SKI Report 2007:06

Research

Probabilistic Safety Goals

Phase 1 – Status and Experiences in Sweden and Finland

Jan-Erik Holmberg
Michael Knochenhauer

February 2007

ISSN 1104-1374
ISRN SKI-R-07/06-SE

SKI

SKI-PERSPEKTIV

Bakgrund
En probabilistisk säkerhetsanalys (PSA) för ett kärnkraftverk genererar både kvalitativa och kvantitativa resultat. Kvantitativa resultat presenteras typiskt som frekvensen för härdskada eller som frekvensen för oacceptabla radioaktiva utsläpp. För att kunna bedöma om resultaten från en PSA är acceptabla behövs kriterier för tolkning och värdering av resultaten. Acceptanskriterierna har normalt en dubbel funktion, d.v.s. de definierar en acceptabel säkerhetsnivå, men har också en bredare och mera generell roll som beslutskriterier.

SKI:s och rapportens syfte
I denna projektfas har syftet i första hand varit att ge en klar beskrivning av temat i sig, probabilistiska säkerhetsmåltal för kärnkraftverk, att beskriva termer och begrepp som används i definition och tillämpning av probabilistiska måltal, samt att beskriva status och erfarenheter i Finland och Sverige.

Resultat
Utgående från en serie intervjuer och en begränsad internationell överblick beskriver projektet de probabilistiska säkerhetsmåltalens historia och aktuella status i Sverige och Finland. Ett antal områden diskuteras mera i detalj, inklusive måltalens status mot bakgrund av att de har överskridits under delar av den tid de varit i bruk, strategier för hantering av överskridanden, och kopplingen mellan säkerhetsmåltal på olika nivåer, exempelvis härdskada respektive oacceptabla utsläpp. Projektets resultat kan användas som en plattform för kraftbolagens diskussioner om hur man skall definiera och använda säkerhetsmåltal, och kan också användas av myndigheter som en referens för riskinformerade aktiviteter. Projektresultaten kan också påverka krav på PSA, t.ex. rörande kvalitet, omfattning, detaljeringsnivå och dokumentation. Slutligen bedöms resultaten kunna vara av generellt intresse som ett stöd för pågående och planerade riskinformerade tillämpningar.

Eventuell fortsatt verksamhet inom området
Ett antal av de områden som identifierats som intressanta eller problematiska kommer studeras mera i detalj under nästa projektfas. Detta inkluderar användning av måltal i situationer när PSA-resultat varierar över tiden, kopplingen mellan probabilistiska och deterministiska beslutskriterier, och kriterier för oacceptabla utsläpp (PSA nivå 2), Dessutom kommer en fördjupad lägesbeskrivning att göras genom att utvidga den internationella överblicken och även studera användningen av måltal inom vissa andra industrigrenar.

Effekt på SKI:s verksamhet
Resultaten bidrar till ökad förståelse för användningen av probabilistiska måltal som besluts- och acceptanskriterier.

Projektinformation
SKI:s handläggare: Ralph Nyman
Diarienummer: SKI 2005/1061
Projektnummer: 2005 02 008

SKI PERSPECTIVE

Background

The outcome of a probabilistic safety assessment (PSA) for a nuclear power plant is a combination of qualitative and quantitative results. Quantitative results are typically presented as the Core Damage Frequency (CDF) and as the frequency of an unacceptable radioactive release. In order to judge the acceptability of PSA results, criteria for the interpretation of results and the assessment of their acceptability need to be defined. However, safety goals usually have a dual function, i.e., they define an acceptable safety level, but they also have a wider and more general use as decision criteria.

The aim of SKI and of the report

In this first phase of the project, the aim has been on providing a clear description of the issue of probabilistic safety goals for nuclear power plants, to define and describe important concepts related to the definition and application of safety goals, and to describe experiences in Finland and Sweden.

Results

Based on a series of interviews and on literature reviews as well as on a limited international over-view, the project has described the history and current status of safety goals in Sweden and Finland. A number of issues were discussed more in detail, including the status of the safety goals in view of the fact that they are often exceeded, strategies for handling violations of safety goals, and relation between safety goals defined on different levels, e.g., for core damage and for unacceptable release. The results from the project can be used as a platform for discussions at the utilities on how to define and use quantitative safety goals. The results can also be used by safety authorities as a reference for risk-informed regulation. The outcome can have an impact on the requirements on PSA, e.g., regarding quality, scope, level of detail, and documentation. Finally, the results can be expected to support on-going activities concerning risk-informed applications.

Possible continued activities within the area

A number of the issues identified as interesting or problematic will be studied more in detail in the next project phase. This includes consistency in the usage of safety goals, realtions between deterministic and probabilistic safety goals,a and criteria for unacceptable releases (level 2 PSA). In addition, the international overview will be extended, and safety goals in some other industries will be studied.

Effect on SKI activities

The project results are expected to increase the understanding of probabilistic target values as decision and acceptance criteria.

Project information

Project responsible at SKI: Ralph Nyman
Project number: SKI 2005/1061
Diary number: 2005 02 008

SKI Report 2007:06

Research

Probabilistic Safety Goals

Phase 1 – Status and Experiences in Sweden and Finland

Jan-Erik Holmberg
VTT, P.O.Box 1000, FI-02044 VTT, Finland

Michael Knochenhauer
Relcon Scandpower AB, 172 25 Sundbyberg, Sweden

February 2007

Sammanfattning

En probabilistisk säkerhetsanalys (PSA) för ett kärnkraftverk genererar både kvalitativa och kvantitativa resultat. Kvantitativa resultat presenteras typiskt som frekvensen för härdskada eller som frekvensen för oacceptabla radioaktiva utsläpp. För att kunna bedöma om resultaten från en PSA är acceptabla behövs kriterier för tolkning och värdering av resultaten. Ytterst skall dessa kriterier eller måltal definiera nivån för acceptabel risk från driften av ett kärnkraftverk. Acceptanskriterierna har dock normalt en dubbel funktion, d.v.s. de definierar en acceptabel säkerhetsnivå, men har också en bredare och mera generell roll som beslutskriterier. Den exakta nivån för dessa kriterier varierar mellan olika organisationer och länder. Det finns också skillnader i definitionen av måltalen och i deras formella status, d.v.s. om de är tvingande eller ej.

I denna projektfas har syftet i första hand varit att ge en klar beskrivning av temat i sig, probabilistiska säkerhetsmåltal för kärnkraftverk, att beskriva termer och begrepp som används i definition och tillämpning av probabilistiska måltal, samt att beskriva status och erfarenheter i Finland och Sverige.

Utgående från en serie intervjuer och en begränsad internationell överblick beskriver projektet de probabilistiska säkerhetsmåltalens historia och aktuella status i Sverige och Finland. Ett antal områden diskuteras mera i detalj, inklusive följande:

- Måltalens status mot bakgrund av det faktum att de har överskridits under stora delar av den tid de varit i bruk, liksom implikationer av dessa överskridanden.
- Säkerhetsmåltal som tvingande respektive vägledande kriterier.
- Strategier för hantering av överskridanden, inklusive graderade angreppssätt av typen ALARP (As Low As Reasonably Practicable).
- Kopplingen mellan säkerhetsmåltal på olika nivåer, exempelvis härdskada respektive oacceptabla utsläpp.

Ett antal av dessa områden kommer studeras mera i detalj under nästa projektfas.

Projektets resultat kan användas som en plattform för kraftbolagens diskussioner om hur man skall definiera och använda säkerhetsmåltal, och kan också användas av myndigheter som en referens för riskinformerade aktiviteter. Projektresultaten kan också påverka krav på PSA, t.ex. rörande kvalitet, omfattning, detaljeringsnivå och dokumentation. Slutligen bedöms resultaten kunna vara av generellt intresse som ett stöd för pågående och planerade riskinformerade tillämpningar.

Summary

The outcome of a probabilistic safety assessment (PSA) for a nuclear power plant is a combination of qualitative and quantitative results. Quantitative results are typically presented as the Core Damage Frequency (CDF) and as the frequency of an unacceptable radioactive release. In order to judge the acceptability of PSA results, criteria for the interpretation of results and the assessment of their acceptability need to be defined. Ultimately, the goals are intended to define an acceptable level of risk from the operation of a nuclear facility. However, safety goals usually have a dual function, i.e., they define an acceptable safety level, but they also have a wider and more general use as decision criteria. The exact levels of the safety goals differ between organisations and between different countries. There are also differences in the definition of the safety goal, and in the formal status of the goals, i.e., whether they are mandatory or not.

In this first phase of the project, the aim has been on providing a clear description of the issue of probabilistic safety goals for nuclear power plants, to define and describe important concepts related to the definition and application of safety goals, and to describe experiences in Finland and Sweden.

Based on a series of interviews and on literature reviews as well as on a limited international over-view, the project has described the history and current status of safety goals in Sweden and Finland, and elaborated on a number of issues, including the following:

- The status of the safety goals in view of the fact that they have been exceeded for much of the time they have been in use, as well as the possible implications of these exceedances.
- Safety goals as informal or mandatory limits.
- Strategies for handling violations of safety goals, including various graded approaches, such as ALARP (As Low As Reasonably Practicable).
- Relation between safety goals defined on different levels, e.g., for core damage and for unacceptable release.

A number of important issues have been identified for continued studies in the next project phase.

The results from the project can be used as a platform for discussions at the utilities on how to define and use quantitative safety goals. The results can also be used by safety authorities as a reference for risk-informed regulation. The outcome can have an impact on the requirements on PSA, e.g., regarding quality, scope, level of detail, and documentation. Finally, the results can be expected to support on-going activities concerning risk-informed applications.

Acknowledgements

We want to express our thanks to the many people who have participated in the interviews – they are all listed in Attachment 1. These interviews have accumulated a large body of information, and are the backbone of the project. We also thank the NKS (Nordic nuclear safety research) and the members of NPSAG (Nordic PSA Group) and SAFIR (The Finnish Research Programme on Nuclear Power Plant Safety 2003–2006) for financial support of the project as well as for other input to the project.

Table of contents

Tables

Figures

1 Introduction

1.1 Background

The outcome of a probabilistic safety assessment (PSA) for a nuclear power plant is a combination of qualitative and quantitative results. Quantitative results are typically presented as the Core Damage Frequency (CDF) and the frequency of an unacceptable radioactive release. The radioactive release is a more complex outcome, and usually important sub-categories are defined, e.g., the Large Early Release Frequency (LERF). In order to judge on the acceptability of PSA results, criteria for the interpretation of results and the assessment of their acceptability need to be defined.

Target values for PSA results, both for CDF and for radioactive releases, are in use in most countries having nuclear power plants. In some countries, the safety authorities define these target values or higher level safety goals. In other countries, they have been set only by the nuclear utilities. Ultimately, the goals are intended to define an acceptable level of risk from the operation of a nuclear facility. There are usually also important secondary objectives, such as providing a tool for identifying and ranking issues with safety impact, which includes both procedural and design related issues. Thus, safety goals usually have a dual function, i.e., they define an acceptable safety level, but they also have a wider and more general use as decision criteria. The exact levels of the safety goals differ between organisations and between different countries. There are also differences in the definitions of the safety goals, and in the formal status of the goals, i.e., whether or not they are mandatory.

Defining quantitative goals for reactor safety may have a large impact on both the analysis burden and on requirements for safety improvements at nuclear power plants. It is therefore of great importance that safety goals are soundly based, that they can be effectively and unambiguously applied, and that they can be accepted and understood by all parties concerned (nuclear utilities, decision makers, analysts, etc.).

The notion of risk acceptance appeared already in 1967 in a paper on siting criteria by F.R. Framer [Farmer_1967] where he outlined the concept of probabilistic safety assessment. He proposed a safety criterion based on the F-N curve. Subsequently, the reactor safety study [WASH-1400] and some pioneering PSA:s, e.g., [NUREG-1150] made comparisons of individual and societal risks from nuclear power plant with other industrial risks.

In most countries, safety goals started to be discussed and defined in the late 1980s [NUREG-0880, IAEA_INSAG-3]. At that time, PSA models were rather limited in scope, often consisting mainly of internal process events (transients and LOCA) during power operation. For various reasons, including limitations in analysis scope and capacity problems with the computer codes used for the analyses, the level of detail of the PSA models was also rather limited. In addition, the focus was on level 1 PSA, i.e., on calculation of CDF. Furthermore, the actual use of early PSA:s was generally rather limited, even if the issue of Living PSA (LPSA) received considerable attention during the 1980s.

During the 1990s, PSA models expanded considerably, both regarding operating states and classes of initiating events. The level of detail of the analyses also increased, especially regarding initiating events (definition of common cause initiator events, CCI), inclusion of functional dependencies (signals, power supply, control logics), and modelling of non-safety systems. In parallel, PSA:s were expanded to level 2, making it possible to calculate the frequency of radioactive releases.

Thus, the scope, level of detail and areas of use of PSA have changed considerably since the time the safety goals were originally defined. This is a change both in quality and in maturity of the PSA technique. At the same time, PSA applications are becoming more and more important. This has lead to an increased interest and need to make active use of PSA results, and thus to make judgments concerning the acceptability of risk contributions calculated with PSA.

1.2 Project aim and scope

The project has been financed jointly by NKS (Nordic Nuclear Safety Research), SKI (Swedish Nuclear Power Inspectorate) and the Swedish and Finnish nuclear utilities. The national financing went through NPSAG, the Nordic PSA Group (Swedish contributions) and SAFIR, the Finnish research programme on NPP safety (Finnish contributions).

The first phase of the project "The Validity of Safety Goals" was carried out mainly during 2006, and the phase 1 results are presented in this project report. The overall aim in this phase has been to discuss and document current views, mainly in Finland and Sweden, on the use of safety goals, including both benefits and problems. Another important aim has been to identify and clearly define the concepts involved in the definition, interpretation and use of safety goals.

The main objective has been to clarify the basis for the evolvement of safety goals for nuclear power plants in Sweden and Finland and to describe the experiences gained. This has been achieved by performing a rather extensive series of detailed interviews with people who are or have been involved in the formulation and application of the safety goals, putting the focus on the question of where the safety goals came from, what they are perceived to stand for, and how they are interpreted. The experiences from their use has also been discussed, as well as development needs. To provide further perspective, crucial references related to the formulation and use of safety goals have been identified and reviewed.

In addition, a limited review of the current status internationally has been performed by letting a number of people and organisations outside the Nordic countries answer a revised version of the questionnaire used for the Nordic interviews.

The results of this project phase was presented at a project seminar in Stockholm in November 2006 [SG_Semin_2006]. The project has also been presented at PSAM 8, an international conference on Probabilistic Safety and Management [PSAM8-0162].

The project report includes the following parts:

Chapter 1. Introduction and background
Aim and scope; Project context; Related previous Nordic activities.

Chapter 2. Background to safety goals
Concepts; Quantification of risk; Consequences; Risk criteria; Decision theory.

Chapter 3. The evolvement of safety goals
Historical review; Reasons for defining safety goals; Context of goals; Parties involved; Areas of application; Experiences with safety goals; Limited international overview.

Chapter 4. Specific issues
Discussion of status related to a number of important issues associated with the definition, interpretation and use of probabilistic safety goals.

Chapter 5. Conclusions
Conclusions, including a summary of planned activities for phase 2 of the project.

1.3 Previous Nordic research projects related to safety goals for nuclear power plants

The issue of safety goals has been discussed in several previous Nordic projects, especially within the NKS programme, i.e., the same framework within which the present project has been performed.

In the NKA[1] programme 1981–84, the project NKA/SÄK-1 "PRA uses and techniques" focused on method development of PSA (called PRA in that time) [NKA/SÄK-1]. The question of implementation of PSA safety goals in regulatory work was left open, since there was *little interest in the Nordic countries concerning the possible implementation of quantitative safety goals*. Using PSA results in a qualitative manner was preferred, because there were limited experience from the performance and use of PSA.

In the NKA programme 1985–89 [NKA_1989:91], several projects dealt with safety goals. The project NKA/RAS 490 "Principles for risk assessment and decision making" developed a scheme for decision making involving risk [NKA/RAS-490]. Cost-benefit evaluations were considered as a possible approach, but such a trade-off was recognised to be surrounded by controversy.

The project NKA/RAS 450 "Optimization of technical specifications by use probabilistic methods" developed methods and decision making criteria for comparison of alternative requirements in Technical Specifications [NKA_1990:33]. Various acceptance and optimisation criteria were discussed, but no formal cost-benefit ratio was addressed. The following procedure was recommended: 1) Quantitative demonstration of numerical acceptability with or without the use of a formal criterion; 2) Case-by-case decision based on weighing of quantitative results against qualitative boundary conditions.

