar consequences in terms of plant response and identical success criteria for prevention of core or fuel damage,

2. those initiating events having the potential for a large radionuclide release (e.g. steam generator tube rupture, catastrophic rupture of the reactor pressure vessel, interfacing systems LOCA, and non-isolable breaks outside containment, etc.) shall be modelled independently in separate groups, and

3. the success criteria for each individual event in the group are less restrictive than the requirements defined for the group.

b. Apart from LOCAs defined in Chapter 4.4.1.1 d, an event group with a frequency less than 10^{-8} per year can be screened out, provided 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 frequencies shall be based on plant-specific raw data.

b. In order to improve statistical confidence, generic frequencies of initiating events (including uncertainties) from internationally accepted sources shall be utilized. The generic data shall be evaluated for applicability.

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

d. Fault tree models shall be used to derive initiating event frequencies resulting from loss of support systems. This also applies to initiating events caused by operating systems, if this is necessary for PSA applications in accordance

with guideline ENSI-A06. Consistency of the frequencies calculated with plant-specific operating experience shall be demonstrated.

e. For LOCAs, the frequencies shall be estimated from generic data accounting for plant-specific features. In order to assess the applicability to the subject plant, plant-specific characteristics, insights from in-service inspection programs, Leak before Break (LBB) analyses or probabilistic fracture mechanics shall be considered. Fracture frequencies can be based on probabilistic fracture mechanics analysis using justifiable and documented assumptions and data.

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

g. Independently of a specific operating state, 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 represented by an appropriate distribution.

4.4.2 Accident sequence analysis

4.4.2.1 Identification of safety functions

Safety functions of the subject plant able 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.

4.4.2.2 Accident 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 relevant design and operational characteristics as well as the requirements in the regulations are addressed.

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

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

d. In general, the accident sequence shall be analysed for a mission time of at least 24 hours. For event sequences which do not reach a safe and stable 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 and stable 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 loss of coolant is terminated for instance by lowering temperature and pressure in the reactor permanently.

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

g. In developing event sequences, secondary effects caused by the initiating event or other subsequent events during accident progression shall be properly considered. In the case of a large LOCA, the phenomenological impacts of flooding (e.g. plugging of screens/filters due to debris) as well as the effects of the elevated temperature and humidity on the availability of systems and components shall be considered.

4.4.2.3 Success criteria analysis

a. Success criteria in terms of the required systems or components including the corresponding support systems shall be determined and documented for each safety function and as a function of the initiating event and the specific accident sequence.

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

c. Numerical analyses shall be performed using validated computer codes.

4.4.3 System 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 systems are shared by multiple units (e.g. diesel generators), the component dependencies across unit boundaries shall be considered.

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:

   1. Unavailabilities of active and passive components due to independent and dependent failures or maintenance activities
   2. Failure modes such as flow diversion or spurious actuation
   3. Operational restrictions imposed by the plant Technical Specifications
   4. Functional dependencies including electrical power, cooling, control and actuation
   5. Varying alignments of the system
   6. Impact of the initiating event on the system
   7. Human errors

e. The component models shall consider:

   1. Mission times
   2. Maintenance durations and frequencies
   3. Test intervals
   4. Number of demands and number of failures
   5. Failure modes (e.g. failure to start or failure during operation)

f. Maintenance unavailability and an active failure mode shall be modelled in distinct basic events.

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. because two or more manual valves in the diversion path would have to be in the wrong position).

h. In order to circumvent logic loops (caused by 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 the following components:

   1. Pumps
   2. Diesel generators
   3. Fans
   4. Control rods
   5. Motor-operated, pneumatic and check valves
   6. Heat exchangers
   7. Transmitters

8. Safety and pressure relief valves
9. Main steam isolation valves
10. Batteries, chargers, inverters, relays
11. Circuit breakers, switches
12. Strainers

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

j. The potential for inter-system CCFs shall be discussed taking into account coupling factors such as identical component type, manufacturer, common design characteristics or maintenance strategy. Inter-system CCFs shall be modelled.

k. A systematic format naming the system or component designator and the failure mode or human error shall be employed for coding basic events.

l. Combining several components into a common component (super-component) may take place in particular 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 traceable manner.

m. For each system modelled in the PSA, the total unavailability shall be presented together with a verification of the plausibility of the most important minimal cutsets contributing to this unavailability.

4.5 Internal plant hazards

4.5.1 Selection process and selection criteria

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

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

1. Explosion
2. Release of toxic gases
3. Turbine missile

c. The events explosion and release of toxic gases do not need to be included in the PSA model when one of the following conditions is satisfied:

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

d. The event turbine missile does not need to be included in the PSA model if a quantitative evaluation shows that the contribution to *CDF* is less than 10^{-9} per year (see Chapter 4.5.4).

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:
   1. Fire compartments (according to the fire protection concept, “Brandschutzkonzept”)
   2. Fire loads (i.e. permanent, temporary and transient combustibles)
   3. Potential ignition sources (e.g. transformers, electrical cabinets, or welding activities) and vulnerable PSA components
   4. Routing of cables
   5. 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:
   1. verify the information collected from the plant documentation,
   2. investigate the physical distribution and separation of the potential ignition sources and the fire loads,
   3. identify and document potential fire propagation paths and fire scenarios, and
   4. analyse vulnerability of PSA components to fire effects (heat and smoke) and to fire suppression actions.

c. For all the operating states modelled in the PSA for non-full-power operation, the differences with the PSA for full-power operation 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 database, the spatial interaction database.

e. A fire compartment can be screened out if it satisfies all the following criteria:

   1. It does not contain any PSA equipment.

   2. A fire occurring within the compartment neither leads to an initiating event nor requires a manual shutdown of the reactor.

   3. Neither neighbouring fire compartments nor fire compartments connected to the compartment considered by ventilation paths contain PSA equipment.

f. Fire compartments can also be screened out as far as the sum of all contributions by the fire scenarios to *CDF* and *FDF* respectively is less than 10^{-8} per year. The calculation of the respective *CDF* and *FDF* shall be based on the following conservative assumptions:

   1. A spreading of fire effects to other fire compartments shall be considered for all neighbouring compartments as well as all compartments connected to the compartment considered by ventilation paths. The probability of such a spreading shall be introduced in the calculation of the *CDF* and *FDF* respectively.

   2. All vulnerable equipment in the fire compartment considered as well as all fire compartments, to which a spreading of fire effects is to be assumed, shall be set as failed due to the fire.

   3. The failure of cables 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 Chapter 4.5.2.2.

g. The results of the screening procedure (relevant and screened out fire compartments) shall be documented in a traceable 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 numbers 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. At least, 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:

   1. Plant operating state
   2. Ignition source location
   3. Cause of the fire
   4. Actuation of fire detection and suppression systems
   5. 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. Fire scenarios in the fire compartments that are to be analysed according to the quantitative screening process shall preferably be analysed in detail by means of a fire propagation event tree. This event tree shall consider the fire event frequency and the availability of the fire detection systems, fire suppression systems and fire barriers in the fire compartment.

b. The failure probability of personnel actions of for manual detection and suppression of a fire shall be quantified based to the methods referred to in Chapter 4.3.2.

c. The failure probabilities of the devices for automatic fire detection and fire suppression as well as 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 the fire barriers (e.g. walls, doors, fire dampers and penetration seals).

e. The consequences of cable fires on their related components shall either be assessed in a detailed manner (circuit analysis) or the conservative boundary conditions described in Chapter 4.5.2.1 f shall be retained.

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 other recognized methods.

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

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

4.5.2.4 Estimation of the fire *CDF* and *FDF*

a. The fire *CDF* and *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 Chapter 4.3.3 shall be verified.

