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): Applications

## Guideline for Swiss Nuclear Installations

**ENSI-A06/e**

**Edition November 2015**

# Probabilistic Safety Analysis (PSA): Applications

Edition November 2015

**Guideline for Swiss Nuclear Installations** **ENSI-A06/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-A06/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 regulatory authority or based on a mandate in an ordinance. Guidelines are support documents that formalise the implementation of legal requirements and facilitate uniformity of implementation practices. They further 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

This guideline formalises the requirements for the application of Probabilistic Safety Analysis (PSA) for nuclear power plants. It presents the general principles, the requirements for maintenance and upgrade of the PSA, as well as the minimum required scope of PSA applications. The risk measures and applicable evaluation criteria are defined for these PSA applications.

# 3 Legal basis

This guideline implements the legal requirements stated in:

a. Article 33, paragraph 1, letter a of the Nuclear Energy Ordinance (732.11)

b. Article 34, paragraph 2, letter d of the Nuclear Energy Ordinance (732.11)

c. Annex 5 of the Nuclear Energy Ordinance (732.11) regarding the list of plant modifications relevant for PSA

d. Annex 3 of the Nuclear Energy Ordinance (732.11) regarding the current plant-specific PSA

e. Article 82 in connection with article 8, paragraph 5, of the Nuclear Energy Ordinance (732.11)

f. Article 12 of the Ordinance on the Hazard Assumptions and the Assessment of the Protection against Accidents in Nuclear Installations (732.112.2)

# 4 General principles

a. The use of the current, plant-specific PSA model that meets the requirements of the guideline ENSI-A05 is mandatory for PSA applications.

b. A justification is necessary if the full-scope PSA model is not used in accordance with the guideline ENSI-A05.

c. Plant modifications and operational experience with impact on plant safety shall be evaluated by the licensee with relevant deterministic, operational and probabilistic arguments.

d. As part of the Periodic Safety Review (PSR), the licensee shall demonstrate that the sum of all plant modifications is either risk-neutral or results in a reduction in risk.

e. The uncertainties quantified with the PSA as well as the model uncertainties shall be adequately considered in the application of PSA.

# 5 Maintenance and upgrade of the PSA

a. A current, plant-specific PSA shall be periodically maintained and upgraded based on the following principles:

b. For the Level 1 PSA:

   1. A complete revision of the PSA shall be carried out no later than the required schedule for the PSR. At this time, it shall be determined whether it is necessary to change the applied methods in order to reflect the state of the art (if not already described in guideline ENSI-A05).

   2. At least once every 5 years, plant-specific data shall be updated and plant modifications shall be incorporated into the PSA model and the associated documentation. The non-full-power PSA shall be updated and submitted to ENSI no later than a year after the update of the full-power PSA has been completed.

   3. If the combined impact of the PSA-relevant plant modifications not yet incorporated in the PSA model is expected to result in more than 10% change in the mean Core Damage Frequency (*CDF*) or the mean Fuel Damage Frequency (*FDF*), respectively, these modifications shall be incorporated into the PSA model and the associated documentation within a year's time.

c. For the Level 2 PSA:

   1. A complete revision of the PSA shall be carried out no later than the required schedule for the PSR. At this time, it shall be determined whether it is necessary to change the applied methods in order to reflect the state of the art (if not already described in guideline ENSI-A05).

   2. The requirement of updating the Level 2 PSA outside the scope of PSR will be decided by ENSI on a case-by-case basis.

d. Changes to the PSA model shall be carried out in accordance with a procedure that ensures that the PSA model represents the current state of the plant. The impact of plant modifications not yet incorporated in the PSA model on the mean *CDF*, the mean *FDF* and the mean Large Early Release Frequency (*LERF*) shall be quantitatively estimated and summarized in a list. The reporting format and contents of the list are specified in Annex 2.

# 6 Required range of PSA applications

This section lists the minimum requirements for PSA applications.

## 6.1 Probabilistic evaluation of the safety level

a. For nuclear power plants the following applies:

   1. Full-power operation: If the mean *CDF* (*LERF*) is greater than $10^{-5}$ per year ($10^{-6}$ per year), measures to reduce the risk shall be identified and – to the extent appropriate – implemented.