The project NKA/RAS 470 "Dependencies, human interactions and uncertainties in probabilistic safety assessment" concentrated on limitations in PSA techniques

---

[1] NKA is the previous acronym of NKS

[NKA_1990:57]. One conclusion of the project was that intrinsic and practical limitations of PSA make the use of absolute probabilistic criteria in decision making difficult.

In the next NKS programme 1990–94, the project NKS/SIK-1 "Safety evaluation by living probabilistic safety assessment and safety indicators" developed the concept of living PSA [SKI_1994:2]. Risk criteria needed in different LPSA applications were presented. It was concluded, that probability based criteria could give guidance of first indication about the acceptability of decision alternatives, but that they alone are not sufficient in complex decision making situations [VTT Publ 146]. In the same project, multi-attribute decision analysis as a tool to support risk decision making was demonstrated [RiskAnal 94 983-991], and the decision analysis panel method was further demonstrated in two cases [STUK-YTO-TR 61].

The External Events[2] Programme (1994–97) of the Swedish utilities and the SKI included the project "Presentation and Interpretation of Results in the Probabilistic Analysis of External Events" [SKI_1997:49]. It was concluded, that many PSA applications presuppose the comparability of results, i.e., that relevant quantitative comparisons can be made between the various parts of the PSA (e.g. between the risks from transients and internal fires). This was perceived to be a problem, as most PSA analyses of area events were based on simplified models and on a mixture of conservative and non-conservative assumptions. The report discusses the prerequisites for comparability and provides an outline of two alternative methods for performing the comparison.

In 1994-97, NKS/RAK-1 "Strategies for Reactor Safety," explored strategies for safety management of NPP:s in Finland and Sweden [NKS(97)FR1]. Quantitative safety goals and other probabilistic decision criteria were discussed only implicitly.

In the next NKS programme, NKS/SOS (1998–2001), the project NKS/SOS-1 "Nuclear Safety in Perspective" aimed at enhancing the common understanding about requirements for nuclear safety by finding improved means of communicating the subject in society [NKS-60].

The project NKS/SOS-2 "Advances in Operational Safety and Severe Accident Research" performed studies related to uncertainty and incompleteness in PSA [NKS-61]. Various probabilistic criteria were reviewed and their use was discussed [NKS-44]. A decision analytic framework for evaluating the criteria was developed, and the different criteria were analysed with regard to their behaviour under incompleteness or uncertainty of the PSA model. Recommendations on the application of the criteria in different decision situations were given.

A comparison was made of the PSA:s for two nearly identical NPP:s, Forsmark 3 and Oskarshamn 3, both third generation ABB Atom BWR:s [NKS-36]. The results of the project indicated that PSA is not a robust method regarding absolute quantitative results, and that results and conclusions can vary a lot between different versions. Therefore a harmonisation of methods would be needed before reasonable comparison of results can be done. In consequence, the use of absolute risk criteria in decision making is problematic, since the scope and level of realism varies between studies.

---

[2] External events refer here to area events such as fires and floodings

2 Background to Safety Goals

2.1 Concepts

2.1.1 Probability and risk concepts

Probability expresses quantitatively the uncertainty related to an event. Mathematically, it is a measure that assigns a number [0,1] to a subset of a given set, and it follows the axioms of the probability theory. In practical application, the interpretation of a subset can be an event, so that the assigned probability represents the uncertainty of the event.

When using probabilities and probability models in decision making, it is important to agree with the interpretation of the probability. The two main interpretations are the *subjective* interpretation (also called *Bayesian*), and the *frequency* interpretation.

According to the frequency interpretation, the probability of an event is the relative frequency with which the event occurs in an infinitely long experiment. This means that the probabilities cannot be known exactly, since in practice there are no infinite series of experiments. However, the frequency interpretation makes it possible to estimate probabilities and to determine confidence bounds for unknown probabilities.

According to the subjective or Bayesian interpretation, probability is a rational degree of belief about the occurrence of an event. The probability depends on the information which the observer has about the occurrence of an event, which means that the assumed probabilities of different observers may be different. The Bayesian approach requires that all uncertainties are modelled with probabilistic concepts, and that the rules of probability calculus are followed in all inference.

The two interpretations of probability understand uncertainties differently. In the Bayesian approach, the probability is the measure of uncertainty, i.e., the uncertainty about the probability can be expressed by probability. This probability of probability, however, disappears when, e.g., finally assessing the uncertainty about an event. In the frequency approach, confidence bounds can be derived for the probability estimate. The confidence bounds cannot be compared with the Bayesian metaprobabilities, since they are answers to different questions.

Two types of uncertainties are distinguished: epistemic and aleatory. *Epistemic uncertainty* is attributable to incomplete knowledge about a phenomenon that affects our ability to model it. Acknowledging epistemic uncertainty would, e.g., mean that the probability of a failed component function can be said to be in certain range, without the possibility to specify it more in detail. Epistemic uncertainty may be reduced with time as more data is collected and more research is completed.

Aleatory uncertainty is caused by the nondeterministic (stochastic, random) nature of phenomena. Aleatory uncertainty is also called *variability*. Acknowledging aleatory uncertainty would, e.g., mean saying that the probability of a failed function of a generic component is p, but as conditions vary between specific components and contexts, the failure probability of a specific component is within a certain range. Aleatory uncertainty cannot be reduced by further study, as it expresses the inherent variability of a phenomenon.

Since most probability estimates include both aleatory and epistemic uncertainties, the range of estimates that would account for both factors will generally be broader than either range assessed separately.

Risk is defined relative to *hazards* or *accidents*. A hazard is something that presents a potential for health, economical or environmental *harm*. Risk associated with the hazard is a combination of the probability (or frequency) of the hazardous event and the magnitude of the consequences. The consequences can be represented in several dimensions.

A usual engineering definition of risk associated with an event i is:

Risk(event i) = "the probability of an event i" · "the consequences of an event i".

To assess the risk associated with a system (e.g. a nuclear power plant), integration over all accidental events associated with the system must be carried out.

In the classical approach to risk assessment, the probability $p = P(A)$ of the unwanted event A is understood in a frequentist sense. p is estimated by using a model linking p and some parameters q, $p = f(q)$. The parameters q can be estimated from data, thus yielding an estimator p^* of p, i.e., $p^* = f(q^*)$. With this approach, the only type of uncertainty that can be quantified is the statistical variation of q^* [RESS_61(1998)3].

In the Bayesian approach, a clear distinction is made between observable quantities (events) and unobservable model parameters, so that the model for the probability of A is $P(A) = g(q)$. Uncertainties are modelled explicitly using the Bayesian approach. The uncertainty of A is epistemic [RESS_75(2002)93].

The *individual risk* is the risk faced by any specific individual as a result of an accidental event. Typically, in risk analysis this is calculated for an anonymous person in the most exposed position. The *collective, group* or *societal risk* is the expected total risk in the population exposed to risk, often expressed as the number of casualties per unit time. Collective risk can be expressed by an *F-N curve*[3] (*The top right corner is associated with the high risk, and bottom left corner with the low risk.*

Figure 1), which demonstrates the relation between the collective risk from small and large accidents. In F-N space, the top right corner is associated with the high risk, and bottom left corner with the low risk. If F-N curves for two systems do not intercept, it can be stated which system has lower risk and which has higher. If the F-N curves intercept, a risk comparison cannot be made without a utility function which expresses how much weight is put on smaller vs. larger accidents (see further discussion in the next chapter).

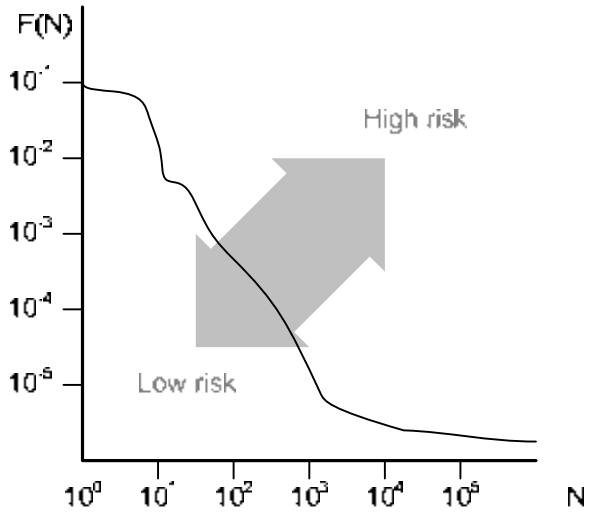
Risk measure and *risk metrics* are two concepts used in the presentation and interpretation of results from a risk assessment. The risk measure is an operation for assigning a number to something, and the risk metrics is our interpretation of the assigned number. In the PSA context, the various numeric results obtained from the quantification of the model are risk measures. The interpretations of these numbers as core damage risk, plant risk profile, safety margin, etc., are risk metrics.

Risk criteria refer to any quantitative decision making criterion used when results of risk assessment are applied to support decision making. Various types of criteria can be

---

[3] F-N = Frequency-Number of fatalities

used, such as: absolute criteria, relative criteria, differential criteria and trade-off criteria [RESS_36(1992)23]. Absolute criteria are discussed in the next chapter.



N = number of casualties, F(N) = the frequency of an accident with N or more casualties.

The top right corner is associated with the high risk, and bottom left corner with the low risk.

Figure 1. Hypothetical F-N curve of risk associated with a system in log-log scale.

2.1.2 Risk acceptance concepts

Risk is *acceptable* if it is tolerated by a person or group. Whether a risk is "acceptable" or not, will depend upon the advantages that the person or group perceives to be obtainable in return for taking the risk, whether they accept whatever scientific and other advice is offered about the magnitude of the risk, and numerous other factors, political, social, and psychological.

Risk acceptance is often presented using the ALARP[4] (As Low As Reasonably Practicable) framework. ALARP divides levels of risk into three regions:

1. Unacceptable (intolerable) region. Risk cannot be justified on any grounds.
2. The ALARP or tolerability region. Risk is tolerable if the benefit is desired. Trade-off analysis is made to evaluate the need for risk reductions.
3. Broadly acceptable region. Risk is negligible. No need for further risk reduction.

ALARP can be applied to a single risk metric. It can be also defined with an F-N curve. Figure 2 presents the risk acceptance criteria for major industrial accidents defined by the Dutch safety authority [VROM-1988].

$$F(N) = 10^{-3} \cdot N^{-2}.$$

[4] Somemetimes also referred to as ALARA (As Low As Reasonably Achievable), with the same meaning.

A *risk neutral* acceptance criterion has the form $k \cdot N^{-1}$, where k is a non-negative factor. Thus, the Dutch criterion for unacceptable risk has an added *aversion* to large accidents.

While the F-N curve represents a high level safety goal, the CDF and LERF criteria used for interpreting PSA results can be regarded as *surrogate* safety goals of the high level safety goals. By using surrogate safety goals, which are easier to address, the role and importance of individual safety barriers can be assessed.

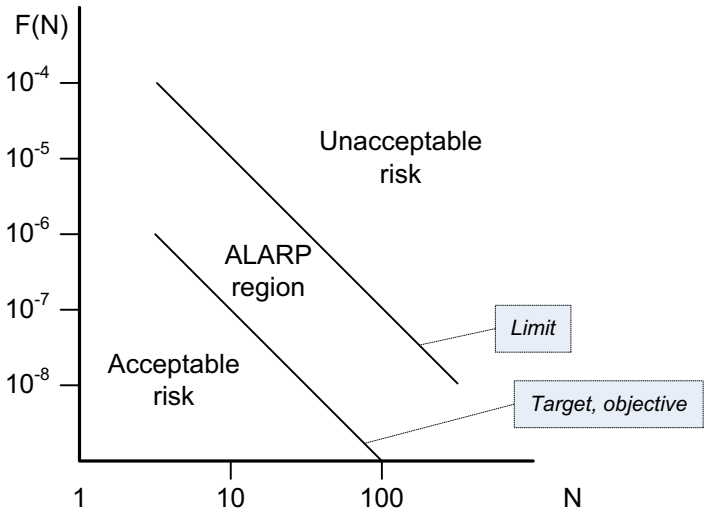


Figure 2. Societal risk curve with ALARP region as defined by VROM [VROM-1988].

Residual risk is the remaining risk which cannot be defined in more detail after elimination or inclusion of all conceivable quantified risks in a risk consideration. Reactor vessel rupture is often given as an example of a residual risk. Based on [WASH-1400], this has been interpreted to correspond to an event with a frequency of about 10^{-7} per year. The residual risk concept is applied in safety analysis as a screening criterion, e.g., as defined in [SKIFS 2004:2].

Safety objectives are the objectives to be achieved, e.g., for safe operation of nuclear power plants (see e.g. [IAEA_INSAG-12]). In the implementation of safety objectives, quantitative targets called (*quantitative*) *safety goals* or *numerical safety objectives* need to be defined.

Regarding safety goals, the terminology varies between different references and countries. For instance, EUR, the European utility requirements document for new light water reactors use the concepts "*safety targets*" and "*probabilistic design targets"* [EUR_2002]. EUR defines "targets" as values established by the utilities (e.g. related to the frequency of release of radioactivity), which are more demanding than current regulatory *limits*, but which are considered reasonably achievable by modern, well designed plants. On the other hand, the UK NII translates the risk acceptance criteria (limit of tolerability) into a *Basic Safety Limit* (BSL), which has the function of the upper bound of the ALARP region. The lower bound of the ALARP region is called *Basic Safety Objective* (BSO).

2.2 Decision theoretic background

In decision theory, decision making means comparison of alternatives using some rule. There is no theory providing a framework for rational collective decision making[5] under risk [NED_93(1986)319]. Nevertheless, decision theory provides a framework for characterising and comparing aspects of different approaches to risk decision making and use of safety goals.

Three types of approaches to risk decision making can be distinguished [NKS-44]. These are defined by the way deterministic analyses and risk analyses together address uncertainties and how the decision makers view the completeness and credibility of the related risk assessment.

1. An approach based on the theory of expected utility.
2. Value theoretic approach (risk-based).
3. Risk-informed approach.

These approaches are all described below. The two main points of view in nuclear risk decision making are also discussed, i.e., the investor's point of view and the regulator's point of view. In simplified terms, the investor makes comparison between risks and benefits of different investments, while the regulator makes comparison between risks (and perhaps benefits) of different risks in society.

2.2.1 The theory of expected utility

The first approach, and the normative way of risk decision making, is the subjective expected utility theory. According to the this theory, a decision maker is rational, when he/she chooses the decision option, which maximises the expected utility [French_1986]. This requires that the decision maker is in a position to formulate all the criteria explicitly and to measure the outcomes of different decision options with respect to these.

The risk model completely represents the best state of knowledge, and deterministic models and analyses have a supporting role only in defining the risk model. Insights obtained from these are redundant or embedded in the risk model. In this approach, all uncertainties are expressed as subjective probabilities (see Figure 3).

Risk acceptance criteria play no role in the expected utility framework. A risk, i.e., a decision option involving a risk, is accepted if it is better than the alternatives. The expected utility of the alternatives determines the acceptance.

---

[5] Collective decision making involves multiple decision makers

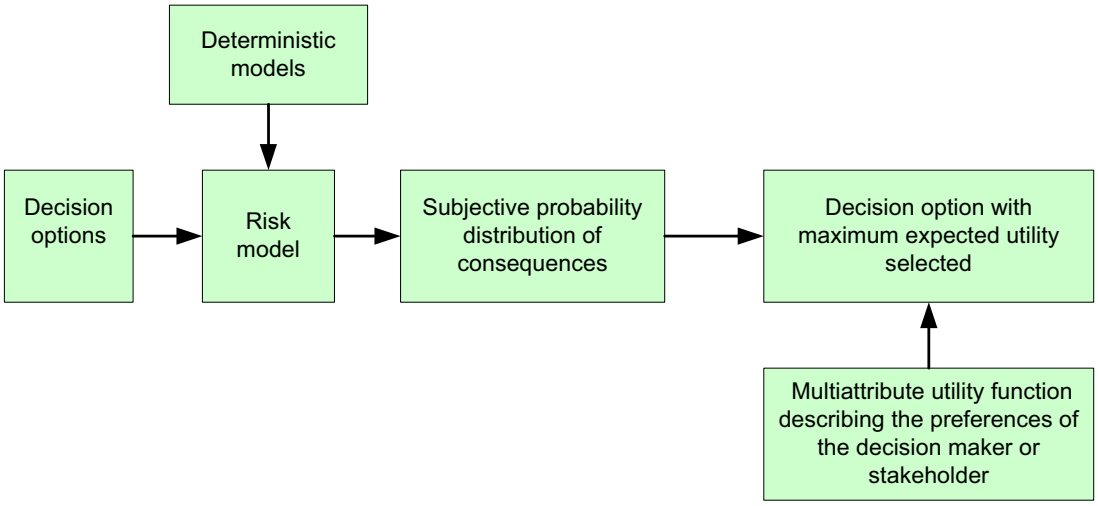


Figure 3. A utility theoretic approach to risk assessment and decision making.