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

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

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:

1. Flood sources (water tanks and piping)
2. Flood areas
3. Potential flood causes (e.g. pipe breaks, spurious actuation of water bearing systems, or human-induced events such as overfilling tanks)
4. Characteristics of the flood sources (e.g. location, capacity, type of flow medium, flow rate)
5. PSA equipment that might be affected by the flood
6. 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

1. verify the information collected from the plant documentation,
2. investigate the spatial distribution of potential flood sources,

3. determine potential flood propagation paths and identify flood scenarios, and

4. analyse 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 PSA for non-full-power operation, the differences with the PSA for full-power operation regarding potential flood sources, propagation routes, 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. A flood area can be screened out if all of the following criteria are met:

1. It does not contain any PSA equipment.

2. A flood in that area does not cause an initiating event nor does it require a manual reactor shutdown.

3. Contiguous flood areas, where flood propagation due to the failure of watertight barriers is possible, do not contain any PSA equipment.

f. The considered flood area can also be screened out if it can be demonstrated under conservative assumptions that a flooding, neither in the considered area nor in the contiguous flood areas, in which a propagation of the flooding is possible due to the failure of watertight barriers, will not compromise any PSA equipment.

g. Flood areas can also be screened out as far as the sum of all contributions by the flood scenarios to *CDF* and *FDF* respectively is less than 10^{-8} per year. The calculation of the respective *CDF* and *FDF* shall be based on the following conservative assumptions:

1. A propagation of the flood to all contiguous flood areas, to which flood propagation due to the failure of watertight barriers is possible, shall be assumed. The probability of failure of barriers shall be considered in the calculation of the *CDF* and *FDF* respectively.

2. All equipment susceptible to effects of flooding in the considered flood area as well as in the contiguous flood areas, to which a propagation of the flood shall be assumed, shall be considered to be failed.

3. 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.

h. The results of the screening procedure (relevant and screened out flood areas) shall be documented in a traceable manner.

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 number 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.

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

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

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

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 devices 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 may be combined.

g. Flood scenarios can be screened out to the extent that the cumulative contribution to *CDF* and *FDF* respectively 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* and *FDF*

a. The flood *CDF* and *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 verified.

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

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

4.5.4 Turbine missiles

a. For the generic frequency distribution of a turbine missile, a lognormal distribution with mean $1.8 \cdot 10^{-4}$ per year and error factor 3 shall be used.

b. For the calculation of the frequency of a turbine missile (f_1), the generic frequency mentioned in Paragraph a above may be combined with manufacturer data using a Bayesian updating process.

c. Potential trajectories of the parts ejected from the turbine (turbine missiles) shall be determined. The following factors shall be considered:

   1. The speed of the projectiles, the variation of the flight angle (the range between -25° and +25° measured from the rotational plane shall be considered)

   2. Potential obstacles (e.g. building or room walls)

d. The speed of the projectiles shall be derived from the maximum rotation speed of the turbine shaft. Damages during normal operation or during the start of the turbine as well as damages due to overspeed shall be considered.

e. 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.

f. Given a turbine missile event, the conditional probability (given a turbine missile) of a missile strike (P_A) shall be determined for each of the identified targets assuming that four missiles with independent trajectories are generated simultaneously.

g. Given a missile strike on an identified target, the conditional failure probability (P_B) shall be evaluated for each of the affected PSA components. If a PSA component is hit directly, guaranteed failure shall be assumed ($P_B = 1$). The frequency of a component failure due to a turbine missile shall be calculated using the formula: $f = f_1 \cdot P_A \cdot P_B$

h. The consequences of the four most adverse independent turbine missiles shall be analysed and grouped in one initiating event:

   1. The frequency according to Paragraph g above shall be assigned to this initiating event.

   2. 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 through 4.6.6.

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

   1. Drought, which leads to low river level and low ground water level

   2. Forest fire

   3. High summer temperature

   4. Low winter temperature

   5. Icing phenomena (like icy rain, accumulation on structures, river freezing)

   6. Snow (drift)

   7. Hail

8. Lightning
9. Sun storm
10. Landslide
11. River diversion
12. Water-intake plugging due to river transported material (e.g. logs, leaves, mussels, algae). Water intake plugging by the effects of external flooding shall be considered in the external flooding analysis (see Chapter 4.6.5).
13. Soil shrink-swell consolidation
14. Industrial or military facility accident
15. Pipeline accident
16. On-site release of chemicals
17. Ground transportation accidents

The impact of these hazards on the plant shall be described. The appropriate physical quantities shall be presented for the relevant hazards.

c. The licensee shall verify if the list of hazards presented under Paragraph b above include all the relevant hazards for his plant, consistent with the state of art. The most important combinations of hazards listed under Paragraphs a and b above, which according to experience are possible, shall be identified and assessed with a matrix.

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

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

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

1. It can be shown based on qualitative arguments that the hazard has a negligible impact on the *CDF* and *FDF* respectively. This can be demonstrated by showing that the specific hazard does not result in actuation of a safety system or that the consequences of the specific hazard are already bounded by events having a significantly higher frequency of occurrence.
2. A bounding analysis of the *CDF* and *FDF* respectively due to the hazard yields a value that is less than 10^{-9} per year.

4.6.2 Earthquakes

4.6.2.1 Vibratory ground motion

4.6.2.1.1 Hazard analysis

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

b. When updating the PSHA, the following requirements shall be met:

1. A detailed project plan shall be submitted to ENSI.

2. The PSHA shall be designed such that the centre, body and range of the uncertainties reported in the results represent the state of the art already consolidated or recognized to be so soon.

3. A participatory and a late-stage review conducted by ENSI shall be included in the project plan.

4. The structure of the PSHA project shall consist of a technical project management, comprising a single expert or a small expert team, and of the four subprojects “seismic source characterisation” (SP 1), “ground motion characterisation” (SP 2), “site response characterisation” (SP 3) and “seismic hazard computation” (SP 4).

5. SP 1 shall comprise an evaluation team of at least 6 experts, SP 2 at least 5 and SP 3 at least 3. The evaluation team of SP 1 shall cover the fields of seismology, geophysics and geology.

6. The involvement of the experts in the PSHA shall at least meet the requirements set out in Appendix 6.

7. The responsibilities shall be clearly defined and in the course of the project, their acknowledgment and accomplishment shall be confirmed in writing.

8. A list of the names of the technical project managers and the evaluators shall be submitted to ENSI for comment.

9. An up-to-date and, relative to the project scope, comprehensive database of geological, seismological, geophysical and geotechnical data shall be created.

10. Project work relevant in terms of the project results or the traceability of the PSHA shall be developed or presented in clearly structured workshops.

11. Processes that have a significant impact on the project results or their reproducibility shall be monitored with project-specific quality assurance procedures. The computer program used for the hazard computation shall be verified and validated with representative test cases.

12. In the PSHA model, the uncertainty shall be captured consistently and systematically and be split into aleatory and epistemic contributions.

13. The hazard shall be quantified for earthquakes having moment magnitudes $M \geq 4.5$.

14. The PSHA documentation shall be comprehensive and traceable. The level of detail of the documentation shall enable the review, application and update of the PSHA.

15. After completion of the PSHA project, the PSHA databases and computer programs shall continue to be kept available and the capability to provide presentations of PSHA data and results shall be maintained.

c. The PSHA shall produce the following results:

1. Ground motion results in the form of acceleration responses of single-degree-of-freedom oscillators for a reference subsurface rock outcrop condition, for the reactor building foundation level, and for the local ground surface, all for free-field conditions

2. Calculated geometric mean of the two horizontal components and, separately, the vertical component of the ground acceleration

3. Hazard curves for spectral frequencies from 0.5 Hz to 50 Hz, with adequate mapping of the resonant frequencies of the soil, and for the Peak Ground Acceleration (PGA) which can be approximately chosen as acceleration at 100 Hz

4. Hazard results for ground motion levels from 0.01 g to at least the ground motion level corresponding to an annual exceedance frequency of 10^{-7} per year

5. Epistemic uncertainty (of the hazard) represented by at least 25 curves which are aggregated and weighted based on similar characteristics (e.g. slope and level)

   Alternatively, at least 25 equally weighted curves may be reported which have been developed on statistical grounds, provided that the 5%, 16%, 50%, 84% and 95% fractile curves and the mean value curve are shown.