   2. Non-full-power operation: If the mean *FDF* is greater than $10^{-5}$ per year, measures to reduce the risk shall be identified and – to the extent appropriate – implemented.

b. If several measures can reduce the mean *LERF* by an equal amount, preference shall be given to measures that not only reduce the mean *LERF* but also reduce the mean *CDF*.

c. The assessment of the safety for operating nuclear power plants shall be carried out during the annual systematic safety evaluation as part of the report on probabilistic evaluation of operational experience (see Annex 3) and as part of the PSR.

## 6.2 Evaluation of the balance of the risk contributors

a. The balance among the contributors to risk shall be investigated as follows:

   1. The balance among the risk contributions from accident sequences, components and human actions shall be evaluated. If any of the accident sequences, components or human actions are found to have a remarkably high contribution to risk, measures to reduce risk shall be identified and – to the extent appropriate – implemented.

   2. If an initiating event category contributes more than 60% to the mean *CDF* and its contribution is more than $6 \cdot 10^{-6}$ per year, measures to reduce risk shall be identified and – to the extent appropriate – implemented.

   3. If the ratio of the mean *CDF* to the $CDF_{Baseline}$ is greater than 1.2, measures to reduce risk due to planned or unplanned maintenance shall be identified and – to the extent appropriate – implemented.

b. The evaluation of the balance of the risk contributions shall at least be carried out in the course of the PSR.

## 6.3 Probabilistic evaluation of the Technical Specifications

### 6.3.1 Probabilistic evaluation of the completeness and the balance of the Completion Times

a. In defining the Completion Times, it shall be ensured that components shown to be significant to safety from the PSA point of view (see Chapter 6.5) are

   1. considered in the Technical Specifications (completeness), and

   2. assigned to correspondingly short Completion Time categories (risk balance).

b. Based on the risk measures *CDF* and *LERF*, a review of the completeness and the balance of the Completion Times shall be carried out in the course of the PSR.

### 6.3.2 Probabilistic evaluation of component maintenance during full-power operation

a. In addition to the deterministic requirements for the maintenance of components (including revision of divisions and trains), the following probabilistic requirements shall be satisfied during power operation:

1. Maintenance work shall be planned in such a way that no component unavailability configuration *i* resulting from maintenance will result in a Conditional Core Damage Frequency ($CCDF_i$; for computation see Annex 3) greater than $1 \cdot 10^{-4}$ per year.

2. Maintenance work shall be planned in such a way that the total cumulative maintenance time for components shall be limited such that the portion of the Incremental Cumulative Core Damage Probability ($IC_{um}CDP$, see Annex 3) resulting from maintenance is less than $5 \cdot 10^{-7}$.

b. Compliance with the requirements mentioned under letter a shall be demonstrated either by a previous bounding analysis along with an additional probabilistic evaluation of operational experience or assessed with the help of a risk monitor. Deviations from the requirements on planning mentioned under letter a shall be justified.

### 6.3.3 Probabilistic evaluation of changes to Technical Specifications

a. The risk impact of all PSA-relevant changes to the Technical Specifications shall be evaluated.

b. A change to the Technical Specifications resulting in an increase in risk is admissible, if

1. the impact of the change on the mean *CDF*, *FDF* and *LERF* is insignificant (i.e. $\Delta CDF < 10^{-7}$ per year, $\Delta FDF < 10^{-7}$ per year, $\Delta LERF < 10^{-8}$ per year), and

2. the mean *CDF* calculated considering the change remains below $10^{-5}$ per year.

c. If the interval between functional tests is extended, it shall be shown additionally that

1. the plant-specific failure rates of the associated components are not greater than the corresponding generic failure rates, and

2. the increase in the mean *CDF* does not exceed 1% when considering the requested change and assuming failure rates of the affected components increased by a factor corresponding to the extension of the test interval.

d. Even if the requirements of Chapter 6.3.3 are met, measures shall be identified and – to the extent appropriate – implemented in order to compensate for or to minimize the risk increase resulting from the plant modification.