The applicability of the theory of expected utility as a practical guideline in decision making under risk can be questioned for several reasons. The theory supposes that possible outcomes and associated probabilities can be fully assessed, which is a very hard requirement for real world cases. Both the assessment of outcomes and of probabilities are demanding exercises. Secondly, real world cases are usually diffuse and complex, so that any model only reflects a small piece of the decision making problem. Thirdly, the points of view of multiple stakeholders should be accounted for. If stakeholders do not agree on the probabilities and outcomes, the problem is outside of the theory of expected utility. Finally, in practical decision making, people do not behave according to the axioms of the theory [Kahneman-Tversky]. These situations deal more with decision making under *uncertainty*, where the probabilities of outcomes are not well explicated.

2.2.2 Risk-based approach using value theory

The second approach to risk assessment is based on the use of value theory [Fishburn_1970]. The risk model yields probabilities of defined adversarial consequences. The decision maker expresses his/her preferences in the form of a value function aggregating the different attributes, which are now the probabilities and the corresponding consequences. The decision option with the maximum value is selected.

In this approach, deterministic models have a double role; in addition to supporting the definition of the risk model, they provide evidence related to deterministic decision criteria, as shown in Figure 4. The deterministic decision criteria may be incorporated into the value model, and it is possible to make trade-offs between the different criteria. The deterministic criteria are typically related to design and/or safety principles, etc., which are models in themselves. The deterministic analyses guide the development of the risk assessment which, in turn, completes the insights obtained from the deterministic analyses.

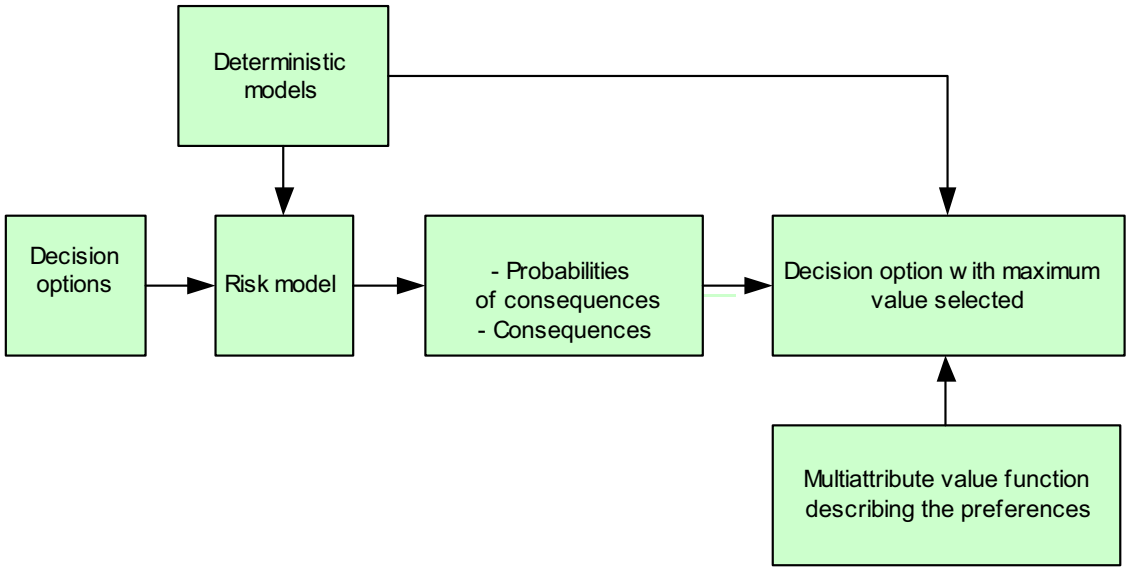


Figure 4. A value theoretic approach to risk assessment and decision making.

It should be noted that known probabilities, e.g., CDF and LERF, are possible to treat as decision criteria in the approach. It is therefore possible to interpret e.g. the ALARP-principle and risk-based decision making from this perspective. Acceptable risk can be used as a boundary condition of the value function.

2.2.3 Risk-informed approach

The third approach to risk assessment is risk informed decision making, which is more informal compared to the previous approaches. It admits a very complex decision context, and only some of its aspects can be described with deterministic and probabilistic models. The risk analysis yields the probabilities of consequences, but the uncertainties are significant, which means there is a need for the stakeholders to establish among themselves a shared understanding of the risk assessment results.

The decision rule(s) and criteria are determined for each case separately, and the values and preferences of the decision maker(s) are informally linked to the risk assessment. Decision panels or other group decision approaches are utilised (Figure 5).

It is important to note that the stakeholders and the decision maker(s) search for evidence consolidating their personal confidence regarding the risk assessment scope and the risk analysis method. Completeness and credibility are important attributes in this process. This informal approach to risk assessment corresponds to the risk informed decision making process.

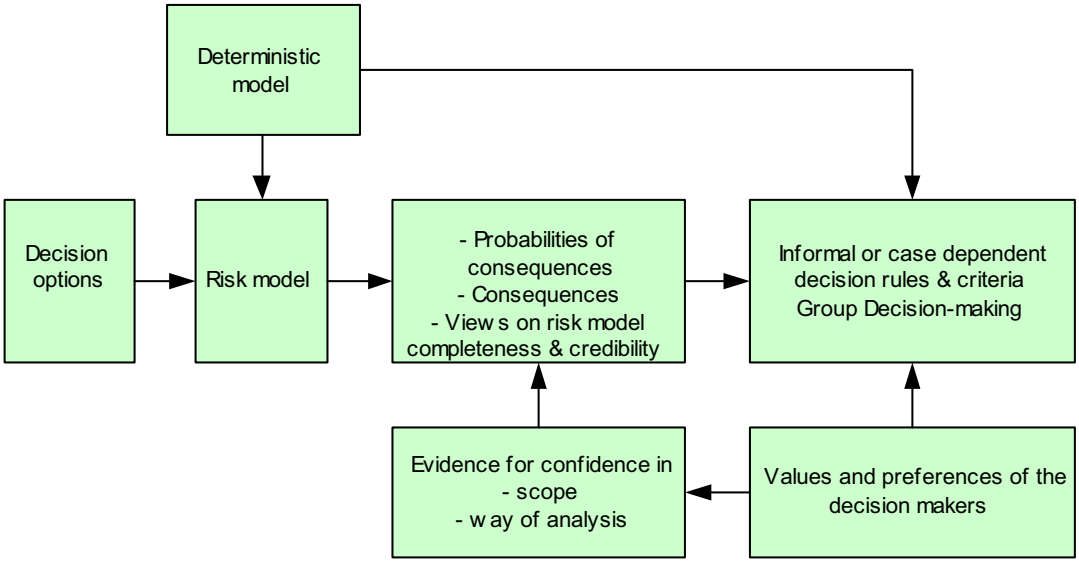


Figure 5. An informal approach to risk assessment and decision making.

2.2.4 Risk decision making as an investment problem

In an investment decision making situation, the following elements need to be assessed and explicated:

- benefits of the intended enterprise (e.g. operation of a nuclear power plant) in monetary terms
- risks (costs and probabilities) associated with the enterprise
- comparison of investor's preferences over different types of investments.

If the investment is accepted, a boundary for the level of acceptable risk can be calculated. The alternative is not to make the investment. In the case of an operating plant, the ultimate alternative for judging the level of acceptable risk is the terminal plant shutdown.

The acceptable risk is specific to the decision making situation. It varies between different plants, it is different for a new plant compared to an operating plant, and it changes during the lifetime of the plant.

2.2.5 Risk decision making from the regulatory perspective

The regulator's perspective is to supervise and regulate all risks to human beings and environment. The decision making on acceptable risk is culminated in the licensing process. A nuclear power plant is a source of risk among other industrial risks. The regulator would like to see a demonstration that the risk from a nuclear power plant is small enough compared to other technological risks. This is the idea of, e.g., the safety goals defined by the U.S.NRC.

To apply the comparative risk acceptance principle, the following tasks should be carried out:

- comparison and valuation of risks in society to be used as reference
- justification of results and conclusions of the risk assessment.

Accident statistics exist for the determination of the overall risk level for human beings. The assessment of different risks is a more complex issue since, many factors affect people's risk perception.

When considering risk from a nuclear power plant, this risk cannot be directly compared to any other man-made risk. However, appropriate references could be risks from other industrial facilities and other cancer-related risks. The assessment of an acceptable risk level can, thus, be a many faceted decision making situation:

- it is a political problem in the sense that society should decide what kind of risks are accepted and carry the responsibility of this decision;
- it is a juridical problem in the sense that the legal role of a safety goal needs to be clarified;
- it is a research problem in the sense that objective knowledge needs to be gained about various risks in society;
- it is a systems engineering problem first to design a plant that fulfils the requirement, and then to demonstrate the fulfilment of the requirement.

2.3 Context of safety goals

There are different reasons for defining safety goals, and the reasons may differ between different types of organisations. One aim may be to provide a tool to control the risk posed to society by the operation of nuclear power plants by defining a maximum acceptable risk. This risk may be related to the population potentially exposed to the risk, but may also be related to some other entities, e.g., land contamination. When relating calculated risks to such a safety goal it can in principle be used in an absolute manner giving the answer 'Yes' or 'No' to the question of whether the risk is acceptable or not.

In other cases the focus is more on using the safety goal as part of a decision criterion. Here, the safety goal constitutes a reference level and the key issue in the analysis is the relative deviation from the absolute level, or the degree of change relative to the results for other plant configurations or designs.

The actual definition of a safety goal involves two elements, the definition of the risk metric and of the maximum frequency allowed in terms of the risk metric chosen. The frequency part is quite simple (but not necessarily uncontroversial), and is done by stating one or more frequency levels, e.g., 10^{-5} per year. The process used to derive the frequency may be more or less complex and sometimes relates to higher level safety goals, e.g., to overall safety goals on a national level.

The definition of the risk metrics can be a more complex activity, as it should be possible to relate the risk metrics to the degree of harm experienced by the population exposed to the risk (or other risk metrics). As an example, there is no simple connection of this kind between the core damage frequency for a nuclear power plant and the degree of risk experienced by the public. For level 2 PSA criteria (radioactive release),

the connection is more evident, but not necessarily straight-forward and easily interpreted. In contrast, safety goals for other man-made risks are often expressed in terms of frequency and number of fatalities (F-N curves), which usually provides safety goals which are easier both to interpret and to apply. The F-N curve approach may also be chosen for criteria related to the results of a level 3 PSA.

A related question is the definition of the *target PSA* of the safety goal, which needs to be precisely stated in order not to create ambiguity in the application of the goal. The target PSA is the probabilistic plant model and calculation procedure that are used in order to calculate the risk level which is to be compared to the safety goal. Thus, the scope of the analysis leading up to the quantitative assessment of the risk measure needs to be clearly stated. Basically the precise and unambiguous definition of the target PSA should be part of the statement of the safety goal.

Once a safety goal has been defined, there is a need for an accepted procedure for carrying out the quantitative risk assessment, for applying the goal to the relevant risk measure, and for acting on the outcome of the application. In this context a number of issues must be considered. The basic outcomes are either that the safety goal is fulfilled, or that the plant is found not to meet the safety goal. In case of exceedance of the safety goal, there is a need for a procedure for handling the deviation and for assessing the severity of the deviation.

Thus, there is a need for defining how to decide that a safety goal has been met, i.e., criteria for accepting a calculated risk. Among other things, it needs to be stated whether it is the mean value of the calculated risk metric that shall meet the goal or if the comparison with the safety goal shall be done for some percentile in the uncertainty distribution of the result.

If, on the other hand, the outcome is that the safety goal is exceeded, there is a need for procedures to handle the deviation. Usually the simple answer “acceptable” or “not acceptable” is not sufficient, and there is often a need for a graded approach, which considers the extent to which the calculated risk deviates from the safety goal.

An important question in cases where the safety evaluation of an activity is more or less continuous, as is the case with the PSA for a NPP, is the consistency of risk judgments over time. Safety goals are typically quite stable, while PSA results may vary considerably over time. This may be due to changes in the actual plant (system redesigns, procedure changes, etc.). However, there is typically also a large impact from changes in the scope of the PSA or from changes in analysis methods or data used.

3 The Evolvement of Safety Goals

3.1 Introduction

This chapter summarises the various probabilistic safety goals defined for nuclear power plants in Finland and Sweden, and also includes a more general PSA related background. It presents the history of the evolvement of safety goals, as well as views and experiences from their usage. The contents of this chapter is to a large extent based on interviews with some of the people who were involved in the definition of the safety goals, or who have had reason to apply the goals in various situations. Much of the information also comes from the background documents referenced in the interviews. The people interviewed are listed in Attachment 1, which also presents the interview questions used.

Table 1 provides an overview of PSA related activities in Sweden and Finland from around 1975 until today.

Table 1. Overview of PSA activities in Sweden and Finland from 1975 until today.

Phase	Activities Sweden	Activities Finland
1975 - 1980	• Government Energy Commission • Reactor Safety Investigation • Comparison with WASH-1400	• Application of WASH-1400 to Loviisa (limited level 2 PSA) • Reliability analyses of safety systems
1980 - 1985	• PSA level 1, internal events • NKA/SÄK Nordic Research Program • Data collection and evaluation (T-book etc.) • Development of computer tools for PSA	• Initiation of PSA programmes
1985 - 1990	• Severe accident mitigation • Initial level 2 PSA:s • PSA for area events • SUPER-ASAR comparative PSA review • NKA/RAS Nordic Research Program	• First YVL-2.8 PSA guide from STUK • Basic level 1 PSA:s completed • STUK's requirement on severe accident mitigation at operating units
1990 - 1995	• Completeness of existing PSA models • Common Cause Initiators (CCI) • PSA level 2 • PSA for shutdown period • NKS/SIK Nordic Research Program • APRI – Research on severe accident phenomena	• Council of State decision 395/1991 • Use of PSA for safety improvements • PSA for area events / external events • PSA for shutdown period • Living PSA and PSA applications
1995 -	• PSA for external events • Living PSA and PSA applications • Quality assurance of PSA:s • SKIFS 1998:1 / 2004:1 (Safety in Nuclear Facilities) • Risk-informed applications • NKS/RAK Nordic Research Program • NKS-R Nordic Research Program	• PSA level 2 • YVL 2.8 guide updated 1996/2003 • Design phase PSA for Olkiluoto 3 • Risk-informed applications

In the 1970s, a few limited PSA:s were made inspired by WASH-1400. The plant-specific PSA programmes were initiated in the 1980s. During this decade, methods and

PSA codes were developed and systematic reliability data collection was initiated. In the 1990s and up to today, PSA:s have been complemented with missing parts and living PSA applications have been tried out. During the past decade, significant plant modifications, involving safety improvements, power up-rates and modernisation of I&C systems, have taken place in the plants. PSA has been used in the planning of these modifications as well as in the licensing context.

3.2 History of PSA safety goals in Finland

The possibilities of using probabilistic methods in nuclear safety management were recognized by the Finnish authorities and licensees in the early 1970s while the Loviisa and Olkiluoto NPP:s were under construction. The first PSA projects were initiated for both the plants in the early 1980s and the first level 1 PSA:s, including analysis of internal initiating events, were submitted to STUK in 1989.

In the 1990s, the PSA:s were complemented with analyses of area events, low power and shutdown operating modes, external events and level 2 PSA. Also the use of PSA in different applications started. Now, PSA:s are part of risk-informed regulation and safety management.

A special aspect in the Finnish history of PSA and safety goals is the long lasting planning of the fifth unit. The STUK's regulatory guide on PSA, YVL2.8, first issued in 1987, was formulated from the very beginning to be used in the licensing of a new NPP. Since the mid 1980s, several NPP concept candidates have been analysed using PSA, keeping not only the STUK's numerical objectives in mind, but also other guides, such as the European Utility Requirements [EUR_2002]. The Olkiluoto 3 NPP, which is now under construction, is the only Finnish plant that has gone through a regulatory review including the comparison with quantitative probabilistic limits.