6. Uniform Hazard Spectra at 5% damping for each order-of-magnitude change in annual exceedance frequencies from 10^{-2} per year to 10^{-7} per year inclusive

7. Direct results, guidance, or a combination thereof, to facilitate the estimation of Peak Ground Velocity (PGV), average spectral acceleration, and spectra at any damping value, as well as the selection of time histories

8. Horizontal components of the hazard results deaggregated in terms of magnitude, distance, and epsilon (number of standard deviations)

9. Documentation and explanation of the hazard contributions by seismic source, of principal contributors to uncertainty, of the upper limit ground motion estimate (depending on depth) and of the comparison with previous hazard studies for Swiss nuclear power plants

4.6.2.1.2 Fragility analysis

a. For the calculation of the floor response spectra the following requirements apply:

   1. To the extent possible, the consistency of the soil properties and of the foundation and free-field movements with the models and results of the hazard analysis shall be ensured.

   2. Three components of ground motion (two horizontal and one vertical) with correlation between the components corresponding to the hazard results shall be used.

   3. A set of input time histories shall be used that is consistent with the hazard results, the response spectra and realistic power spectra, and sufficiently large in number and characteristics to map the variability.

   4. The analysis of the soil-structure interaction shall consider (i) strain-compatible soil properties (e.g. shear modulus and damping), (ii) relevant dynamic properties and applicable phenomenological models for the behaviour of structural elements, and (iii) fully three-dimensional responses which represent the translational and the rotational vibrations of the soil-structure system.

   5. The scope of the parameters for which uncertainties are not considered shall be justified.

   6. Each scaling of the floor response spectra shall be identified and the adequacy of the scaling factors shall also be justified.

b. For the fragility analysis, information related to the seismic capacity of structures and components shall be collected, in particular:

1. List of PSA equipment including their location
2. Layout drawings of piping
3. Preliminary list of the structures and components potentially compromising PSA equipment or piping in case of earthquake
4. Seismic design documents of the components and structures (providing information related to layout, dimension, material properties, anchorage, failure modes, design methods, and qualification tests and results)
5. Generic information about the seismic design and fragilities

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

d. 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:
   1. 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* and *FDF* respectively.

2. For structures or components no seismic failure needs to be considered in the PSA model if the structure or component is shown to have a seismic *HCLPF* capacity higher than the screening level and failure of the structure or component will not directly lead to a containment bypass. In this case, the *HCLPF* capacity can be demonstrated by conservative expert judgment.

3. For the other structures or components realistic fragility parameters shall be assessed if (i) the structure or component has a high importance value to *CDF* and *FDF* respectively, or (ii) the seismic failure of the structure or component leads directly to a containment bypass.

4. For the remaining structures and components, conservative fragility parameters can be assessed by means of expert judgement.

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

   1. 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.

   2. The conditional failure probability of structures or components affected by seismically induced fires, explosions and floods shall be estimated as a function of ground motion or a guaranteed failure shall be assumed.

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

   1. Component identification number

   2. Location

   3. Failure modes

   4. Fragility parameters

   5. *HCLPF*

   6. Equipment affected by the failure and their failure modes and conditional failure probabilities

   7. Applied screening procedure

   8. Reference to the underlying fragility analysis

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

h. A very small LOCA caused by leakage due to seismic failure of measuring lines on the reactor cooling system shall be assumed. The equivalent size of the leak shall be determined based primarily on the insights gained from the plant walkdown.

i. 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 analysing outage schedules and activities, and conducting interviews with outage management personnel.

4.6.2.1.3 Analysis of earthquake accident sequences

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

b. Initiating events shall be defined as follows:

   1. The ground motion range between the lowest *HCLPF* value and the screening value shall be covered by at least 7 initiating events.

   2. For ground motions exceeding the screening value, an initiating event shall be defined.

c. 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:

   1. For ground motions exceeding the screening level, guaranteed core/fuel damage shall be assumed.

   2. The HEPs used in the internal events PSA shall be reviewed and adjusted according to the requirements given in Chapter 4.3.3.

   3. The PSA model shall explicitly reflect all seismically induced failures identified that were not screened out in the fragility analysis.

   4. Direct and indirect failures of a component shall be modelled separately.

d. For the quantification of the seismic *CDF* and *FDF*, the uncertainties of the initiating event frequencies, of the failure probabilities of components and structures and of the HEPs shall be considered. Correlations among the seismic failures shall be identified and considered in the uncertainty analysis.

4.6.2.2 Further seismic hazards

In addition to the failures caused by the direct effects of the earthquake vibratory ground motions (see Chapter 4.6.2.1), further 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. A comprehensive and up-to-date database on wind occurrences and wind gust velocities in the region of the installation shall be developed consisting in particular of the following data:

   1. For several quality-assured, certified weather stations in the region of the installation: measured wind gust velocities (short-term measurement data)
   2. Long-term measurement data from at least another weather station
   3. Data on historical windstorm events outside the measurement period of short-term and long-term data
   4. Data on wind fields (maps of windstorm hazard) in Switzerland

b. The wind speeds to be considered for the site shall be derived in particular from the short-term measurements in the region of the installation and from the long-term measurements of another weather station.

c. When mapping the measured wind speeds to specific heights of interest, the Thom equation 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 that depends on the surface roughness

d. A site-specific wind hazard curve (annual exceedance frequency of maximum wind gust velocity) shall be developed by means of an extreme value statistical evaluation of the available measurement data. The mean value of the hazard shall be determined. For the quantification of the uncertainties, recognized methods such as bootstrapping shall be applied.

e. The plausibility of the obtained wind hazard shall be checked. At least on a qualitative basis, the plausibility of the results shall be validated on the basis of historical windstorm events and windstorm hazard maps in Switzerland.

f. A plant walkdown shall be conducted. The walkdown shall include identification of vulnerable components and structures (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 components and structures. Uncertainties shall be taken into account.

h. The “extreme wind” load case shall be represented and quantified in the PSA model with an adequate number of initiating events.

i. When modelling the “extreme wind” load case, a loss of offsite power supply shall be assumed. Alternatively, the probability of failure based on a fragility analysis shall be determined.

j. At one second wind gust velocities 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.

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

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. The different conditions in full power and non-full-power operation shall be taken into account.

4.6.4 Tornadoes

a. For the tornado categories of the Enhanced Fujita scale (EF scale), the wind gust speeds and the mean frequencies of occurrence shall be taken from Appendix 7, Table A7-1.

b. The mean dimensions of the strike areas of the tornadoes shall be taken from Appendix 7, Table A7-2.

c. Using the frequency of occurrence, the dimensions of the strike area and the dimensions of the site area, the annual frequency of tornado impact on the site area shall be determined for each tornado category. The uncertainties shall be taken into account.

d. A tornado hazard curve (annual frequency of exceedance of wind gust speed at the site area) shall be derived for the mean value and the 5%, 50%, and 95% fractiles.

e. 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.

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

g. The “tornado” load case shall be represented and quantified in the PSA model with an adequate number of initiating events.

h. When modelling the “tornado” load case, a loss of offsite power supply shall be assumed. Alternatively, the probability of failure based on a fragility analysis shall be determined.

i. For each tornado 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.

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

k. 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. The different conditions in full-power and non-full-power operation shall be taken into account.