## 6.4 Probabilistic evaluation of changes to structures and systems

a. The impact of modifications of PSA-relevant structures, systems and components on the risk shall be assessed.

b. A structural or system-related plant modification associated with a risk increase is admissible if

   1. the impact of the modification on the mean *CDF*, *FDF* and *LERF* is insignificant, and

   2. the calculated mean *CDF* considering the modification remains below $10^{-5}$ per year.

c. Even if the above mentioned requirements are met, measures shall be identified and – to the extent appropriate – implemented in order to compensate for or to minimize the risk increase resulting from to the plant modification.

## 6.5 Risk significance of components

a. The following criteria shall be used for the evaluation of the risk significance of components:

   1. A component is regarded as significant to safety from the PSA stand point if the following – in terms of the mean *CDF* or *FDF* or *LERF* – applies (selection criterion):

      $FV \geq 10^{-3}$ or $RAW \geq 2$

      The Fussell-Vesely (*FV*) and Risk Achievement Worth (*RAW*) importance measures for components shall be determined according to Annex 5.

   2. Components, which are regarded as significant to safety from the PSA stand point, shall be included in a list with the above mentioned importance measures. This list is an integral part of the operating documents.

b. The list shall be updated at the time of the PSR.

## 6.6 Probabilistic evaluation of operational experience

### 6.6.1 Annual evaluation of operational experience

a. The effects of PSA-relevant plant modifications carried out during the year considered shall be assessed as specified in Annex 2.

b. The following probabilistic safety indicators shall be determined and assessed as specified in Annex 3:

   1. The maximum annual risk peak ($CCDF_{i,\ max}$ )

   2. The incremental cumulative core damage probability ($IC_{um}CDP$)

c. The trend of these safety indicators shall be assessed.

d. The contribution to $IC_{um}CDP$ of latent errors (see Annex 3) detected during the year considered shall be reported and assessed.

e. The contributions to $IC_{um}CDP$ shall be reported in terms of the four categories of maintenance, repair, test and reactor trip. The maintenance contribution to $IC_{um}CDP$ shall be assessed in compliance with the criterion described in Chapter 6.3.2.

f. The dominant contributions to $IC_{um}CDP$ shall be identified and evaluated for both events and susceptibility to component or system failure.

g. If methodological changes are made in the PSA and have significant impact on the *CDF*, the probabilistic safety indicators (Annex 3) shall be updated retrospectively such that a current assessment of these indicators is available for a minimum of 5 calendar years.

h. The probabilistic evaluation of operational experience shall be documented in accordance with Annex 3.

### 6.6.2 Probabilistic rating of reportable events

a. Reportable events that affect PSA-relevant structures, systems, components or operator actions shall be evaluated by means of PSA.

b. The probabilistic rating of events shall be established as follows:

| $ICCDP_{Event}$ | INES |
|---|---|
| $1 > ICCDP_{Event} \geq 1 \cdot 10^{-2}$ | 3 |
| $1 \cdot 10^{-2} > ICCDP_{Event} \geq 1 \cdot 10^{-4}$ | 2 |
| $1 \cdot 10^{-4} > ICCDP_{Event} \geq 1 \cdot 10^{-6}$ | 1 |
| $1 \cdot 10^{-6} > ICCDP_{Event} \geq 1 \cdot 10^{-8}$ | 0 |

c. $ICCDP_{Event}$ shall be determined as specified in Annex 4.

# 7 List of references

K. Kim, D. I. Kang, and J.-E. Yang, On the use of the balancing method for calculating component RAW involving CCFs in SSC categorization, Reliability Engineering and System Safety, 2005, Vol. 87, pp. 233 – 242.

This guideline was approved by ENSI on 4 November 2015.

The Director General of ENSI: signed H. Wanner

# Annex 1: Terms and definitions (as per the ENSI Glossary)

**Baseline Core Damage Frequency (*$CDF_{Baseline}$*)**

The Baseline Core Damage Frequency (*$CDF_{Baseline}$*) is the *CDF* quantified by the zero maintenance model.