3.2.1 Radiation and Nuclear Safety Authority of Finland (STUK)

3.2.1.1 Nuclear regulation in Finland

Nuclear regulation in Finland is set forth in the Nuclear Energy Act [YE-laki 990/1987] and the nuclear decree [YE-asetus 161/1988]. The nuclear law and decree are rather detailed and define some fundamental issues connected to the licensing process and to nuclear safety. The Decision of the Council of State [VnP 395/1991] gives the second level of nuclear regulatory requirements as applied in Finland. More detailed requirements, i.e., the YVL guides, are issued by STUK according to Nuclear Energy Act 55 § and VNp 990/1991 29 § [YVL-review].

The YVL guides form the actual regulatory system, although they in principle are on a lower level (less prescriptive) than the decisions of STUK. YVL guides are not legally binding, but constitute advisory rules for the licensees. The regulatory system allows deviations from the requirements of the YVL guides, provided the licence holder presents an acceptable solution by which the safety level given in the YVL guides is attained.

The YVL guides as such apply to new nuclear facilities. Upon revision of an old guide when a new guide is issued, the licensees send to STUK a statement, how the requirements of the new guide are to be applied on the installation. STUK then makes a

separate decision regarding the application to existing installations. The publication of a YVL guide does not necessarily alter any decisions made by STUK prior to the publication.

The nuclear energy act and decrees gives STUK the mandate to define and supervise the safety requirements of the nuclear installations. In Finland this is done through the regulatory system and not in individual plant licensing conditions. In addition STUK can issue letters (decisions) to the licence holder if a plant inspection or some other cause reveals findings that require corrective actions. Letters may also list new requirements to implement or actions that the licence holder must conduct within a specified time. As an example, requirements on PSA activities for operating plants are mostly stated in letters. According to VNp 395/1991, 27 §, actions for further safety safety enhancement shall be taken which can be regarded as justified considering operating experience and the results of safety research as well as the advancement of science and technology.

3.2.1.2 History of safety goals

In the late 1980s, the plan to build a new plant caused a need to develop regulatory guides for licensing a new NPP. The first version of the regulatory guide for PSA, Guide YVL 2.8 was issued in 1987 [STUK_YVL-2.8-1987]. In this issue, performance of a so called mini-PSA was required for the construction permit, and numerical design objectives were defined for important safety functions. The idea of using safety function level criteria was STUK's own innovation. At this time, the PSA methodology was not regarded as mature enough for use of CDF- and LERF-level criteria.

The mini-PSA required for a construction permit was a level 1 PSA including the most important initiating events. For an operating license, a complete level 1 PSA and a concise level 2 PSA were required.

The YVL 2.8 was revised in 1996, e.g., by extending the requirements on the use of PSA to further applications [STUK_YVL-2.8-1996]. A design phase PSA was required for a construction license. The contents of the design phase PSA was defined in more detailed compared to the mini PSA defined in the 1987 guide. Regarding PSA safety goals, numerical design objectives were now also defined for the core damage frequency and the frequency of a large radioactive release. The numerical objectives 10^{-5} per year for core damage and $5 \cdot 10^{-7}$ per year for release were derived by comparing results from existing PSA:s in the 1980s and early 1990s and criteria presented in international guidelines, above all the IAEA INSAG-3 [IAEA_INSAG-3].

The CDF criterion 10^{-5} per year was considered a challenging but possible objective for a new NPP. The release criterion $5 \cdot 10^{-7}$ per year corresponds to a conditional probability of 0,05 for a containment failure. The limit for a severe accident, 100 TBq release of Cs-137, was defined in a Decision of the Council of State [VnP 395/1991] in 1991. It was taken from Swedish studies performed in the context of designing filtered venting systems in the 1980s [SKI_SSI_1985], further described in Chapter 3.3.2.2. The limit of 100 TBq corresponds to a small release, which makes the level 2 PSA objective very tight. In this way the probabilistic criterion is in line with the stringent deterministic criteria.

The present version of YVL 2.8 was issued in 2003 [STUK_YVL-2.8]. It extended further the area of PSA applications and former optional applications were made mandatory. Regarding numerical design objectives, safety function level objectives

were removed from the guide. The reason for this was, that safety functions presumed the reactor type to be of certain kind, which could make the guide inapplicable for other conceivable reactor types.

Table 2 summarises the numerical design objectives defined in different versions of guide YVL 2.8.

Table 2. Numerical design objectives defined in different versions of STUK's PSA guide YVL-2.8

Version	Numerical design objective
1987	The unreliability of the most important safety functions is required to be below the following design objectives, with a confidence of at least 90 %: Safety function — Failure probability per demand • Reactor scram — 10^{-5} • Isolation of the containment — $5 \cdot 10^{-3}$ • Supply of feedwater when off-site power is lost and the main feed water system has failed — 10^{-4} • Operation of emergency core cooling, including long term recirculation in the case of a small LOCA — 10^{-4} • Reactor depressurisation together with long-term cooling of condensation pool (BWR) — 10^{-4}
1996	The mean unreliability of the most important safety functions shall be smaller than the following design objectives: Safety function — Failure probability per demand • Reactor scram — 10^{-5} • Supply of feedwater to steam generators (PWR) or to the reactor vessel (BWR) — 10^{-4} • Operation of emergency core cooling in the case of a small LOCA — 10^{-4} • Isolation of the containment — 10^{-3} The mean value of the probability of core damage is less than 10^{-5} per year. The mean value of the probability of a release exceeding the target value defined in section 12 of the Council of State Decision (359/1991)[1] must be smaller than $5 \cdot 10^{-7}$ per year. However, the containment has to be designed in such a way that its integrity is maintained with a high likelihood in case of both low and high pressure core damage.
2003	The mean value of the probability of core damage is less than 10^{-5} per year. The mean value of the probability of a release exceeding the target value defined in section12 of the Government Resolution (359/1991) [1] must be smaller than $5 \cdot 10^{-5}$ per year.

[1] Section 12 of the Government Resolution (359/1991) [VnP 395/1991]. Limit for a severe accident: The limit for the release of radioactive materials arising from a severe accident is a release which causes neither acute harmful health effects to the population in the vicinity of the nuclear power plant nor any long-term restrictions on the use of extensive areas of land and water. For satisfying the requirement applied to long-term effects, the limit for an atmospheric release of Cs-137 is 100 TBq. The combined fall-out consisting of nuclides other than caesium isotopes shall not cause, in the long term, starting three months from the accident, a hazard greater than would arise from a caesium release corresponding to the above-mentioned limit.

In addition to the above numerical objectives, the regulatory guide requires a balanced risk profile: *The risks associated with various initiators and accident sequences, taking into account their uncertainties, shall be compared with the numerical safety objectives*

and with each other in order to ensure that no single or few prevailing risk factors will stay at the plant. Particularly, such phenomena whose frequency of occurrence and consequences include large uncertainties shall be carefully examined. These are for example exceptional weather conditions, other possible harsh environmental conditions and seismic events. This paragraph has been used in Olkiluoto 3 licensing context.

According to STUK's decision on the application of Guide YVL 2.8, the numerical objectives are not applied to the operating plants. However, the principle of further safety enhancement is applied.

3.2.2 Teollisuuden Voima Oy (TVO)/Olkiluoto NPP

TVO operates two identical boiling water reactor units of ASEA Atom design, Olkiluoto 1 and 2 and is constructing Olkiluoto 3, a new pressurised water reactor of Areva design.

TVO started development of numerical criteria while developing PSA applications in the early 1990s. The first applications were planning of preventive maintenance during power operation, optimisation of allowed outage times, and test interval optimisation. The criteria were based on results from PSA, numerical objectives defined in YVL-2.8 and the U.S.NRC's regulatory guides 1.174-1.178 [RG_1.174, RG_1.175, RG_1.176, RG_1.177, and RG_1.178]. They are formulated in an internal PSA guide [TVO-PSA-ohje].

According to the PSA guide, a permanent design change is not allowed to increase the core damage frequency or frequency for unacceptable radioactive release by more than 1% of the target value. Target values are the same as in YVL 2.8 (10^{-5} per year, $5 \cdot 10^{-7}$ per year). A higher risk increase must be justified. Temporary work (done only once in plant lifetime) may not cause more than a 40% risk increase compared to the annual target value. The 40% criterion relates to the planned lifetime for the plant, i.e., 40 years.

For temporary exemptions from Technical Specifications, STUK requires a PSA evaluation. In this case as well, TVO applies the 1% risk increase criterion, as well as the requirement, that higher risk increases must be justified.

TVO's PSA guide has been sent to STUK for notification. STUK has not formally approved the criteria, and each PSA application is evaluated separately by STUK.

Regarding objectives for core damage frequency and LERF, the numerical objectives defined in YVL-2.8 are desired but not mandatory targets for the operating units OL1/OL2. Currently (2006), the CDF calculated by PSA is $1{,}5 \cdot 10^{-5}$ per year. For OL3, the numerical objectives defined in YVL-2.8 are mandatory.

3.2.3 Fortum/Loviisa NPP

Fortum operates two identical Russian type (VVER) pressurised water reactor units, Loviisa 1 and 2.

In Loviisa NPP, PSA has been used in decision making on plant modifications since 1989 when the basic level 1 PSA was completed. The first results showed high core damage frequency, which lead to several safety improvements. PSA was used in the prioritisation of changes and comparison of alternatives. In this decision making,

criteria are needed and therefore goals were developed. The aim has been to have realistic goals. Comparisons have been made with goals defined in other countries and with risks accepted by the society in other activities. US references were used mostly, since the USA has the longest history in the nuclear field.

Numeric PSA goals are formulated in a bulletin, which is not part of an official instruction procedure. The goal regarding core damage frequency is 10^{-4} per year and regarding frequency of large release 10^{-5} per year. Loviisa has so far always been above these goal numbers, but the CDF is now below 10^{-4} per year [CM-06-Fortum]. Significant plant improvements have been made during the last decades to decrease the risk level of the plant.

Loviisa has also developed economic criteria for justification of safety improvements [NED_185(1998)335, Vaurio_NKS-99]. These criteria could be used also for justification of plant modifications that can increase core damage risk. In practice, compensating measures are often applied, especially since the CDF has not been below the limit 10^{-4} per year until now. Criteria have been defined based on an estimation of the monetary value of core damage and large release. In the mid 1990s, the value in level 1 PSA was 200 kFIM equal to $\Delta CDF = 10^{-6}$ per year[6]. In level 2 PSA, the price was 30 times higher.

3.2.4 Finnish experience

The overall Finnish experience on the use of PSA safety goals is positive. Attention is paid to the comparison of numerical results. Safety goals also affect the quality of PSA by requiring more detailed modelling of some issues. Conservative assumptions need to be avoided since they do not only make the numbers look too bad but most importantly, can misdirect resources to areas that may not be as important as others. Safety goals thus are an incentive to make better analyses.

There is a common view regarding the definitions for core damage and large release. Core damage is defined as local fuel temperature above 1204 ºC and large release as an atmospheric release of more than 100 TBq of Cs-137, as defined in [VnP 395/1991]. It is also a common understanding that a full scope PSA should be used in the comparison with safety goals.

For old plants, the safety goals defined by the utilities are unofficial targets, and set an ambitious goal for safety improvements. Safety goals also mean that plant changes and exemptions from licensing conditions need to be assessed numerically. PSA and PSA criteria have become well-known in the organisations.

The probabilistic criteria applied to operating plants are not strict, which allows more flexible handling of risk. An open question is how old plants will be treated in the regulatory decision making in the future. Application principles may change, which may cause uncertainty among licensees.

Making plant improvements promptly based on the most current PSA has satisfied authorities and so allowed the utility to proceed in a self-controlled manner. In some cases PSA has helped to avoid unnecessary changes suggested on a deterministic basis.

---

6 200 kFIM corresponds to about 35 kEUR/kUSD.

PSA has gained acceptance, although in some cases a later PSA update has shown that earlier modifications were not quite enough or optimal. Whenever PSA is complemented and updated, the risk profile will change, which can weaken trust in PSA.

Concerning needs for improvements, the most discussed issue in Finland is the definition for a large release, which is currently considered to be very stringent in the PSA context. The current release limit was originally defined as a deterministic requirement to be used in the design of severe accident management strategy and systems. The performance of level 3 PSA could be needed to judge the feasibility of the 100 TBq limit. On the other hand, an update of the Government Resolution (359/1991) is ongoing. The caesium release based definition is not considered to be fully logical in the present form, and could be improved in order to enhance the communication.

3.3 History of PSA safety goals in Sweden

3.3.1 Overview of early PSA activities in Sweden

The PSA status report [SKI_1996:40] describes in detail the development of PSA in Sweden up to the mid-90s; an extract from the report is presented below.

After the Three Mile Island accident (TMI), the Reactor Safety Investigation (RSU, Reaktorsäkerhetsstudien) [SOU 1979:86] was initiated in 1979, with the aim to

- consider if there was reason to change the general assessment of the level of safety in the production of electrical energy in nuclear power plants, and
- propose possible safety enhancing measures in Swedish nuclear power plants, as well as indicate the need of research concerning such measures.

The RSU showed that there was no reason to change the conclusions from previous assessments of the level of safety in nuclear power plants. However, it was stressed that both previous risk assessments and the TMI accident indicate the need for considerably increased requirements on safety activities in connection with nuclear power. These requirements should apply to all parts of nuclear activities, from the design of the plants and their safety systems, through the activities of the supervising authorities, and to the day-to-day safety work at the nuclear power plants.

The RSU also stressed the need to properly evaluate experiences from disturbances and incidents occurring during plant operation and outages in order to prevent accidents. It was also stressed, that there is always a risk for future accidents. Therefore, the RSU recommended that more attention should be given to measures aimed at mitigating the consequences from such accidents. This recommendation was later to result in considerable research efforts in connection with accident mitigating systems, and ultimately resulted in the design and installation of filtered venting systems in all Swedish nuclear power plants.

In 1981, following the recommendations of the RSU, the Swedish Parliament ruled, that every nuclear power plant should be made subject to at least three complete safety reviews during its useful life. These ASAR (As-operated Safety Analysis Report) were to be submitted every 8–10 years by SKI, and compiled on the basis of analyses carried

out by the utilities. The ASAR guidelines issued by SKI for the first and second ASAR:s included requirements on performance PSA:s, first on level 1 [SKI_ASAR80] and for the second round on level 2 [SKI_ASAR90], with gradually increased scope and level of detail.

The SKI guidelines did not contain any specific recommendations concerning the choice of methods or the layout, contents and level of detail of the PSA. This resulted in considerable differences between the analyses performed by the different licensees. The differences reduced the comparability of the PSA:s, but also contributed to a rapid early development of PSA, by encouraging the development and testing of alternative methods, and by improving the possibilities to detect problem areas.

After this stage and up to today, PSA activities at the utilities have gradually gone into more of a steady-state situation, where PSA:s are kept up to date with plant changes on a yearly basis, and are more or less continuously used as tools for various safety related issues. In parallel, the PSA:s have been considerably extended, and have today (2006) reached or are in the process of reaching full scope (all initiators, all operating modes). This way of working with PSA is in line with current policies at all utilities and with current SKI regulations, and will be further described in the sections below.

3.3.2 Swedish Nuclear Power Inspectorate (SKI)

3.3.2.1 Background

The Swedish regulatory tradition is mainly non-prescriptive, meaning that often high-level requirements are given, while the exact ways to fulfil the requirements is left to the licensees to decide. An important aim of SKI inspections it to maintain confidence in the fulfilment of requirements.

The SKI PSA Review Handbook [SKI_2003:48] indirectly describes the expectations on PSA. The handbook was issued in 2003, and is intended to be a support in SKI supervision of licensee PSA activities by describing SKI procedures for review of PSA:s and inspection of PSA activities. The handbook focuses on good practice and compliance with state of the art.

Lately, the focus has been on compliance with the regulation [SKIFS 2004:1] “The Swedish Nuclear Power Inspectorate's Regulation concerning Safety in Nuclear Facilities”, which is discussed in the next section.