4.6.5 External floods

a. The following categories of flooding events shall be considered in the PSA:

   1. Heavy rainstorms or sudden large snowmelt events causing a high river water level at the plant

   2. Failures of water flow control structures (e.g. dams, weirs, levees) both up and downstream as well as on-site

      Potential domino failures and simultaneous failures (e.g. due to earthquakes) shall be considered.

   3. Intense precipitation events at the site and in the local vicinity

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

   1. Outflow possibilities on the site (drainage, slope of the area)

   2. Local water flow control facilities including operational and maintenance requirements and procedures

   3. Pathways for water ingress

4. Flood-exposed structures and components

5. The potential for roof ponding (i.e. examination of roofs, roof drainage systems, maintenance procedures)

6. Local factor that may exacerbate the effects of flooding (e.g. clogging of drains and damming of a river by landslides or log jam).

c. Based on the flow rates data at the site, a flood hazard curve (annual exceedance frequency of maximum flow rates) shall be developed. Insights into historical flood events shall be used either for the derivation of the flood hazard curve or for its plausibility check.

d. In order to determine the water level at critical structures, 2D flooding calculations with sediment transport shall be carried out, accounting for local topographical and hydrological features. In particular, river bottlenecks at risk of log jam, whose accumulation or break-up can have a relevant impact on the water level at the site of the nuclear power plant, shall be identified. The probability of debris jam shall be considered when determining the frequency of exceedance of critical water levels. Similarly, hydraulic structures, whose malfunction may have a relevant impact on the water level at the site of the nuclear power plant, shall be identified and the probability of a malfunction in determining the frequency of exceedance of critical water levels shall be considered.

e. The failure frequency and the failure consequences of hydraulic engineering facilities shall be determined for each construction type.

f. In case a detailed study following Paragraph e above is not performed, 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 an error factor of 10) with the following consequences:

   1. 100% reservoir inventory loss in 10% of the dam/weir failures

   2. 50% reservoir inventory loss in 80% of the dam/weir failures

   3. 20% reservoir inventory loss in 10% of the dam/weir failures

g. Hazards due to extreme rainfall in the local vicinity of the plant can be screened out in the PSA if the 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.

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

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

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

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

l. Hazards due to domino failure or simultaneous failure of hydraulic engineering facilities can be screened out if a quantitative estimate shows that the sum of the *CDF* and *FDF* contributions respectively of such events is lower than 10^{-9} per year.

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

4.6.6 Aircraft crash

The following three aircraft categories shall be considered in the PSA:

a. Commercial aircraft (mass > 5.7 tons)

b. Jet-powered combat aircraft

c. Light aeroplanes (mass < 5.7 tons) and helicopters

4.6.6.1 Commercial aircraft

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

a. Commercial aircraft crash on the reactor building

b. Commercial aircraft crash on the bunkered emergency building

c. Commercial aircraft crash on other buildings, if relevant

d. Commercial aircraft crash on the remaining plant area

4.6.6.1.1 Determination of crash frequency

a. The aircraft crash frequency shall be estimated using the four-factor formula below:

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

with:

F estimated annual aircraft crash impact frequency on a given target (specific plant building or area)

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

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

$\rho_{i,j}$ conditional aircraft crash density per exposed area in the vicinity of the airport or per exposed flight length for the in-flight phase

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

i index for flight phase

j index for airport or air corridor

b. Depending on the site, the analysis of the commercial aircraft crash frequency shall distinguish between the following flight phases:

1. Operation in the vicinity of the airport (i.e. take-off and landing)
2. In-flight operation

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

d. All airports within a radius of 50 km around the plant shall be considered.

e. For the crash rate in the vicinity of the airport, there shall be a distinction between departures and arrivals. For departures, a lognormal distribution with mean value $C = 9.4 \cdot 10^{-8}$ and error factor 3 shall be assumed. For arrivals, a lognormal distribution with mean value $C = 4.7 \cdot 10^{-7}$ and error factor 3 shall be assumed.

f. For the vicinity of the airport, the conditional aircraft crash density $\rho_{AV,j}$ shall be calculated as follows:

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

with:

g power-off glide ratio ($g = 17$)

h_j average flying altitude [km] in the vicinity of the airport

g. For the estimation of the annual in-flight aircraft operations N, all air corridors within a radius of 100 km from the site shall be considered. The $N_{T,j}$ (number of in-flight operations on air corridor j) and $\rho_{T,j}$ shall be determined separately for the entire set of air corridors, or for a reduced set of air corridors pooled together by bounding aggregations.

h. For the crash rate for in-flight operation, a lognormal distribution with mean value $C = 3.4 \cdot 10^{-11}$ (per kilometre) and error factor 3 shall be assumed.

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

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

with:

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

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

and:

j index of air corridor

d_j flight distance in corridor j from which the plant can be reached in a glide (i.e. with failed engines) [km]

A_j crash exposure area for aircrafts coming from specific air corridor j

g power-off glide ratio (g = 17)

h_j average flying altitude [km] for air corridor j

b_j horizontal component of the minimum distance [km] between the air corridor j and the nuclear power plant

j. The virtual impact area of a building $A_{virt,\ building}$ 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_{gr} ground area of the building = (length of the building + 1/2 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 aircrafts 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°, $f_k = 1/\sqrt{3}$ can be assumed, otherwise f_k = 1.)

For the calculation of the virtual crash area shielding offered by adjacent buildings may be credited considering the impact angle φ_k and the real dimensions of the shielding buildings. Round buildings shall be treated as enveloping rectangular buildings.

k. 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 a radius r = 100 m
m	index of the building

4.6.6.1.2 Direct effects of an aircraft crash (mechanical impact)

a. For the reactor building and the bunkered emergency building, the conditional failure probability (given that the plane hits the building) shall be assessed considering the variability in aircraft type (e.g. dimensions, weights) and velocities. Local (i.e. wall penetration) and global (e.g. overturn, displacement) damages to the buildings shall be considered.

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

c. For accident sequences involving penetration of the building wall, either guaranteed failure of all equipment within the building shall be assumed, or the assumptions on the damage incurred due to debris, internal fires, internal floodings and further consequential effects shall be justified by means of detailed analyses.

d. For any building for which no conditional failure probability was assessed, guaranteed failure of all equipment located within the building shall be assumed in case of a crash on the building. Furthermore, no actions of personnel present in the building shall be credited.

4.6.6.1.3 Indirect effects of an aircraft crash (debris, fire and explosion effects)

a. The effects of debris, fires and explosions 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.

b. For buildings designed against missile impact, only fire effects shall be assessed considering fire and explosion sources (e.g. aviation fuel or 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 aviation fuel in the plant area.

c. Guaranteed failure of all equipment located within the building shall be assumed if the protection against the indirect effects of an aircraft crash appears insufficient according to an applicable analysis.

d. All outdoor equipment shall be assumed to be failed. In particular, a Loss of Offsite Power (LOOP) shall be assumed.

4.6.6.2 Jet-powered combat aircraft

a. The *CDF* and *FDF* contribution of the following initiating events shall be quantified:

   1. Combat aircraft crash on the reactor building

   2. Combat 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 may be described by a lognormal distribution with a mean value and standard deviation calculated from the data.

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

4.6.6.3 Light aeroplanes and helicopters

a. The *CDF* and *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 per unit area shall be directly quantified from the number of crash occurrences in Switzerland. The time interval to be considered shall at least comprise the most recent 5 years. The uncertainty may be described by a lognormal distribution with a mean value and standard deviation calculated from the data.

c. Guaranteed failure of all equipment located within a building not designed to resist to the impact of debris 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 estimation of the *CDF* and *FDF* contribution due to light-aircraft crash yields a respective value that is 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 respectively.

b. The assessment shall include:

   1. A detailed review of the relevant available information
   2. A plant walkdown (if necessary)
   3. An identification of possible hazard scenarios
   4. A determination of the conditional probabilities of SSC failures (fragilities) and human errors

c. The event shall be implemented in the PSA model.