**Component unavailability configuration**

A component unavailability configuration is a state during power operation in which a constant set of components is unavailable.

**Conditional Core Damage Frequency (*CCDF*)**

The Conditional Core Damage Frequency (*CCDF*) is the *CDF* quantified for a specific component unavailability configuration.

**Incremental Conditional Core Damage Probability (*ICCDP*)**

The determination of the Incremental Conditional Core Damage Probability (*ICCDP*) is described in Annex 3 of the guideline ENSI-A06.

**Incremental Cumulative Core Damage Probability (*$IC_{um}CDP$*)**

The determination of the Incremental Cumulative Core Damage Probability (*$IC_{um}CDP$*) is described in Annex 3 of the guideline ENSI-A06.

**Zero maintenance model**

A zero maintenance model is a modified PSA model where all basic events representing mean component unavailabilities due to planned maintenance, repair, or tests are set to available.

# Annex 2: List of PSA-relevant plant modifications

The list of PSA-relevant plant modifications required in the Chapters 5 letter d and 6.6.1 letter a of this guideline shall be documented as follows:

| No. of modification request | Description of modification | Date of implementation | Incorporated in PSA model | Impact | | | |
|---|---|---|---|---|---|---|---|
| | | | | Comments | Quantitative estimate | | |
| | | | | | $\Delta CDF$ | $\Delta FDF$ | $\Delta LERF$ |
| | | | | | | | |
| | | | | | | | |
| Total effect of all plant modifications | | | | | | | |
| Percentage effect of plant modifications not incorporated in model | | | | | | | |

# Annex 3: Procedure for probabilistic evaluation of operational experience

## A3.1 Risk Measures for the annual evaluation of operational experience

This section describes the procedure for the determination of risk measures for the probabilistic evaluation of operational experience.

a. A so-called zero maintenance model shall be constructed and used based on the current plant-specific PSA model.

b. When calculating the duration of component unavailability, a distinction is made between the following three scenarios:

   1. In case of a component failure, the duration of the resulting component unavailability is the component maintenance down time, plus the unavailability duration resulting from latent failure. A latent failure is a failure that remains undiscovered until, e.g., the affected (standby) component is functionally tested. In cases where no exact time for the beginning of the unavailability can be determined, half of the time interval between the last functional test and the detection of the failure shall be assumed.

   2. In case of maintenance, the duration of maintenance (maintenance down time) shall be taken as the component unavailability duration.

   3. In case of a test during which the considered component is unavailable, the duration of the component unavailability is assumed to be the test duration.

c. The conditional core damage frequency of the *i*-th component unavailability configuration, during which one or more components are unavailable, is denoted in the following as $CCDF_i$ and shall be determined as follows:

   1. With an approximation or

   2. based on a more precise calculation, if the approximate method shows that the $CCDF_i$ of a component unavailability configuration for the year in question represents a relevant risk peak, or if the same component unavailability configuration occurs several times in a single year.

      In the latter case, a more accurate calculation shall be performed by re-quantifying the zero maintenance model setting the corresponding components in the model to unavailable.

d. The incremental conditional core damage probability $ICCDP_i$ of the *i*-th component unavailability configuration shall be estimated as follows:

$$ICCDP_i = (CCDF_i - CDF_{Baseline}) \cdot \frac{\Delta t_i}{8760 \ \ [\text{hours / year}]}$$

whereby $\Delta t_i$ is the duration of component unavailability configuration in hours and $CCDF_i$ is the conditional core damage frequency per calendar year.

e. The $ICCDP_j$ of the $j$-th reactor trip shall be estimated as follows: In the zero maintenance model, the corresponding initiating event shall be set to guaranteed occurred (true) and the other initiating events shall be set to guaranteed not occurred (false). In case of simultaneous component unavailabilities, the corresponding components shall be set to unavailable in the zero maintenance model.

f. The annual incremental cumulative core damage probability $ICumCDP$ is defined as follows:

$$ICumCDP = \sum_{i=1}^{m} ICCDP_i$$

$m$ is the number of all component unavailability configurations plus the number of all reactor trips that occurred during the calendar year.