3.3.2.2 History of safety goals

The focus of the SKI is on avoidance of radiological accidents, i.e., safety goals are directed towards protection of the public rather than towards avoidance of core damage. This became evident in the discussions related to the government decisions following the Reactor Safety Investigation [SOU 1979:86] requiring the introduction of severe accident mitigation system first at the Barsebäck plants 1981 [IndDep_1183/81] and then at all other plants in 1986 [IndDep_2717/85]. Basically, these government decisions define the conditions for allowing continued operation of the plants. On the basis of the government's proposition [Prop 1980/81:90] regarding guidelines for the national energy policy, it was stated that in spite of the fact, that the risks for uncontrolled radioactive release from nuclear power plants is extremely small, measures shall be taken to further reduce such risks. At that time, the level of requirements was quite high from an international point of view.

The FILTRA system in Barsebäck was taken into operation in October 1985; for the remaining Swedish NPP:s severe accident mitigating systems including filtered venting were to be installed by the end of 1989. A rather detailed document served as a basis for the decision in 1985. The document "Release mitigating measures after severe accidents" [SKI_SSI_1985] was written by the SKI and the Swedish Radiation Protection Institute (SSI). Based on the document, a number of acceptance criteria for the mitigating systems after a severe accident were defined (items 1 to 4 in section 4.4 and item 5 in section 8.2 of the reference):

- Events with extremely low probabilities (extremt låga sannolikheter) can be neglected.
  It is accepted that the filtered venting system cannot handle a reactor vessel rupture.
- The same requirements on maximum acceptable release of radioactive substances apply to all NPP:s, regardless of location.
  The justification for this requirement, is that the same level of individual risk shall be achieved at all sites, regardless of population density and property values.
- Long-term ground contamination of large areas shall be avoided.
  This is judged to be fulfilled if the radioactive release after a severe accident is limited to below 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MW, excluding noble gases.
- There shall be no short-term fatalities in acute radiation syndrome (akut strålsjuka).
  This is judged to be fulfilled if the radioactive release after a severe accident is limited to below 1 % of the inventory of a core of 1800 MW, excluding noble gases.
- The containment shall remain intact for 10-15 hours after a core melt.

A simplifying interpretation to part of the requirements is given by stating that these requirements can be considered fulfilled if the radioactive release after a severe accident is limited to below 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MWt, provided all nuclides causing unacceptable ground contamination are limited correspondingly. Considering the fact, that the inventory of Cs-134 is 89 TBq/MW and of Cs-137 is 57 TBq/MW, the 0,1 % / 1800MW requirement corresponds to a release of 160 TBq of Cs-134 and of 103 TBq of Cs-137. The requirement that the containment shall remain intact for 10–15 hours after a core melt implies that mitigating measures protecting the containment from over-pressurisation and by-pass shall be designed in a way that practically eliminate the possibility of early releases.

As part of the background description and justification for the selected release criterion, SSI presented a comparison between the fatality risk from exposure to radon in habitations to other risks in society, see Figure 6. The 0,1 % criterion is also justified by the argument that the requirement on the filtering capacity of the filtered venting systems to be installed should not exceed the level of diffuse leakage that is to be expected.

The quantification of the frequency requirement, i.e., converting “extremely low probabilities” into a frequency of occurrence, was done by relating to the concept of residual risk. In [SKI_SSI_1985], reactor vessel rupture is given as an example of a

residual risk[7]. Based on the quantification of this event in WASH-1400, this was interpreted by both the SKI and the licensees to correspond to an event with a frequency of about 10^{-7} per year. However, this frequency is not spelled out in any of the government decisions, neither in [SKI_SSI_1985].

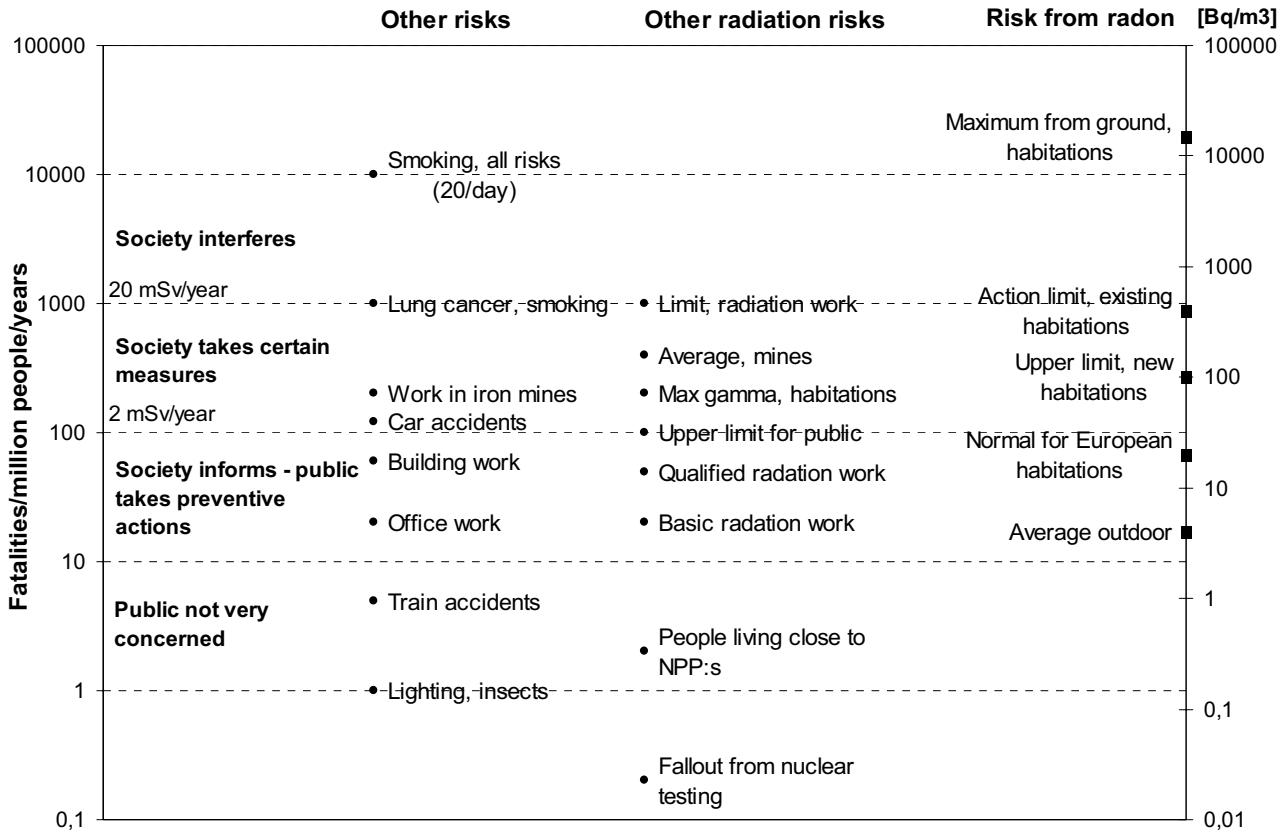


Figure 6. Simplified comparison of risks from exposure to radon with other common risks [SKI_SSI_1985]

Except for the implicit numerical safety goal described above, the SKI has not defined any safety goals. However, the newly issued regulation concerning safety in nuclear facilities [SKIFS 2004:1] requires the licensees to have clearly defined goals for their activities. It is worth noting, that defining numerical safety goals in the SKIFS would be problematic, as the regulations are legally binding, which means that violations of the goals would be liable for prosecution.

Chapter 2 §9 in SKIFS 2004:1 mentions *documented safety goals*, which is commented in the following way in the General Recommendations accompanying the SKIFS "The safety goals may be both quantitative and qualitative. Goals should be formulated so that they can be followed up." No detailed guidance is given, but it is expected that the

---

7 In SKIFS 2004:2, the definition is given as "Extremely improbable events (residual risks). Events that are so improbable that they do not need to be taken into account as initiating events in connection with safety analysis."

licensees develop more elaborated procedures based on e.g. international standards and guidance documents. The basis for the safety assessment is deterministic, but in the view of SKI, PSA can and should be used to verify the deterministic requirements. SKIFS 2004:1 chapter 4 §1 states ”In addition to deterministic analyses … the facility shall be analyzed by probabilistic methods in order to obtain as comprehensive a view as possible of safety.”. As a result of SKIFS 2004:1, it is expected that PSA will be increasingly important in SKI handling of future applications.

One additional criterion with relevance for judgement of results from probabilistic analysis is defined, and concerns the uniformity of the risk profile. SKIFS 2004:1 (chapter 4§1) states ”One aim should be to achieve a safety level without dominant weaknesses.”

Generally, the probabilistic criteria suggested by the IAEA [IAEA_INSAG-12] are informally treated as reference levels by the SKI, but without defining this as a strategy for identifying deviations, and without seeing the levels as absolute. The SKI also considers the IAEA view [IAEA_CB-5] on graded actions, which depend on the magnitude of an identified deviation as reasonable, and this approach is in principle applied by the SKI.

3.3.2.3 Application of safety goals

The licensees are required to have a safety policy, and if the policy includes probabilistic safety goals the licensee is, in principle, expected to fulfil these goals. In the view of the SKI, safety goal defined on the level of core damage or large release should reasonably cover the complete spectrum of risks as calculated in a full-scope PSA, i.e., all categories of initiating events and all plant operating modes.

However, the SKI does not desire a situation where actions need automatically to be taken because of the violation of a safety goal, i.e., it is not judged to be feasible to treat safety goals as absolute acceptance limits. Fluctuations in PSA results over time are unavoidable (updates, extension) and sharp acceptance criteria might in fact be counter-productive. Therefore it is judged reasonable to see safety goals as target values, and to treat exceedances as triggers for further analysis or planning of safety enhancing actions.

Thus, while the fulfilment of the safety goals defined by the licensees is basically mandatory, the actual procedure is more flexible. Exceedance of safety goals is allowed, but should be accompanied by an evaluation stating the reason for the exceedance and — if needed — a plan for correction.

3.3.2.4 Experiences of using safety goals

Exceedance of safety goals is normally not a problem in safety related activities, and can often be justified (uncertainty, conservative approach, etc.). However, an exceedance can be complicated to communicate to the public, and may also be a problem due to the general requirement that licensees are expected to fulfil their safety policy. Deviations which are not handled may cause doubts regarding the self inspection of the licensee.

PSA results are at present (2006) not used very actively at SKI, but more PSA applications are expected in the near future. SKI is not itself performing any PSA modelling or calculations. To date, some issues have been supported by PSA, and SKI has sometimes had PSA evaluation as a condition for acceptance. However, this is still done on a rather

small scale. The degree to which PSA related information is considered in SKI decisions depends on the perceived degree of importance of the information.

PSA results and fulfilment of safety goals has been important in some applications and influenced the decision taken by the SKI, e.g., in the FENIX project for restart of Oskarshamn 1.

A general view is that the evaluation of results needs to be more efficient, which is even more important in view of the fact that safety goals are not absolute. There is a need to break down the top level safety goals to make them useful for more detailed applications.

3.3.3 Sydkraft/E.ON – Barsebäck and Oskarshamn NPP:s

3.3.3.1 History of safety goals

The Sydkraft company (now E.ON Nordic) was the owner of the Barsebäck plants (twin BWR:s of ASEA Atom design); these plants are now decommissioned. The company has a majority share of the Oskarshamn plants (three BWR:s of ASEA Atom design representing three different plant generations). It also has a minority share of the Ringhals plants (one BWR of ASEA Atom design and three Westinghouse PWR:s representing two different plant generations).

The Sydkraft group issued a safety policy in 1995, listing a number of key areas for safety, stressing living up to regulations, experience feed-back, and safety culture [SK_1995_Ahlström]. The policy was developed by the company Advisory Safety Council (säkerhetsråd). The policy also defined safety goals for the frequency of core damage and large releases. The levels defined were 10^{-5} per year for core damage and 10^{-7} per year for a release involving more than 0,1% of the core inventory excluding noble gases. The safety goals were not mandatory, but in case of PSA results above these levels, safety enhancing measures were to be prioritised. For large releases, the safety goals were based on the government decisions regarding severe accident management measures [IndDep_1183/81] and [IndDep_2717/85]. The requirement on "prioritising" means that resources shall be allocated for handling the problem identified, and that the problem handling shall have high priority in comparison with other ongoing activities.

The policy was effective until 2004 when it was updated and re-issued as the E.ON Nordic safety policy [EON_2005_Fritiof]. As part of the update, the quantitative safety goals were deleted from the top-level policy document, slightly revised and presented in an interpretation document [EON_2005_Larsson]. The revised core damage criterion is still at 10^{-5} per year but applies to severe core damage and the criterion for unacceptable releases now states that the frequency shall be considerably lower than the core damage criterion of 10^{-5} per year, which could be interpreted as at least a factor of 10 (the factor is not defined). The policy states that the frequencies shall be used as a basis for assessing the severity of safety problems.

The requirements locally applied at the Oskarshamn NPP were originally derived from the Sydkraft safety policy, and the E.ON safety policy still defines the basic levels. In addition more detailed local criteria for interpretation and judgement of PSA results have been developed [OKG_1996-00385]. They are referred to in the SAR for Oskarshamn , but are expected soon to be deleted from the SAR. The release criterion has been

adapted to the power ratings of the Oskarshamn plants, i.e., it is set to 0,13 % for Oskarshamn 1, 0,07 % for Oskarshamn 2, and 0,055% for Oskarshamn 3.

The internal guidelines for judgement of PSA results regarding impact on reactor safety includes the graded approach described in the IAEA document *Safety Evaluation of Operating Nuclear Power Plants Built to Earlier Standards* [IAEA_CB-5]. This document was never issued by the IAEA, but appeared in a somewhat reduced version in the safety report series as [IAEA_SRS_12]. The action levels specified for core damage frequency are:

- PSA results $>10^{-3}$ per year – immediate shutdown
- 10^{-3} per year > PSA results > 10^{-4} per year – correction at next planned yearly shutdown
- 10^{-4} per year > PSA results > 10^{-5} per year – long-term planning of actions

An additional criterion for the Oskarshamn plants states that if the core damage frequency is within 10% from 10^{-5} per year, then no initiating event family shall contribute more than 10^{-6} per year; this criterion is usually not applicable.

Additional probabilistic criteria have been defined, with a focus on assessment of the remaining system barrier after an initiating event. PSA results are presented based on the cause of the core damage (failure of shut-down systems, emergency core cooling or residual heat removal) and on a split-up of initiating events according to the event category they belong to (H2, H3, H4). This has worked well, especially for events with large uncertainties in initiator frequencies. Criteria have been defined according to an internal document [OKG_2005-14190]. For area events a procedure has been defined for assessing the acceptability of the system barrier against core damage [OKG_2006-09475].

3.3.3.2 Application of safety goals

It is basically problematic to include probabilistic safety goals in the SAR, as these are legally binding document (basis for operational permit), which means that violations may led to prosecution. For this reason, safety goals are better included in policy documents and used as internal indicators for identification of potential safety related issues. They are also a help in the internal argumentation and safety assessment.

The safety goals are used as a limit value for singling out situations that need to be further studied, i.e., as a trigger for starting analysis and evaluation of whether an identified plant condition is a safety problem.

For a completed PSA (including finalised update) an evaluation report is written, where results are evaluated with respect to degree of relevance and impact on reactor safety. The procedure was originally defined in [OKG_2000-03886], now updated in the internal evaluation guidelines [OKG_2005-14190] and [OKG_2006-09475]. Identified deviations are judged with respect to cause, e.g., if the cause is due to an incomplete or conservative PSA model or if it is due to a weakness in the plant. The basic procedure is that identified weaknesses are eliminated. However, if there is a major impact to the result from complex modelling issues, e.g., CCF, decisions on changes will be delayed until a more detailed description is available.

3.3.3.3 Experiences of using safety goals

In spite of problems in connection with discussion of high PSA results both internally and externally in media, the use of probabilistic safety goals has triggered a number of important safety improvements in the Oskarshamn plants (and previously at Barsebäck).

PSA has generally provided an aspect on safety that has been valuable for the total activities at the plants, but this has largely been achieved independently of the safety goals.

A number of major plant changes have been triggered by PSA results or involved PSA in the process. Important examples in both the Barsebäck plants and in Oskarshamn 1 and 2 are the improvement of cable separation in order to improve robustness with respect to area events, especially internal fires. In the FENIX project for Oskarshamn 1 (large-scale renovation 1993–95) the probabilistic criteria for plants built to earlier standards as defined in [IAEA_CB-5] were crucial for the decision by SKI to allow restart of the plant.

A general concern with probabilistic safety goals is the risk of the goals being seen as absolute limits, as this might indirectly have an impact on the quality and relevance of the PSA models.