4.7 Quantification and Level 1 PSA results

4.7.1 Quantification

a. To quantify the PSA model, 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* and *FDF*, respectively).

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

d. Cutsets/sequences with mutually 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 correlation effects.

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 respective *CDF* and *FDF* contributions categorized by groups of initiating events shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-1).

b. The *CDF* and *FDF* contributions respectively of all individual initiating events shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-2).

c. The *FDF* contribution of each plant outage state shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-3).

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 full-power and non-full-power-operation of the plant, the 1,000 most important basic events, sorted by Fussell-Vesely (*FV*) and Risk Achievement Worth (*RAW*) values shall be provided (cf. Appendix 8, Table A8-4).

b. For each operating mode modelled, the most important components, sorted by *FV* and *RAW* shall be provided. The lists shall contain all components significant to safety in accordance to guideline ENSI-A06, Chapter 6.5 a (cf. Appendix 8, Table A8-5).

c. For each operating mode modelled, the 30 most important personnel actions, sorted by *FV* and *RAW* shall be provided (cf. Appendix 8, Table A8-6).

d. For each operating mode modelled, the *FV* and *RAW* values of all systems considered in the PSA shall be provided (cf. Appendix 8, Table A8-7).

e. For each operating mode modelled, a list of approximately the 10,000 most important failure sequences shall be provided where possible (cf. Appendix 8, Table A8-8).

f. For full-power and non-full-power operation of the plant, a ranking of the 30 most important accident sequences of the model shall be provided (cf. Appendix 8, Table A8-9).

4.7.2.3 Insights

a. Any (potential) improvements (backfits) of the plant (including the procedural guidance for its operation) identified during the development of the PSA shall be evaluated and documented.

b. 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.

c. It shall be investigated whether a historical trend in the component reliability data or the initiating event frequencies can be observed.

d. The risk insights of the updated PSA shall be compared with the risk insights from the previous version of the PSA performed by the licensee 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 resulting from the Level 1 PSA that have similar severe accident progression and containment response characteristics shall be grouped into Plant Damage States (PDS). The PDS shall be characterized using at the minimum the following attributes:

   1. The type of the initiating event (e.g. transient or LOCA, etc.)

      Only for separated Level 1/Level 2 models.

   2. The reactor coolant system pressure at the time of core or fuel damage (if the core is inside the vessel)

   3. The status of front-line systems

   4. The containment isolation status

      Availability of containment isolation systems shall be modelled explicitly using fault tree techniques.

   5. Accident sequences resulting in containment bypass (i.e. steam generator tube rupture (SGTR) for PWR, and interfacing system LOCA), and

   6. The status of containment systems for heat removal or pressure reduction and of the systems for reduction of fission products.

      Availability of containment heat removal systems credited in the Level 2 PSA shall be modelled explicitly using fault tree techniques.

b. For the grouping of non-full-power 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.

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

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

e. The characteristics and mean frequencies of the PDSs shall be presented preferentially in a form of a PDS matrix.

5.2 Containment performance

a. To determine the containment response to accident conditions, a structural response analysis that is consistent with the state of the art shall be performed.

b. All relevant containment design data regarding the structural response analysis shall be considered, such as:

   1. Properties of construction materials and reinforcement
   2. Sizes and locations of containment penetrations
   3. Penetration seal configuration and materials
   4. Local discontinuities, e.g. shape transitions, changes in steel shell or concrete reinforcement
   5. 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 data.

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, the impact of temperature 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 all containment failure locations. These analyses shall provide best-estimate failure pressures at given temperatures 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 uncertainties to arrive at the failure location fragilities. These fragilities shall be combined to an enveloping fragility curve (pressure and temperature dependent) for the entire 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 available results in literature for a similar containment design, and differences discussed.

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:

   1. 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)
   2. In-vessel melt-coolant interactions (including energetic steam explosions)
   3. Interaction of core debris with the reactor pressure vessel (RPV) lower head and lower head failure modes (including the impact of external lower head cooling, if applicable)
   4. Loss of primary coolant system integrity
   5. High pressure melt ejection
   6. RPV failure
   7. Containment pressurization due to steam and non-condensable gas blowdown from the primary coolant system
   8. Vessel thrust forces (in case of RPV failure at high pressure)
   9. Direct Containment Heating (DCH)
   10. Melt-dispersal and spreading

11. Ex-vessel melt-coolant interactions (including energetic steam explosions)

12. Core Concrete Interactions (CCI), considering debris coolability, basemat and side wall attack by core debris, hydrogen and carbon monoxide generation, and generation of other non-condensable gases (e.g. carbon dioxide)

13. Quasi-static pressurization due to 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 into fuel assemblies or potential for increased oxidation and zirconium fire).

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

5.4 Severe accident progression

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

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

1. From core or fuel damage to vessel breach

2. Immediately after vessel breach

3. Longer-term following vessel breach

c. The nodal questions in the APET shall address:

1. Severe accident phenomena

2. The availability of systems required for severe accident management (e.g. containment venting system, circulating air cooler, hydrogen recombiners)

3. Actions related to severe accident management including recovery of power and/or system functions (e.g. actuation of containment heat removal)

4. The status of containment

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

e. When assessing nodal probabilities of operator actions, characteristic boundary conditions for the Level 2 PSA shall be considered (e.g. the less binding nature of written guidance, increased stress and workload). A general consideration of these conditions using the conservative ASEP screening method is acceptable.

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

    1. 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. Alternatively, the quantification of the APET nodal probabilities potentially involving significant uncertainties should be supported by sensitivity cases covering the broad range of uncertainties. If a computer code is used to support these sensitivity cases, the range of parameters should be clearly justified and documented.

    2. The limitations of the computer codes used shall be taken into consideration when addressing uncertainties in the phenomenological issues.

g. A minimum mission time of 48 hours after the initiating event 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), core damage or fuel damage is considered imminent, this mission time shall be extended beyond 48 hours.

h. 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:

    1. Containment status, for instance open due to shutdown activities, vented, isolated (with respect to the expected leakage), non-isolated, bypassed, ruptured, or basemat penetrated

    2. Time of release (e.g. early or late)

    3. Mode of ex-vessel release (i.e. dry or submerged core concrete interaction)

4. Effectiveness of containment fission product removal mechanisms (e.g. scrubbing by containment sprays or by an overlying water pool)

i. 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 releases.

b. The source terms shall be represented by radiological groups characterizing the radiological inventory of the fuel. These groups shall be based on similarities in thermodynamic and chemical properties of the various radionuclides. As a minimum the radiological groups according to Appendix 8, Table A8-10 shall be considered.

c. The source term calculations shall be based on a plant-specific model adequately representing the radiological inventory of the fuel, the RCS and secondary coolant system for PWR, the water-steam cycle for BWR respectively, the containment and safety systems, etc. A state-of-the art, fully integrated computer code shall be used coupling 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.

5.6 Quantification and 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 throughout the model.

c. An integrated 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 regarding 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 documentation (cf. Appendix 8, Table A8-11).

b. The contribution of the PDS or the initiating events to each release category shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-12).

c. The frequency of each release category and other release parameters shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-13).

d. The contribution of the release categories to the *LERF*, *SLERF*, *LRF* and *SLRF* shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-14).

e. The contribution of the initiating event groups to the *LERF* and *SLERF* shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-15).

f. For each release category making a relevant contribution to *TRAR* or *STRAR* respectively, the most important parameters regarding the release categories shall be provided as part of the PSA documentation (cf. Appendix 8, Table A8-16).

5.6.2.2 Importance analysis

For both basic events and components, Fussell-Vesely (*FV*) and Risk Achievement Worth (*RAW*) importance values with regard to *LERF* and *SLERF* shall be provided (cf. Appendix 8, Table A8-17 and Table A8-18). If an integrated PSA model is used, these importance values shall be calculated directly from the model. Otherwise, an approximation is acceptable.