### A3.2 Report on the probabilistic evaluation of operational experience

The report on the probabilistic evaluation of operating experience, which also comprises information on component unavailabilities, shall cover the following:

a. Documentation of the version of the PSA model used

b. Brief description and justification of any special modelling assumptions concerning human reliability analysis and/or Common Cause Failures (CCF)

c. Characteristics of the year under review (date and duration of outages, $CDF_{Baseline}$ used)

d. Representation (as per Annex 2) and evaluation of PSA-relevant plant modifications implemented during the year under review

e. Discussion of the annual evaluation of operational experience according to Chapter 6.6.1

   In order to do so

   1. the value of the two probabilistic safety indicators ($ICumCDP$ and $CCDF_{i,\,max}$) for at least the last 5 years,
   2. the contributions to $ICumCDP$, and
   3. the approximate evolution of the $CCDF$ as a function of time

shall be depicted graphically.

f. List of unavailable components including the designation of the unavailable component, a brief description of the cause of the component unavailability, its start time and duration

g. The following data in tabular form for each identified component unavailability configuration (this shall also be sent electronically to ENSI):

   1. Reference number for each component unavailability configuration
   2. Designation of the unavailable component(s)
   3. Brief description of component unavailability configuration
   4. Start of component unavailability configuration (date and time)
   5. End of component unavailability (date and time)
   6. Conditional core damage frequency of component unavailability configuration $i$ ($CCDF_i$)
   7. Incremental conditional core damage probability of component unavailability configuration or of reactor trip $i$ ($ICCDP_i$)
   8. Cause (select one of the four categories; repair, maintenance, test, reactor trip) for every $ICCDP_i$

   This data shall also be sent electronically to ENSI.

# Annex 4: Assessment of reportable events

The incremental conditional core damage probability $ICCDP_{Event}$ for the event to be evaluated shall be determined as follows:

a. If the event represents an unplanned component unavailability configuration, then the $ICCDP_{Event}$ is the sum of all $ICCDP_i$ of the $k$ unavailability configurations occurring during the unplanned unavailability configuration:

$$ICCDP_{Event} = \sum_{i=1}^{k} ICCDP_i$$

The consideration of the unavailability duration is limited to the calendar year.

b. Developments of the existing PSA model to realistically assess the event shall be justified.

c. Additional operator actions can be considered as long as they do not consist of repairs or similar activities (e.g. assembling of a disassembled component). The failure probability of an additional operator action shall be determined according to the guideline ENSI-A05. Alternatively, a failure probability of 0.1 can be used for simple switch actions when at least 30 minutes are available for diagnosis.

d. If the event consists of an initiating event modelled in the PSA, the $ICCDP_{Event}$ shall be quantified according to Annex 3 (A3.1 letter e).

e. If the event involves a component unavailability, then the potential impact on the frequency of initiating events and on the probability of CCF shall be considered.

# Annex 5: Determination of the risk measures of components

a. To determine the *FV* and *RAW* value of a component, all basic events assigned to the component in question in the current plant-specific PSA model shall be taken into account.

b. When determining the risk measures *FV* and *RAW*, it shall be taken into consideration that the unavailability of components may have an influence on the initiating event frequencies and on the probability of CCF. For the assessment of the impact of the CCF probability, e.g. the following approaches are acceptable:

   1. The FV/RAW value of the relevant CCF group is included as an additional basic event when calculating the FV/RAW value of components.

   2. Balancing Method according to K. Kim et al. (see Chapter 7)

c. It shall be shown that the number of components just failing to meet the selection criterion is small. In particular, for components just failing to meet the selection criterion according to Chapter 6.5, the risk measures *FV* and *RAW* shall be determined based on re-quantification of the entire PSA model.

d. If *FV* and *RAW* are not determined based on re-quantification of the entire PSA model, then the uncertainty in the computational approximation shall be discussed.

e. The *FV* and *RAW* values of a component based on *FDF* and *LERF* shall be determined in a similar way to those based on *CDF*.

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