3.3.4 Vattenfall – Ringhals and Forsmark NPP:s

3.3.4.1 History of safety goals

Vattenfall is the main owner of the Forsmark plants (three BWR:s of ASEA Atom design) and of the Ringhals plants (one BWR of ASEA Atom design and three Westinghouse PWR:s representing two different plant generations).

Safety goals were first discussed at the end of the 1980s within the production department at the Vattenfall central office in Stockholm. This resulted in the publication of a company policy for reactor safety in 1990 [SV_PK 301:1], which was adopted by the central safety committee of the company. PSA related issues in the safety policy have been continuously discussed through the years, and minor revisions of the policy, not affecting the PSA related safety goals, were made from time to time. In 1992 a Vattenfall policy for reactor safety was issued within the business area electrical production [RAB_950227045], including safety goals. The policy stated that high priority is given to safety enhancing measures if probabilistic analyses indicate that the core damage frequency is above 10^{-5} per year with a high degree of confidence or above 10^{-7} per year for a release involving more than 0,1% of the core inventory of substances causing ground contamination.

The latest version of the policy [SV_KSÄK_2006] is part of the management system for electrical production. The policy stresses the integrated aspects of safety assessment, stating that the planning of safety improvements shall be based on a combination of deterministic criteria, probabilistic methods, human factors analysis and utilisation of experience feedback. Regarding plant PSA:s, it is stated that they shall be realistic and site specific, and shall be used for verification of balanced safety (jämnstyrkekontroll) as well as for assessment of the technical safety of the plants. The probabilistic safety goals for Vattenfall NPP:s are the same as in 1992. In case of exceedance of the safety goals, correcting actions shall be planned and PSA results shall be used as part of the basis for planning safety improvements.

The safety policy on company level has been converted to site specific policies at the Ringhals and Forsmark plants. At Ringhals this is done in a three-level hierarchy of documents with ”Fackområdesdirektiv – reaktorsäkerhet” (Technical area directive – Reactor safety) [RAB_990714068] and ”VD-direktiv – Reaktorsäkerhet” (Management directive – Rector safety) [RAB_1723490] at the top, setting high-level requirements, which are further detailed in “VDD-tillämpning – Övergripande mål och förhållnings-sätt för reaktorsäkerhet” (Application of management directive – Over-all goals and approach to rector safety) [RAB_1839723]. The latter document includes detailed requirements and some additional criteria. The probabilistic safety goals on the level of core damage and large release are taken directly from the Vattenfall safety policy [SV_KSÄK_2006]. In addition, the use of probabilistic analyses is generally discussed, and it is stated that the focus shall not be on absolute numerical results. Instead priority shall be on long-term safety improvements, identification of weaknesses and prioritisation of safety improvements.

The local policy for Ringhals includes a set of additional criteria for the judgement of detected deviations which do not result in violation of the Technical Specifications:

- If the CDF is > 10^{-4} per year, immediate corrective actions for identified deviations are required. If this is not possible, the plant shall be immediately shut down.
- If the CDF is between 10^{-4} per year and 10^{-5} per year, the plant may remain in operation for a limited period of time. Temporary corrective actions are allowed while permanent safety enhancing measures are developed, designed and implemented.
- If the CDF is < 10^{-5} per year, long term planning of safety enhancing measures is allowed, to be implemented in connection with plant modernisations.

These criteria are in line with the levels defined in the draft IAEA guide CB-5 [IAEA_CB-5], but one order of magnitude stricter.

3.3.4.2 Application of safety goals

PSA results exceeding the probabilistic safety goals require planning for corrective actions. At the Forsmark plant, this is done by writing a deviation report, which is then handled by the local safety committee, except in case of minor deviations, where the handling is done by the quality department.

There is a difference between exceedances caused by “deterministic deviations” and by “PSA method issues”, i.e., identified design weaknesses are considered more important as they concern basic plant properties that are part of the basis for the operating license. PSA method issues are often due to non-fulfilment of the requirement on realistic PSA models, and are handled by deviation handling.

3.3.4.3 Experiences of using safety goals

At Vattenfall sites the development has been a move from a rather negative impression of PSA to a more positive one. The ASAR process with regular updates has increased the awareness in the organisation of the value of PSA. The current view is that PSA in the right context and accompanied by other relevant information (deterministic analyses, human reliability analyses, and operating experiences) gives a very valuable contribution to safety analysis, and PSA has become an integrated part of the total safety analysis concept.

This relates to PSA as such rather than to safety goals, but safety goals have also to some extent contributed to an increased awareness of the usefulness of PSA. At an earlier stage, they are also believed to have had a slightly repellent effect, mainly because of a fear that exceedances might lead to unreasonable requirements on implementation of safety improvements, and that such actions might then be based on crude assumptions and prerequisites. An important background to this concern is the fact that previous updates and extensions of PSA:s have resulted in large variations of results both regarding the total CDF or release frequency and the distribution between different groups of initiating events. These concerns still exist to some extent. For this reason, the view is that safety goals are mainly to be used as checkpoints showing that changes made point in the right direction, and that they can be useful as guidelines in the safety work.

At the sites, safety goals have not had a decisive impact. The focus has been on the identification and importance ranking of dominating contributors. PSA has also been an efficient tool for identification of functional dependencies. However, one perceived positive effect of the safety goals is that they have increased the focus on the correctness of the PSA models. Another experience is that the quality requirements on PSA increase in risk-informed applications. In discussion with the SKI, safety goals have never had any importance.

3.3.5 Westinghouse Electric (previously ASEA Atom)

3.3.5.1 History of safety goals

The same definitions are used as by the power companies, i.e., maximum core damage frequency 10^{-5} per year and maximum frequency of large releases 10^{-7} per year. These criteria have been important for issues related to diversification.

In addition, Westinghouse uses complementary probabilistic goals, especially the frequencies defining the limits between event classes. These event classes (H1–H5) are basically the best estimate frequency of occurrence [per year] defined for different plant conditions (PC1–PC5) in [ANSI/ANS-52.1-1983], i.e.:

H1	Normal Operations	1
H2	Expected events	$1 > F \geq 10^{-2}$
H3	Non-expected events	$10^{-2} > F \geq 10^{-4}$
H4	Unlikely event (DBA)	$10^{-4} > F \geq 10^{-6}$
H5	Very unlikely event (BDBA)	$F < 10^{-6}$
Residual risk	Extremely unlikely event	$F < 10^{-7}$

With this approach, the event categories define the probabilistic target values. Exceedances, i.e., events not meeting the class/frequency relation, are handled either by reducing or eliminating the events consequence or by reducing the event frequency to make it fall into a higher event class. The approach is primarily used on initiating events, but is sometimes also applied to more sequence related functions (initiating event and safety function).

3.3.5.2 Application of safety goals

Safety goals are never used as the only acceptance criterion to decide if the required safety level for a plant has been met. The aim when applying safety goals is always to design and dimension diversifications. The acceptance criteria are then needed in order to answer the question "How safe is safe enough?". This means that acceptance criteria are mandatory in design applications, because the probabilistic goals defined must be fulfilled. This also applies to the use of event classes as safety goals.

However, the safety goals defined by the licensees are found to be too crude and on too high a level to be fully useful as evaluation criteria for PSA results. A consequence of this is, that additional analysis and judgement is usually needed also in cases where the safety goals are met.

3.3.5.3 Experiences of using safety goals

Safety goals are indispensable as design aids, i.e., in order to decide at what point a design has become good enough. This is especially important in the evaluation of the required degree of diversity in a design, where the goals are needed as guidance for the planning and implementation of the diversity.

Basically, safety goals are seen as necessary, and requirements that have gradually been put on the plants cannot be met without the use of safety goals. This need has been more marked after the appearance of the regulation [SKIFS 2004:2] concerning the design and construction of NPP:s.

3.3.6 Summary of Swedish safety goals

Table 3 summarises the safety goals defined for Swedish NPPS through the years.

Table 3. Probabilistic safety goals in Sweden – a summary

Authorities	**Vattenfall**	**Sydkraft / EON**
1985 Core damage - Release Release of more than 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MWt shall be "extremely unlikely" (Interpreted as < 10^{-7} per year).	**1990** Core damage 10^{-5} per year with a high degree of confidence Release 10^{-7} per year for a release involving more than 0,1% of the core inventory of substances causing ground contamination.	**1995** Core damage 10^{-5} per year Release 10^{-7} per year for release involving more than 0,1% of the core inventory excluding noble gases.
	2006 Core damage 10^{-5} per year Release 10^{-7} per year for a release involving more than 0,1% of the core inventory of substances causing ground contamination	**2006** Core damage 10^{-5} per year for *severe* core damage Release Frequency of release involving more than 0,1% (1800 MWt) of the core inventory excluding noble gases shall be considerably lower than 10^{-5} per year.

The definitions of the safety goals are basically identical among all organisations, i.e.,

- Core damage
  Defined as local fuel temperature above 1204 ºC, i.e., the limit defined in section 1b of 10 CFR 50.46, Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors.
  Note: The recently issued EON criterion has revised this to "severe core damage". However, no additional criteria are given for defining "severe".

- Large release
  In spite of the slightly different wordings, sometimes lacking in stringency, the basis is always in the definitions given in the government decision regarding severe accident mitigating measures from 1985 [SKI_SSI_1985], i.e., according to the first column in Table 3.

The definitions of the frequencies of the safety goals are also more or less identical among all organisations, i.e.,

- Maximum frequency of core damage < 10^{-5} per year.
  However, there seem to be two different justifications for this frequency:

  Based on INSAG-12, which suggests the safety goal 10^{-4} per year for existing plants, but reduced by a factor of 10.

  Based on the government requirement regarding large releases, interpreted as 10^{-7} per year, and defined by assuming a barrier of two orders of magnitude relative to this frequency.

- Maximum frequency of large release < 10^{-7} per year.
  In this case as well, there seem to be two different justifications for this frequency:

  Based on the government requirement regarding large releases, interpreted as 10^{-7} per year.
  Note: This frequency is not spelled out in any of the government decisions, neither in [SKI_SSI_1985]. All of these only refer to the concept of an "extremely unlikely event".

  Based on quantifying a reasonable and achievable additional barrier in relation to the CDF safety goal. In the 1980s this was believed to be two orders of magnitude. Lately, the assumptions is closer to one order of magnitude, which has influenced some of the safety goal updates. This has also been considered in the reformulation of the E.ON safety goals.

Some other types of safety goals are also used by some of the organisations:

- Westinghouse uses complementary probabilistic goals, defined on the basis of event classes (H1–H5), where the related frequencies define the probabilistic target values.
- OKG is actively using acceptance criteria related to barrier strength for events with major uncertainties in the initiating event frequency, e.g., internal fires.

Finally, it is worth mentioning, that safety goals have also been addressed in the VGX project (the Värnamogruppen expert group), a common utility project dealing with

safety requirements and design principles for Swedish NPP:s [VGX-0003-01]. The project suggested safety goals, on the same lines as the ones described above, and defined the role of probabilistic analysis, i.e., to give an integrated view of how specific equipment interacts and affects the over-all plant safety, as well as of the required degrees of redundancy and separation in order to achieve the safety goals defined. However, the VGX report was never officially issued.

3.4 Limited international overview

Target values for PSA results are in use in most countries having nuclear power plants. Criteria are defined corresponding to all PSA levels:

- PSA level 1 – Core damage frequency
- PSA level 2 – Magnitude of radioactive releases
- PSA level 3 – Consequences from release (health effects)
- In some countries there are also lower level criteria, e.g., for important safety functions.

Even though the status of PSA programmes is quite similar in most countries, the safety goals defined by the industry or the regulatory bodies vary between countries. Existing safety goal approaches could be divided into the following main categories:

- No numerical safety goals are stated by the regulatory body, but utilities may have safety goals and numerical evaluations can be used in regulatory decision making and in risk-informed applications, e.g., Belgium, Canada, Czech Republic, Germany, France, Hungary, Japan, Korea, Mexico, Spain, and Sweden (for core damage frequency).
- Numerical safety goals are defined for nuclear power plants (new and/or existing) in terms of core damage frequency or large early release frequency, e.g., Finland, Russia, Slovak Republic, Switzerland, Sweden (for maximum allowed releases), and Taiwan.
- Numerical safety goals are defined for hazardous industry in terms of human mortality risk, and safety goals for NPP:s are derived from the overall safety goal, e.g., the Netherlands, UK, and USA.

In addition to the national safety goals, international and national organisations have defined safety goals. The International Atomic Energy Agency (IAEA) defined safety goals already in the 1980s [IAEA_INSAG-3]. The report was updated in 1999 [IAEA_INSAG-12]. The European Utility Requirements for LWR nuclear power plants (EUR) include also definitions for probabilistic design targets [EUR_2002]. EUR frequency targets include shutdown states which have been shown to be a significant contributor in assessments of present reactor designs.

Table 4 summarizes examples of numerical safety goals defined in different countries and by the IAEA as well as EUR guidelines.

Table 4. Safety goals defined by some countries and organisations.

Country	PSA level 1	PSA level 2	PSA level 3	Comment
Finland *[STUK_YVL-2.8]*	Core damage $f < 10^{-5}$ per year	Large release > 100 TBq Cs-137 $f < 5 \cdot 10^{-7}$ per year		Applicable to new plants.
Netherlands [VROM-1988]			Individual risk (all sources) $f < 10^{-5}$ per year Individual risk (single sources) $f < 10^{-6}$ per year Group risk $F(n) = 10^{-3}/n^2$	General goals based on F-N approach for major accidents in all hazardous industries. Long-term effects are not included in the group risk.
Russia [OPB-88/97]	Severe beyond DBA 10^{-5} per year	Limited release 10^{-7} per year		
Slovakia *[Slovakia-2005]*	Core damage $f < 10^{-4}$ per year	LERF $f < 10^{-5}$ per year		Additional criteria: Safety systems > 10^{-3} per demand. RPS < 10^{-5} per demand.
Sweden *[SKI_SSI_1985]*		*Unacceptable release* *> 0,1 % of the inventory of Cs-134 and Cs-137 in a 1800 MWt core* *f < extremely unlikely*		*"Extremely unlikely" interpreted as 10^{-7} per year*
Switzerland [HSK-R-100/d]	Core damage $f < 10^{-5}$ per year			New plants Applicable to existing plants to the extent reasonably achievable.
UK [HMI_SAP_1992]	Core damage BSL 10^{-4} per year BSO 10^{-5} per year	Large release > 10^4 TBq I_{131}, > 200 TBq Cs-137 BSL 10^{-5} per year BSO 10^{-7} per year	NPP worker BSL 10^{-4} per year BSO 10^{-6} per year Group risk For dose>1 Sv BSL 10^{-4} per year BSO 10^{-6} per year	BSL = basic safety limit BSO = basic safety objective Group risk limits defined also for other doses. Note: Major changes will be introduced in on-going SAP update.
USA [USNRC SECY-01-0009]	Core damage $f < 10^{-4}$ per year	LERF $f < 10^{-5}$ per year	Group risk Prompt fatalities < 0.1% of prompt fatality risk from other accidents. Cancer fatalities < 0.1% of cancer fatality risks from all other causes.	Goals on Levels 1 and 2 are subsidiary objectives intended to achieve the same intent as the quantitative health objective (level 3)
IAEA *[IAEA_INSAG-12]*	Core damage *$f < 10^{-4}$ per year*	LERF *$f < 10^{-5}$* per year		Existing plants LERF = "*Large off-site releases requiring short term off-site response*"
	Core damage *$f < 10^{-5}$ per year*	LERF *"Practical elimination"*		Future plants
EUR *[EUR_2002]*	Core damage *$f < 10^{-5}$ per year*	*Criteria for limiting* impact *$f < 10^{-6}$* per year *LERF* Significantly *lower frequency.*		New plants

4 Selected Issues

This chapter focuses on selected issues that were highlighted in the first phase of the project, with the purpose to present different points of views on these sometimes controversial issues. The aim is to continue investigating the issues and possibly to give recommendations in phases 2 and 3 of the project.

4.1 Use of safety goals in decision making

A numerical safety goal can be a mandatory criterion (limit), a desired target (an objective), a compensatory criterion, or an informal goal. In mandatory use, the value must be strictly met. This is typically the situation when numerical objectives are used for new NPP:s.