5.6.2.3 Sensitivity analysis

Sensitivity analyses shall address two sets of issues related to the *LERF* and to the *SLERF*, respectively:

a. Determination of the impact of assumptions related to severe accident phenomenological issues

b. Other significant modelling assumptions that were employed in the Level 2 analysis

5.6.2.4 Insights

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

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

   1. any modifications are required for the plant-specific Severe Accident Management Guidance (SAMG),

   2. there are any issues to be investigated in future severe accident research programs.

c. 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.

6 Quality assurance

6.1 QA process and peer review

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

b. The team conducting a new PSA or an update of a PSA shall consist of members having extensive hands-on experience and broad knowledge of PSA, as well as the installation.

c. The licensee (or the applicant for a licence) shall be strongly involved in the development, updating 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 shall 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

6.2.1 Content-related requirements

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.

c. All important details of the methods and data used in the PSA development 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.

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

e. All PSA information and data sources shall be cited. The referenced documents should be accessible.

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

6.2.2 Submission-related regulations

a. The PSA documentation can be submitted to ENSI electronically (i.e. in a searchable format on a digital media).

b. A summary report providing general information on the preparation of the PSA, the overall results of the PSA according to Chapters 4.7.2 and 5.6.2 as well as the corresponding applications of the PSA according to the guideline ENSI-A06 shall be submitted to ENSI.

c. The level 1 PSA models shall be submitted electronically together with appropriate viewer software. In case of the Level 2 PSA models, at least the fault trees and event trees shall be submitted electronically.

7 PSA for other nuclear installations

7.1 Research reactors and intermediate storage facilities

For research reactors and intermediate storage facilities the following probabilistic analyses shall be conducted in the framework of the licensing procedure and the implementation of the risk-based aspects in Art. 22 of the Nuclear Energy Ordinance:

a. For all accidents referred to in Art. 8 of the Nuclear Energy Ordinance 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 they apply to the facility.

b. If the sum of all accident frequencies with a dose rate larger than 1 mSv amounts to at most $1 \cdot 10^{-6}$ per year, 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.

7.2 Deep geological repositories

In the context of the licensing procedures for construction and operation of deep geological repositories including part of the plant such as the main facility, pilot facility, access structures and surface facilities the following PSA requirements apply:

a. A risk metric shall be suitably defined to quantify the risk caused by accidents in the deep geological repository.

b. A PSA according to the technical requirements of Chapters 4 to 6 of this guideline shall be developed, insofar as these requirements are appropriate and applicable. This PSA is to enable a risk assessment of nuclear safety and balance in the design.

This guideline was approved by ENSI on 19 January 2018.

The Director General of ENSI: signed H. Wanner

Appendix 1: Definition of terms (according to ENSI Glossary)

Basic event

A basic event is an event in a fault tree that is not subdivided further, e.g. the failure to start of a pump.

Category A actions

Category A actions comprise actions in routine testing and in maintenance and repair of systems that are performed prior to the initiating event and may lead to errors contributing to the unavailability of systems needed during the accident sequence.

Category B actions

Category B actions comprise actions or errors that contribute to the occurrence of an initiating event.

Category C actions

Category C actions comprise actions taken to prevent or mitigate accidents according to the instructions in operating and emergency operating procedures, and accident management measures.

Category C actions in accident sequences requiring the emergency response team

Category C actions in accident sequences requiring the emergency response team comprise actions whose applicable procedure calls for prior consultation of the emergency response team or which are required in an accident that is sufficiently serious (e. g. necessity of accident management measures) to expect an involvement of the emergency response team in decision-making.

Common Cause Failure (CCF)

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

Core Damage Frequency (*CDF*)

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

Error of Commission (EOC)

An Error of Commission is an action with a negative influence on the accident sequence resulting from an error, a mistake or a misdirection by faulty or unclear instructions or indications.

Fire compartment

A fire compartment is an area of buildings and installations that is separated from other fire compartments by enclosing structures such as fire barriers, walls and ceilings, fire-retarding sealing and bulkheads.

Flood area

The flood area is considered to be the area of the plant 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.

Fuel Damage Frequency (*FDF*)

The Fuel Damage Frequency 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.

Full-power operation

Full-power operation comprises the operating states during the commercial plant operation at full-power and comparable low-power states.

Fussell-Vesely importance (*FV*)

The Fussell-Vesely importance FV_i is a measure for the importance of a basic event *i*. It indicates by which relative portion the risk *R* (*CDF*, *FDF*, *LERF*, or *SLERF*) would decrease, if the occurrence of the basic event were guaranteed to be avoided and is calculated as follows:

$FV_i = (R - R_S) / R$

where

R_S: risk in case of guaranteed non-occurrence of basic event *i*

R: mean risk

Human Error Probability (HEP)

The Human Error Probability is the failure probability of an operator action required in an accident.

High Confidence of Low Probability of Failure (*HCLPF*)

The *HCLPF* designates the level of seismic ground motion, at which there is a high (95 %) confidence of a low (≤ 5 %) 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

An integrated PSA model permits the continuous calculation of accident scenarios from the initiating event to the release category without the need for grouping of core damage states in the transition from Level 1 to Level 2 PSA outside of the automatic quantification of the model.

Level 1 PSA

The Level 1 PSA is the probabilistic safety analysis to identify and quantify the accident sequences leading to the onset of core or fuel damage, respectively.

Level 2 PSA

The Level 2 PSA is the probabilistic safety analysis to explore the processes taking place after core or fuel damage as well as to quantify the frequency of radioactive releases and their magnitude.

Large Early Release Frequency (*LERF*)

The *LERF* is the expected number of events at full-power operation per calendar year with a release of more than $2 \cdot 10^{15}$ Bq of Iodine-131 to the environment within 10 hours after core damage.

Large Release Frequency (*LRF*)

The LRF is the expected number of events at full-power operation per calendar year with a release of more than $2 \cdot 10^{14}$ Bq of Caesium-137 to the environment.

Master Logic Diagrams (MLD)

The Master Logic Diagram (MLD) is a method used to identify initiating events. An MLD is a logic diagram similar to a fault tree, but without its formal mathematical properties. The MLD begins with a top event “Core Damage” and splits with ever increasing refinement into the individual contributing events.

Non-full-power operation

Non-full-power operation comprises all operating modes other than full-power operation.

Performance Shaping Factors (PSFs)

Performance Shaping Factors are plant and scenario-specific influences on the failure probability of operator actions.

Permanent combustibles

Permanent combustibles are combustibles that are permanently installed or stored in a certain area of the plant.

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

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

PSA for full-power operation

The PSA for full-power operation assesses the risk caused by initiating events during full-power operation.

PSA for non-full-power operation

The PSA for full-power operation assesses the risk caused by initiating events during non-full-power operation.

PSA component

A PSA component is any component explicitly modelled in the PSA.

PSA-relevant

Structures, systems, components, operator actions, fire compartments and flood areas are PSA-relevant if they need to be considered in the PSA model.

Risk Achievement Worth (*RAW*)

The Risk Achievement Worth RAW_i is a measure for the importance of a basic event *i*. This importance measure indicates by which factor the risk *R* (*CDF*, *FDF*, *LERF*, and *SLERF*) will increase, if the basic event is guaranteed to occur, and is calculated as follows:

$RAW_i = R_F / R$

where

R_F: risk at guaranteed occurrence of basic event *i*

R: mean risk

Recovery Action

A Recovery Action is an alternate measure to restore a safety function unavailable due to a component failure (e. g. manual opening of a valve after failure of the automatic opening signal) in which the execution of the action may be specified independently of the cause of the component failure. Repairs of failed components thus are no Recovery Actions to be considered within the scope of an HRA.