An objective is a desired target that should be aimed at, but where violations can be accepted and justified. Many licensees have defined safety goals for their plants as objectives, e.g., CDF < 10^{-5} per year. In this usage, the safety goal is part of a long-term strategy to improve the safety of the plant. Some utilities include the PSA safety goals in their formal safety policy (Swedish utilities), while others keep them informal (Finnish utilities).

A safety goal can also be compensatory, meaning that trade-off can be made. Cost-benefit evaluations and the ALARP principle allow such use. Finally, a goal can be informal, which is the case in risk-informed applications.

All of the organisations interviewed in this phase seem to favour an informal use of safety goals, due both to the uncertainties in the PSA methodology and to the possibility for flexible handling of risk. It is feared that strict safety goal may switch the attention from an open-minded assessment of safety to the strict fulfilment of safety goals. This was stated in many of the interviews, and is also stated to be one reason why there are no official safety goals in France. One could also speculate whether very strictly applied safety goals could not lead to manipulation of results.

Use of trade-off analyses has also been suggested by several authors [NKA_1989:91, RESS_61(1998)11, RESS_90(2005)15]. The basic argument for this position, is that risk is never accepted unconditionally. The problem of acceptable risk is a decision making problem. Pre-determined acceptance criteria may result in the wrong focus rather than support the search for good and cost-effective solutions.

The use of safety goals, implies a need for rules to handle violations. In Sweden, rather formal procedures for applying PSA safety goals are in place, but seem not to be strictly enforced. This is probably due to the fact that PSA results have exceeded the safety goals most of the time since they were defined. Implicitly, a graded ALARP-like approach has been applied, i.e.,:

- CDF <10^{-4} per year, i.e. the IAEA goal is a *limit,*
- CDF <10^{-5} per year, i.e., the own goal is a *target*.

In Finland, the companies' own safety goals for operating plants are informal and are interpreted as targets, not as limits. For this reason, discussion on handling of violations has not yet been necessary.

Success in the use of safety goals depends on the role of safety goals for decision making among the negotiating parties (safety authority, utility, vendor). Conflicts may arise if PSA and safety goals do not have the same status in decision making within an organisation or between organisations.

Principally, the purpose of the utility is to maximize the return of investments and the purpose of the safety authority is to supervise and regulate all risk to human beings and environment. Theoretically, this could be a game situation with conflicting objectives. In practice, rules for operation of hazardous industries are defined in laws and in related regulatory documents. The utility must prioritize safety and the safety authority needs to take account of economical facts. As a result, there is in practice to a large extent a consensus situation with common objectives. The question is what is safe enough and what kind of demonstration of safety is sufficient. Balance between different safety requirements may also cause debate.

Although there has been a continuous progress in the development and use of PSA in decision making, there has also been variation in the enthusiasm for PSA. This depends on the experience gained from the use of PSA. Examples of positive experience are the complementary view on safety provided by PSA and the possibilities to relax stringent deterministic rules. Resistance to the use of PSA can arise if PSA is felt to be an extra burden in addition to deterministic rules. Also, large variations in PSA results when updated can weaken the credibility of the method, especially among decision makers with a limited knowledge of the technique.

A controversial issue related to safety goals is the interactions between deterministic and probabilistic safety requirements [YVL-review]. Up to now, these concepts have been difficult to integrate in practice and people seem often to be tuned to one or the other. Finding a correct balance between deterministic and probabilistic safety thinking has to do with the fundamental question of what is safe enough. It would be beneficial to enter a discussion on the relationships between such deterministic and probabilistic criteria and their interpretation in illustrative cases.

4.2 Ambiguities in definitions of safety goals

There is quite good consensus about the definition of a core damage. For the frequency, most organisations have chosen either the levels 10^{-4} per year or 10^{-5} per year, usually referring to IAEA safety goals suggested for existing plants and future plants, respectively. The actual definition of what constitutes a "core damage" shows a larger variation, spanning from the 10 CFR 50.46 limit for local fuel temperature of 1204 ºC, which is a very conservative definition, to "severe core damage" which is more realistic but less stringently defined. Obviously, other reactor types may require differently defined criteria, such as the Canadian more general definition for core damage, i.e., "failure to maintain the core coolable geometry", to be interpreted as failure of more than one fuel channel in a CANDU reactor.

A question not addressed in any of the safety goals reviewed, is the need for additional fuel damage criteria for cases when fuel is not in the reactor vessel or not damaged due to overheating. However, this may be better handled as part of a level 2 safety goal.

The definitions of a large release vary considerably. There is both a considerably larger variation in the frequency limits, and very different answers to the question of what constitutes an unacceptable release. As with the CDF, the magnitudes are sometimes based on IAEA safety goals suggested for existing plants, i.e., on the level of 10^{-5} per year. However, most countries seem to define much stricter limits, between 10^{-6} per year and 10^{-7} per year. The definition of what constitutes an unacceptable release differs a lot, and there are many parameters involved in the definition, the most important ones being the time, the amount, and the composition of the release. Additionally, other aspects may be of interest, such as the height above ground of the point of release. The underlying reason for the complexity of the release definition, is largely the fact that the release definition constitutes the link between the PSA level 2 results and an indirect attempt to assess health effects from the release. However, such consequence issues are basically adressed in PSA level 3, and can only be fully covered in such an analysis.

In Sweden and Finland, existing definitions of an unacceptable release are directly or indirectly based on the Swedish government decision in 1985 regarding severe accident mitigating, i.e., “0,1% of a 1800 MWt core”, corresponding to a release of 100 TBq of Cs-137. This “unacceptable” release is not necessarily large, and the definition includes no timing aspects, which makes the scope of the criterion very wide. Therefore, additional release criteria may be beneficial for the sake of efficient analysis and utilisation of results.

As previously stated, PSA results for most Nordic plants have most of the time exceeded the safety goals defined internally by the utilities. This has caused some confusion regarding the status of the criteria, at least in Sweden, but the PSA results have nonetheless been considered acceptable on an over-all level. In reality, this indicates an implicit use of an ALARP approach, where the defined safety goals have been considered to be safety objectives, while the actual PSA results have been considered tolerable, on the basis of being lower than an (undefined) safety limit.

4.3 Treatment of uncertainties in the application of safety goals

Uncertainties of PSA make the application of safety goals problematic, as there are uncertainties in PSA which are clearly identifiable but difficult to quantify. Uncertainties should be accounted for in decision making but there is no formal method, within PSA methodology, to do it. As long as safety goals have an informal role, uncertainties can be handled by discussion. However, a mandatory goal requires strict comparison of two numbers.

One approach is to make a quantitative uncertainty analysis and to apply a numeric goal for uncertainties, too. The previous version of the guide YVL 2.8 included such a formulation: *The unreliability of the most important safety functions is required to be below the following design objectives, at least with a confidence of 90 %* [STUK-YVL-2.8-1987]. There is, however, no theoretical framework to justify the use of the median, the mean or some other characteristics of an uncertainty distribution for this type of evaluation. A typical approach to handle uncertainties, is to perform combinations of qualitative and quantitative uncertainty analyses combined with sensitivity analyses. No numerical acceptance criterion is applied, but results are discussed qualitatively.

The problem of uncertainties can be turned around by focussing on the demonstration of safety goals instead of aiming at a realistic assessment of risk. Theofanus [RESS_54(1996)243] suggests that, in the presence of epistemic uncertainty, safety goals can be defined only qualitatively. In his approach called ROAAM (Risk Oriented Accident Analysis Methodology), the aim is to explicitly separate out the epistemic uncertainty and quantify them using a specific probability scale defined for phenomenological uncertainties. ROAAM has been applied in level 2 PSA for Loviisa. A similar approach for achieving comparability of results was suggested in a project dealing with the interpretation of PSA results within the Swedish external events project in the 1990s [SKI_1997:49].

Another approach to account for uncertainties is to make the necessary complementary assessments to PSA, e.g., simplified judgements regarding missing parts in the scope of the “original” PSA. The aim with the comprehensive uncertainty evaluation (CEU) is to complement the scope of PSA with additional judgments so that a ”true” comparison against the safety goal can be made [Brown_1999].

Regardless of the approach used in the analysis of uncertainties and their impact on the comparison of PSA results to safety goals, the main issue is always to demonstrate that the plant (or system) is safe enough. This should be carried out as in a safety case, which is a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment [Bishop_SC]. In order to be sufficient, the safety case should include convincing arguments about handling of uncertainties. Figure 7 shows a generic structure for a justification of the compliance with the safety objectives where probabilistic goals are part of the justification, which is based on a claims-argument-evidence structure. The idea of this structure is that PSA results can be complemented with other assessments if PSA is regarded as incomplete.

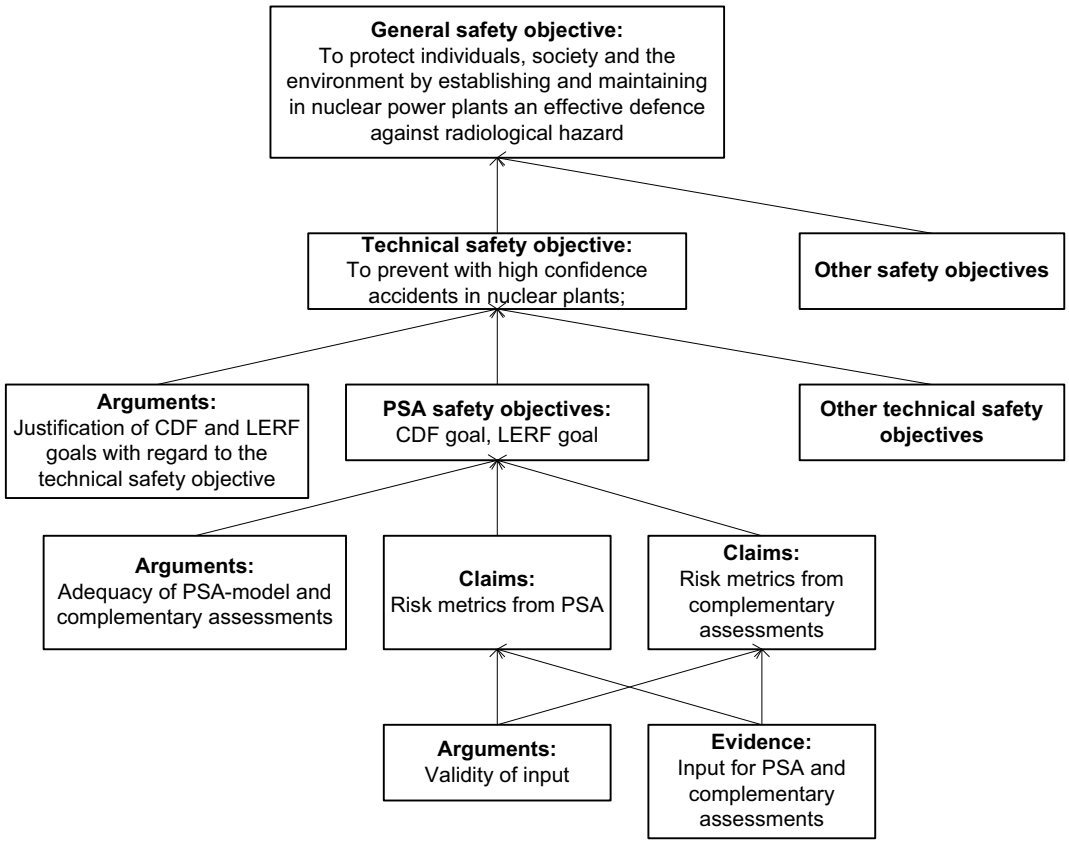


Figure 7. Safety case or goal based approach for showing the compliance with safety objectives by means of PSA [Bishop_SC].

4.4 Ambiguities in the scope safety goals

The status of PSA:s in the late 1980s, i.e., at the time of discussing and issuing the first sets of safety goals, was necessarily less mature than today and PSA:s at the time were very incomplete in comparison to today's full scope PSA:s. It seems to have been implicitly assumed that the safety goals issued were applicable to a "typical PSA", which at that time was limited to power operation and included mainly internal events. Based on results from PSA:s performed at that time it was also assumed that the safety goals defined could be reasonably expected to be fulfilled. It is worth noting that the U.S.NRC also assumed in the 1980s that only internal events are included when applying PSA safety goals.

The gradual extension of the PSA:s and the inclusion of new initiating event categories and operating modes has lead to a situation where safety goals defined are frequently violated. There are further complications when analysing complex initiators, e.g., internal fires, or complex operating states, e.g., cold shut-down.

A reasonable position, is that the high level criteria dealing with health effects or contamination of surrounding land and sea areas, i.e., the criteria which are closest to the subject at risk, should remain unaffected by the scope of a PSA. An example are the Swedish requirements regarding unacceptable releases to the surroundings (0,1% / 1800 MWt).

Thus, the safety goals shall in principle be applied to a full scope PSA, i.e., to the total risk of the plant. This is also a prerequisite when aiming at rational risk-based decision making, which would be problematic with an incomplete PSA. In such a case, it might be considered to adjust the safety goal depending on the scope and quality of the PSA. However, such an approach might lead to circular reasoning, by requiring an assessment to be made of the magnitude of the missing parts of the PSA in order to make possible the definition of a modified safety goal. Therefore, if the PSA scope is not complete, (conservative) complementary assessment of risk from omitted parts is required.

Another type of problem arises for certain initiating event classes which include much larger uncertainties than the basic PSA, e.g., area events and external events. The uncertainty usually relates both to the frequency of occurrence of the events and to their characteristics (strength, duration, etc.). The analysis approaches for such event categories include both conservative assumptions to simplify the analysis of complex scenarios, and potentially non-conservative simplifications. In this case, there may be reason to consider alternative approaches, such as the introduction of lower level criteria for analysis of crucial parts of the scenarios. As an example, criteria can be defined for barrier strength after the postulated occurrence of an initiating event with high uncertainty, e.g., a certain fire scenario. Such an approach can be efficient as a decision tool, but has the drawback, that it does not allow an integrated assessment of risks from different initiators.

4.5 Relationship between goals on different levels

When ranking safety goals on different levels, it seems once again to be a reasonable positions that high level criteria, which are closest to the subject at risk, are the more important ones. With such a view, lower level safety goals are seen as subsidiary goals, which are used in order to gain some degree of confidence, based on lower level results, in the ability of plant systems and functions to contribute to the fulfilment of the high-level goal. There may be an added advantage of reduced uncertainties on lower levels, leading to less ambiguity in decision making.

If multiple criteria are defined, it is reasonable to expect the safety goals on different levels to be consistent, i.e., they shall not lead to contradictory decisions. This will usually be fulfilled as the goals address different aspects of plant safety, by relating to different defence-in-depth levels.

Another view on the reasons and benefits for having multiple safety goals is, that results on the level of core damage are closer to the design and may therefore be easier to communicate both internally and externally for a utility. Analysing the progression of an accident after a core damage includes very low frequencies and large uncertainties. As a result, releases are more difficult to understand and communicate. The basis for the safety work of a utility is to avoid core damage, which is a further reason to have a safety goal on this level. Thus, the core damage criterion may be seen as mainly an operational criterion for the licensee, while the release criterion is related to risks on society level.

Efficient interpretation and utilisation of PSA results in practical safety related activities, e.g., design and maintenance, requires additional goals to be defined on lower

levels of defence-in-depth than core damage and release. At present, additional analysis and judgement is needed also in cases where high level safety goals are met, but where lower levels of defence-in-depth may have been violated.

Figure 8 illustrates some of these concepts, linking PSA levels to levels of defence-in-depth and to the various safety goals.