Shutdown Large Early Release Frequency (*SLERF*)

The S*LERF* is the expected number of events at non-full-power operation per calendar year with a release of more than $2 \cdot 10^{15}$ Bq of Iodine-131 to the environment within 10 hours after fuel damage.

Shutdown Large Release Frequency (*SLRF*)

The *SLRF* is the expected number of events at non-full-power operation per calendar year with a release of more than $2 \cdot 10^{14}$ Bq of Caesium-137 to the environment.

Shutdown Total Risk of Activity Release (*STRAR*)

The risk measure *STRAR* is an indication for the expected total release of radioactive materials after a fuel damage per calendar year. It is calculated by multiplying, beginning at the *FDF*, the frequency of each release category by its corresponding source term and taking the sum of these products.

unit: Bq/year

Temporary combustibles

Temporary combustibles are combustibles that are temporarily stored in certain areas (in particular during non-full-power operation of the plant).

Transient combustibles

Transient combustibles are combustibles that can appear at different locations.

Total Risk of Activity Release (*TRAR*)

The risk measure *TRAR* is an indication for the expected total release of radioactive materials after a core damage per calendar year. It is calculated by multiplying, beginning at the *CDF*, the frequency of each release category by its corresponding source term and taking the sum of these products.

unit: Bq/year

Appendix 2: Abbreviations

APET	Accident Progression Event Tree
ASEP	Accident Sequence Evaluation Procedure
ATWS	Anticipated Transient without Scram
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCI	Core Concrete Interaction
CDF	Core Damage Frequency
DCH	Direct Containment Heating
ECCS	Emergency Core Cooling System
EF Scale	Enhanced Fujita Scale
EOC	Error of Commission
FDF	Fuel Damage Frequency
FMEA	Failure Mode and Effect Analysis
FV	Fussell-Vesely (Importance)
HCLPF	High Confidence of Low Probability of Failure
HEP	Human Error Probability
HID	Hazard Input Document
HRA	Human Reliability Analysis
LBB	Leak Before Break
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LRF	Large Release Frequency
MLD	Master Logic Diagram
NPP	Nuclear Power Plant
PDS	Plant Damage State
PGA	Peak Ground Acceleration
PGV	Peak Ground Velocity

POS	Plant Operating State
PSA	Probabilistic Safety Analysis
PSF	Performance Shaping Factor
PSHA	Probabilistic Seismic Hazard Analysis
PWR	Pressurized Water Reactor
QA	Quality Assurance
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RPV	Reactor Pressure Vessel
SAMG	Severe Accident Management Guidance
SGTR	Steam Generator Tube Rupture
SI	Système international d'unités
SLERF	Shutdown Large Early Release Frequency
SLIM	Success Likelihood Index Methodology
SLRF	Shutdown Large Release Frequency
SSC	Structure, System and Component
STRAR	Shutdown Total Risk of Activity Release
THERP	Technique for Human Error Rate Prediction
TRAR	Total Risk of Activity Release

Appendix 3: Description sheet for Category A 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 other failure events

Appendix 4: Description sheet for Category C 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		Characteristics of the quantification, for example, dependence on other failure events

Appendix 5: Human error probabilities in case of earthquake

A5.1 Simplified adjustment

A5.1.1 Basic model

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

1. 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 human actions can be taken over from the model for internal events (transients and LOCAs) without modification.
2. 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.
3. From 0.6 g, all personnel actions shall be considered as guaranteed failed.

The model is described graphically in Figure A5-1:

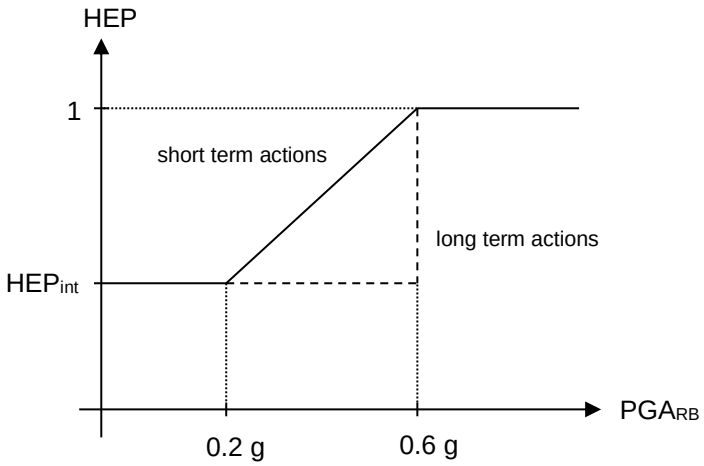

Figure A5-1: Dependence of HEPs on the earthquake intensity

A5.1.2 Refined basic model

1. In the earthquake PSA, those human actions for which the
   a. instrumentation or
   b. guidance within the emergency operating procedures

   needed for diagnosis, execution or monitoring is not available, shall be set as guaranteed failed.
2. If the instrumentation and operating procedures are available, the HEP is determined as follows:
   a. Up to a PGA of 0.2 g (at the foundation level of the reactor building), the HEPs can be taken over from the model for internal events without modification.

b. To determine the HEP when the PGA is above the 0.2 g lower bound, the required actions are divided into short term (required < 1 h after earthquake), mid term (required 1-12 h after earthquake), and long term (required > 12 h after earthquake) actions. The limit (12 h) for beginning of the long-term range can be reduced to 8 hours, if precautions have been taken to ensure external support within 8 hours even if the earthquake accident occurs outside normal working hours and involves the destruction of normal access roads.

c. In case of a PGA above 0.2 g, the HEP increase from HEP_{int} (the HEP value from the model for internal events) is modeled as a function of PGA via a lognormal distribution:

$$\mathrm{HEP} = \begin{cases} \mathrm{HEP_{int}} + (1\text{-}\mathrm{HEP_{int}})\Phi\left[\dfrac{ln\left(\frac{\mathrm{PGA}-0.2g}{0.273g}\right)}{0.566}\right], & \text{short term actions} \\ \mathrm{HEP_{int}} + (1\text{-}\mathrm{HEP_{int}})\Phi\left[\dfrac{ln\left(\frac{\mathrm{PGA}-0.2g}{0.4g}\right)}{0.566}\right], & \text{mid term actions} \\ \mathrm{HEP_{int}} + (1\text{-}\mathrm{HEP_{int}})\Phi\left[\dfrac{ln\left(\frac{\mathrm{PGA}-0.2g}{0.586g}\right)}{0.566}\right], & \text{long term actions} \end{cases}$$

where Φ(...) is the cumulative distribution function of the standard normal distribution.

Appendix 6: Experts in the PSHA

With regard to the involvement of experts in the PSHA, the following requirements and responsibilities apply.

1. Requirements for the technical project managers:
    a. They shall be internationally recognized experts.
    b. They shall collectively have proven knowledge and experience in the areas of PSHA implementation, modelling and calculation, expert elicitation and applied probability techniques.
    c. Their expertise in their subproject shall be at least equal to that of the evaluators.
2. Responsibilities of the technical project managers:
    a. They are responsible for the technical implementation of the PSHA and the technical correctness of the results.
    b. They are responsible for the facts that every evaluation considered in the PSHA model is documented traceably and each evaluator scrutinizes and assesses whether the evaluation is based on an acceptable reasoning.
    c. They are responsible for ensuring that the evaluators are aware of the evaluative nature of their task, strictly comply with their role and, in particular, do not act in the role of an advocate of specific technical aspects.
    d. They are responsible for the fact that interface problems between the individual subprojects are identified and do not lead to double counting of uncertainties.
    e. They are responsible for the fact that in the PSHA model the uncertainty is captured thoroughly, systematically and split into aleatoric and epistemic contributions.
    f. In view of the reproducibility of the PSHA, they are responsible for the fact that both the PSHA process and results are documented fully traceable.
3. Requirements for the evaluators:
    a. He is a nationally or internationally recognized expert in his area of responsibility, able to identify alternative models, hypotheses and theories of the international community, to assess their validity and to carry out evaluations by means of statistics.
    b. He is not a member of the technical project management.
4. Responsibilities of the evaluators:
    a. In his subproject he is jointly responsible for the technical correctness of the contribution to the results of the PSHA and for the fact that the uncertainty is captured thoroughly, systematically and split into aleatoric and epistemic contributions.
    b. In view of the reproducibility of the PSHA, he is responsible for the fully traceable documentation of his evaluations including the underlying considerations and reasoning.
    c. He scrutinizes and assesses each evaluation of his subproject that is considered in the PSHA model as to whether the evaluation is based on an acceptable reasoning.

d. He confirms in writing that, in his opinion, the Hazard Input Document (HID) resulting from the evaluations of his subproject accurately and completely reflects the evaluations and is valid as the sole input of the subproject in the hazard calculation.

e. Taking into account the necessary sensitivity analyses and the well-reasoned alternative models, hypotheses and theories of the international community in his area of responsibility, he confirms in writing that in his opinion the centre, body and range of the uncertainty in the results of the PSHA represent the state of the art already consolidated or recognized to be so soon.

5. Responsibilities of the expert conducting the numerical hazard computation:

   a. He is co-author of the HIDs and confirms in writing that the HIDs contain all the information needed as input for the computer program.

   b. He confirms in writing that he, if necessary after consultation with the subproject managers or the evaluators, has transferred to the input format required by the computer program the information contained in the HIDs completely and without content-related interpretations or simplifications.

Appendix 7: Requirements for the determination of the tornado hazard

Table A7-1: Annual frequencies of tornado occurrence

Tornado Category	Wind Speed (3 s Gust) [km/h]	Frequency of Occurrence [per year and km^2] (Mean)
EF0	[105, 137)	1.23E-04
EF1	[137, 177)	5.53E-05
EF2	[177, 217)	1.59E-05
EF3	[217, 266)	4.65E-06
EF4	[266, 322)	1.04E-06
EF5	[322, ...]	1.00E-07

Table A7-2: Dimensions of tornado strike areas

Tornado Category	Length of Strike Area [km] (Mean)	Width of Strike Area [km] (Mean)
EF0	2.6	0.035
EF1	6.9	0.082
EF2	10.2	0.124
EF3	17.5	0.343
EF4	23.1	0.383
EF5	53.4	0.450

Appendix 8: Reportable results

Table A8-1: Contribution of initiating event categories to *CDF* and *FDF*, respectively

Groups	Initiating Event Category	*CDF* or *FDF*				Contribution to Grand Total [%] (Mean)
		Mean	5 %	50 %	95 %	
	Transients					
	LOCA					
Internal Events (Total)						
	Fires					
	Internal floods					
	Other internal plant hazards					
Internal Plant Hazards (Total)						
	Earthquakes					
	Extreme winds and tornadoes					
	External floods					
	Aircraft crash					
	Other external plant hazards					
External Plant Hazards (Total)						
Grand Total (*CDF* or *FDF*)						

Table A8-2: Contribution of the initiating events to *CDF* and *FDF*, respectively

Initiating Event			
ID	**Description**	**Frequency**	***CDF* or *FDF* (Mean)**
Seismic 1			
Fire 1			
…			

Table A8-3: Contribution of the non-full-power operating modes to *FDF*

Operating Mode		Reactor Cooling System				Containment	Activation of the Safety Systems	Duration [h]	Contribution to *FDF* [%]
ID	Description	$P_{abs.}$ [bar]	T [°C]	Pressurizer Level (PWR) [%]	RPV				
A1	*Shutdown*	*150-20*	*300-150*	*60*	*closed*	*closed*	*automatic*	*20*	*6.3*
A2	*Fuel Unloading*								
...									

Table A8-4: Both *FV* and *RAW* values of basic events with regard to *CDF* and *FDF,* respectively

	Basic-Event ID	Description	*FV* or *RAW*
1			
2			

Table A8-5: Both *FV* and *RAW* values of components with regard to *CDF* and *FDF,* respectively

	Component ID	Description	*FV* or *RAW*
1			
2			

Table A8-6: Both *FV* and *RAW* values of personnel actions with regard to *CDF* and *FDF,* respectively

	Personnel-Action ID	Description	*FV* or *RAW*
1			
2			

Table A8-7: Both *FV* and *RAW* values of the systems with regard to *CDF* and *FDF,* respectively

	System ID	Description	*FV* or *RAW*
1	*TH*	*TH system (all safety functions)*	
2	*TH Recirculation*	*TH system, recirculation mode*	
3	*TH Injection*	*TH system, feed mode*	

Table A8-8: Most important cutsets with regard to *CDF* and *FDF* contributions, respectively

	Contribution to *CDF* or *FDF* (Mean)	[%]	Cutset	
			Name	Description
1	*1.63E-06*	*6.00*	*IEXZ1*	*Initiating event XZ1*
			XY111ABC	*Diesel generator 111 fails to start*
			AXYZNCC	*CCF of components XYZ*
2	…			

Table A8-9: Description of most important accident sequences with regard to *CDF* and *FDF* contributions, respectively

Sequence Number	
Sequence Frequency [yr^{-1}]	
Contribution to *CDF* or *FDF* [%] (Mean)	
Initiating Event	
Unavailabilities due to Initiating Event – **Direct, Guaranteed Failure** – **Dependent Failure (e.g. Fragility)**	
Support Systems Failed	
Safety Systems Failed	
Personnel Actions Failed	
Description	

Table A8-10: Radiological groups for the source term analysis

No.	Representative	Group Name	Remark
1	Xe	Noble Gases	
2	I	Halogens	CsI shall be grouped to the halogens
3	Cs	Alkali Metals	CsOH shall be grouped to the alkali metals
4	Te	Chalkogens	
5	Ba	Alkaline Earth Metals	
6	Mo	Transition Metals	
7	Ru	Platinoids	
8	Ce	Tetravalents	
9	La	Trivalents	

Table A8-11: PDS matrix (simplified example)

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

Table A8-12: Contribution of PDS or Initiating Events to the release categories

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

Table A8-13: Release Categories

Release Category		Frequency [yr^{-1}]	Time of Release [h] Time of the (first) release of noble gases	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 %													

Table A8-14: Contribution of release categories to *LERF, LRF* and *SLERF,* and *SLRF,* respectively

Frequency [yr^{-1}]						
Risk Measure	**Mean**	**5 %**	**50 %**	**95 %**	**Release Category**	**Contribution**
LERF or SLERF					*RC-3*	*47.1 %*
					RC-6	*43.6 %*
					RC-4	*7.2 %*
					RC-1	*2.1 %*
LRF or SLRF					*RC-6*	*85.1 %*
					RC-1	*10.1 %*
					RC-2	*4.3 %*

Table A8-15: Contribution of initiating event categories to *LERF* and *SLERF*, respectively

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

Table A8-16: Main parameters for each release category with notable contribution to *TRAR* and *STRAR*, respectively

Release Category	Mean Frequency of Release [yr^{-1}]	Activity of Aerosol Release [Bq]	Risk of Aerosol Release [Bq/yr]	Contribution to Aerosol Risk [%]	Total Release (incl. Noble Gases) [Bq]	*TRAR* or *STRAR* [Bq/yr]	Contribution to *TRAR* or *STRAR* [%]
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**

Table A8-17: Both FV and RAW values of basic events with regard to *LERF* and *SLERF,* respectively

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

Table A8-18: Both FV and RAW values of components with regard to *LERF* and *SLERF,* respectively

Component ID	Description	*FV* or *RAW*
1		
2		

ENSI, Industriestrasse 19, 5200 Brugg, Switzerland, Phone +41 56 460 84 00, info@ensi.ch, www.ensi.ch