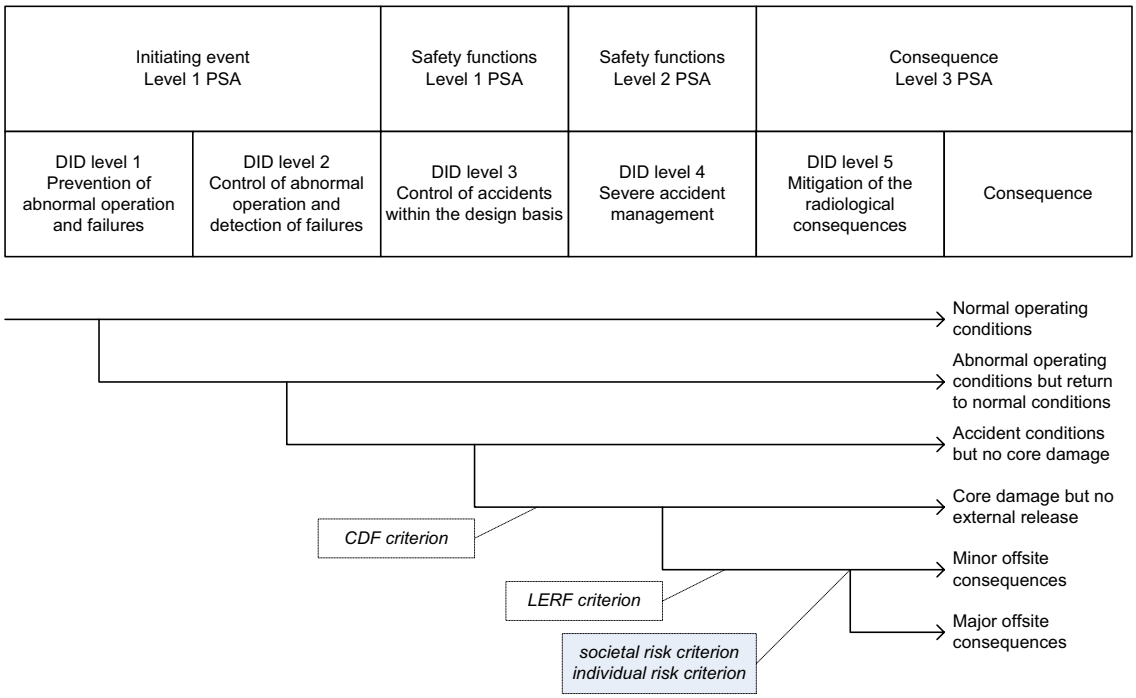


Figure 8. Simplified PSA event tree and corresponding levels of defence-in-depth (DID) linking event tree branches with different high level and surrogate safety goals [IAEA_INSAG-10].

A reasonable position is that both the CDF and release goals should be fulfilled. However, they are not equally important, as the release goal is closer to the subject of the risk (people or plant surroundings) and therefore should have priority over the CDF goal. On the other hand, it is easier to compare CDF results in a level 1 PSA where the methodology is more stable and uncertainties smaller than in a level 2 PSA. This aspect prioritises the use of level 1 goal. In practice, both these considerations will need to be kept in mind when viewing PSA results in the light of safety goals.

To validate safety goals related to CDF and large releases as surrogates of societal risk calls for assessments of the environmental consequences of event sequences resulting in radioactive releases. The results of a level 3 PSA includes this aspect. Level 3 PSA is only required in few countries, typically those with safety goals defined on the level of population risk, e.g., Australia and the Netherlands. In Finland and Sweden, there are not yet any plans to perform level 3 PSA:s. However, there is a need to discuss and define more precisely the safety goals related to unacceptable releases, as they seem to be understood differently in different organisations. For instance, the inclusion or exclusion of long-term effects makes a big difference as well as the inclusion or exclusion of the affected population in neighbouring countries. This issue will be explored in the next phase of the work.

A related question in this context is the relationship between safety goals and decision criteria used in different PSA applications. Risk informed applications (allowed outage times, surveillance test intervals, in-service-inspection, safety classification) study different risk control methods and their influence on, e.g., core damage frequency. The aim of these methods is to identify deviations in the operational rules or maintenance programme from the risk point of view and to support optimisation of these rules and programmes.

There are several approaches for each application. Some of the approaches directly aim at optimisation (minimisation) of the core damage and large release frequency. These approaches are comparable to each other, and can be linked to the use of safety goals.

However, many approaches apply risk importance measure based indicators to balance the risk profile of the plant with respect to the risk control method under consideration. In these approaches relative risk measures are optimised and the approaches are not necessarily comparable to each other. As a result, the link to the overall safety goal usually remains implicit.

4.6 Use of safety goals for new plants vs. for operating plants

New plants and old plants are not in the same position regarding the use of safety goals. For the oldest plants, the design basis is solely deterministic and PSA was not used at all during the design and licensing phase. A design phase PSA is also different from an as-operated PSA with regard to level of details and quality of data.

In the case of new plants, safety goals are used by the utility both in relation to the vendor and to the safety authority. In the regulatory use, the role of safety goals is principally clear, i.e., PSA results are compared with numerical objectives and no violations are accepted in this situation. Identified uncertainties and recognised quality problems in PSA may cause problems when judging the acceptability. The same acceptance problems exist in the review of deterministic safety analyses. Important questions in this context are which numerical goals that are defined, and the scope and quality of the PSA that is required in the design phase.

The role of safety goals for operating plants is less clear. In the present situation in Sweden and Finland, the regulatory guides focus on PSA activities, i.e., they require performance of PSA and use of PSA in safety management. It is mainly up to utilities to define the evaluation criteria, including safety goals, and the way of applying them. Therefore great variations exist between utilities, even if the safety goals defined for new plants are relevant references [IAEA_INSAG-12]. Also the U.S.NRC's guides for risk-informed applications are a widely used standard.

A frequently encountered regulatory requirement for operating plants is to require continuous improvement of safety. It is often not clear, if this should be understood such that risk increasing plant modifications are not accepted regardless of the absolute level of the frequency of core damage or large release.

4.7 Comparison of safety goals defined in different contexts

There is a need to compare safety goals defined in different contexts, e.g., for different industries. In this way a better basis could be gained for justifying that the safety goals are such that compliance warrants a "safe enough" plant. In the next phase of the project, one aim is to make a thorough compilation of high level safety goals used in other contexts (offshore industry, transportation, etc.).

The societal level criteria (F-N-curves) and individual risk criteria used in other areas are as such applicable references for high level safety goals. A variety of criteria can be found. The numerical societal criteria defined in the UK and the Netherlands define the limit 10^{-5} per year (UK) or 10^{-7} per year (the Netherlands) for an accident with more than 100 deaths. In the USA, the societal risk criterion is comparative and qualitative so that the risk to society from generating electricity using nuclear power should be comparable with that from generating electricity by other techniques. It should not be a significant addition to other societal risks, and the quantitative criterion is that the risk of death should be <0,1% of the sum of cancer fatalities from other sources. Individual risk criteria vary between 10^{-4} per year (limit in the UK and Canada) and 10^{-6} per year (objective in the UK, Japan and Canada, limit in the Netherlands for a single source).

Cost-benefit ratios for saving a human life (e.g. in traffic safety) or for justification of receiving radiation doses (e.g. 2000 USD/person-rem [NUREG-1530]) may also be used as references, if a comparison of these risks with nuclear accident risks is considered reasonable.

Comparison of safety goals used in different contexts raises the question of the extent to which different risks can be meaningfully compared. In cases like this, there is always the possibility, that risk comparisons are perceived to be an effort to pre-empt judgments about the acceptability of a risk. On the basis of this experience, different kinds of risk comparisons have been ranked in terms of their acceptability to people in the community [Covello_RiskComp]. Examples of high-ranking comparisons, i.e., widely accepted ones, include comparisons of the same risk at different times, comparisons with a standard, and comparisons with different estimates of the same risk. On the other hand, the comparison of unrelated risks is very low-ranking, meaning that one should be very cautious when comparing, e.g., traffic risks with nuclear risks. Low-ranking comparisons can be misleading and regarded as manipulative. This complicating nature of risk comparisons is a fact to be accounted for when justifications for safety goals are looked for in other contexts.

5 Conclusions

In this first phase of the project, the aim has been on providing an adequate description of the issue of probabilistic safety goals for nuclear power plants, to define and describe important concepts related to the definition and application of safety goals, and to describe experiences in Finland and Sweden.

The issue of safety goals is of great immediate interest, and the results from the project can be used as a platform for discussions at the utilities on how to define and use quantitative safety goals. The results can also be used by safety authorities as a

reference for risk-informed regulation. The outcome can have an impact on the requirements on PSA, e.g., regarding quality, scope, level of detail, and documentation. Finally, the results can be expected to support on-going activities concerning risk-informed applications.

In Sweden and Finland there are more than 20 years of experience of performing PSA, which includes several revisions of the studies, a gradual increase in scope and level of detail, as well as steadily increasing use of PSA for decision making. In spite of the many safety improvements made through the years based on PSA results, a current view is that the safety goals outlined in the 1980s, i.e., 10^{-5} per year for CDF and 10^{-7} per year for unacceptable release, are hard to achieve for operating NPP:s. This experience arouses confusion that should be resolved in order to further strengthen the confidence in the PSA methodology. Questions aroused include what safety goals should be applied for operating plants, whether the risk level of the plants is too high, whether PSA:s are too conservative, and if safety goals are being applied in an incorrect way? The situation can be somewhat different for a new plant, for which risk insights have been utilised already from the design phase. Therefore, it will be interesting to see to what extent the Olkiluoto 3 NPP currently being built in Finland will fulfil the safety goals and what influence the safety goals will have on the final design of the plant.

The use of safety goals is mostly understood to have had a positive impact from a PSA quality point of view. In order to meet safety goals, unnecessary conservatism needs to be avoided in the modelling, i.e., the basic aim should be to have realistic PSA models. It seems that informal use of safety goals and cost-benefit evaluations is preferred by most to a situation with strictly enforced safety acceptance criteria. One perceived reason to avoid strict use of safety goals, is that this might switch the attention from an open-minded assessment of plant safety to the mere fulfilment of safety goals.

The use of safety goals implies a need for rules to handle violations. In Sweden, formal procedures for handling PSA safety goals are in place, but do not seem to be strictly enforced. This is probably due to the fact that PSA results have exceeded the safety goals during most of the time since they were defined. In consequence, a graded approach similar to ALARP has been implicitly applied, i.e., the IAEA safety goal for existing plants, i.e., CDF = 10^{-4} per year has been seen as a limit, while the internal utility safety goal of CDF = 10^{-5} per year has been the target. In Finland, the internal safety goals for operating plants are informal and can also be interpreted as targets rather than limits.

From the regulatory perspective, quantitative safety goals are not strictly applied for operating plants. Utilities may define safety goals and the way they are applied. In the regulatory decision making, i.e., in risk-informed applications and plant modifications, decisions are made case by case. There is, however, a general regulatory requirement on continuous improvement of safety. Principally this means that risk increasing changes are not allowed even if the plant fulfils its safety goal. There is a need to clarify the role of this requirement relative to the role of numerical safety goals.

Since the 1990s, much focus has been on the development of various risk-informed applications, e.g., optimisation of allowed outage times, test intervals, and in-service-inspection programmes. The risk criteria used in these applications are typically based on risk importance measures and are application specific. With this approach, a sub-

optimisation will often be made in applications within the domain of the application specific risk control methods.

Goals related to CDF and unacceptable release are surrogates to societal risk level criteria. To fully validate these goals, calculations of environmental consequences of release sequences would need to be made. In a few countries, the performance of level 3 PSA:s is required, which includes this aspect. In Finland and Sweden, there are not yet plans to perform level 3 PSA:s. However, there is a need to discuss and define more precisely the safety goals related to radioactive release, as this is understood differently in different organisations.

Integration of deterministic and probabilistic criteria is still a problematic issue. These concepts seem difficult to integrate in practice and people often seem to be tuned to one or the other. Finding a correct balance between deterministic and probabilistic safety thinking has to do with the fundamental question of "how safe is safe enough?" and how to prove this safety level. It would be beneficial to discuss the relationships between deterministic and probabilistic criteria and their interpretation in illustrative cases. Fulfilment of defence-in-depth principle as well as criteria regarding redundancy, diversity and separation for various initiating event categories are examples of fundamental questions.

The final underlying obstacle in the use of safety goals are the uncertainties of PSA. Differences in the scope of PSA and different methods used in different parts of PSA makes it difficult to make consistent comparisons of risks. The only way to resolve the problem of uncertainties is to put emphasis on justification of the results and conclusions. This implies explicit presentation of claims, arguments and the underlying evidence, in order to convince the reviewer of the conclusions that the plant is safe enough. This is the so called safety case approach. How this approach is carried out with a full-scope PSA in relation to safety goals is a huge systems engineering exercise.

The second project phase aims at providing guidance for the resolution of some of the problems identified in the project and described above. In parallel, additional context information will be provided by extending the international overview and including experiences from other industrial areas. Thus, the main issues will be:

- Consistency in the usage of safety goals
  Addresses the problem of consistency of judgement in a situation when safety goals are applied to PSA results which change over time.
- Criteria when using PSA in support of deterministic safety analysis
  Probabilistic results will be used as decision input in a growing number of risk-informed applications, and criteria for the assessment of acceptability will be needed. Examples are the evaluation of safety margins or defence-in-depth.
- Criteria for assessment of results from PSA level 2
  There is a considerable spread in the safety goals for PSA level 2 used by different countries and organisations. Criteria are defined with respect to large and early releases, but both parameters are partly subjective. It will be tried to explore this issue more in depth.
- Overview of international safety goals and experiences from their use
  Reasonably full coverage in the overview desireable. This is mainly achieved by participation in the Safety Goals project in the OECD/NEA Working Group on

Risk Assessment (WGRisk), which will start in 2007. The results of phase 1 of the NKS/NPSAG project will be used in the planning of the scope and contents of the WGRisk project.

- Safety goals related to other man-made risks in society
  The aim of this activity is to provide perspective and present experiences from other areas with focus on transportation and offshore industry.

Insights from other on-going national and international research projects will be considered. In addition to the OECD/NEA project on safety goals mentioned above, this applies to an SKI project on using PSA in the assessment of defense in depth and to the ongoing EU programme SARNET (Severe accident research network).

6 References

ANSI/ANS-51.1-1983	ANS; Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants; ANSI/ANS-51.1-1983; ANS / American Nuclear Society; 1983
Bishop_SC	Bishop, P., Bloomfield, R.; A Methodology for Safety Case Development; Adelard;
Brown_1999	Brown, R.; Using soft data to make probabilistic risk assessments realistic; Brown_1999; George Mason University; 1999
CM-06-Fortum	Jänkälä, K.; Current PSA activities for Loviisa NPP; PSA Castle Meeting 2006-Fortum-PSA-status; FNS; 2006
CM-06-TVO	Himanen, R.; Current PSA activities TVO; PSA Castle Meeting 2006-TVO-PSA-status; TVO; 2006
Covello_RiskComp	Covello, V.T., Sandman, P.M., Slovic, P.; Risk Communication, Risk Statistics, and Risk Comparisons: A Manual for Plant Managers; Covello_RiskComp, Washington, DC: Chemical Manufacturers Association, 1988), pp. 16–22 http://www.psandman.com/articles/cma-
EON_2005_Fritiof	Fritiof, Lars; Safety Policy Nuclear Power E.ON Nordic / Säkerhetspolicy Kärnkraft E.ON Nordic; EON Nordic 2005; E.ON Nordic; 2005
EON_2005_Larsson	Larsson, Stig-Erik; E.ON Nordic Säkerhetspolicy för kärnkraft inkl. förklarande text; EON/ SKKÖT-050609-01; E.ON Kärnkraft Sverige AB; 2005
EUR_2002	EUR; European Utility Requirement for LWR Nuclear Power Plants; EUR European Utility Requirement for LWR Nuclear Power Plants; EUR; 2002
Farmer_1967	Farmer, F.R; Siting Criteria – a new approach; IAEA SM-89/34, 1967; reprinted in Nuclear Safety, 8 (1967) 539-48; 1967
Fishburn_1970	Fishburn, Peter.C.; Utility Theory for Decision Making; Fishburn, P.C., 1970. Wiley, New York. ISBN 0471260606; 1970
French_1986	French, S.; Decision theory: An Introduction to the Mathematics of Rationality; Frech, 1986, Ellis Horwood Limited, Chichester.; 1986
HMI_SAP_1992	HSE/NII; Safety Assessment Principles for Nuclear Plants; HMI_SAP_1992 ISBN0118836420; HSE/NII; 1992
HSK-R-100/d	HSK, Haubtabteil für Sicherheit der Kernanlagen (CH); Nachweis ausreichender Vorsorge gegen Störfälle in Kernkraftwerken (Störfall-Richtlinie); HSK-R-100/d; HSK; 2004
IAEA_CB-5	IAEA; Safety Evaluation of Operating Nuclear Power Plants Built to Earlier Standards – A Common Basis for Judgement (draft version of IAEA Safety Reports Series No. 12); IAEA CB 5 (draft version of IAEA Safety Reports Series No. 12); IAEA; 1996
IAEA_INSAG-10	IAEA; Defence in Depth in Nuclear Safety INSAG-10; IAEA Safety Series No. 75-INSAG-10. ISBN 92-0-103295-1; IAEA; 1996
IAEA_INSAG-12	IAEA; Basic Safety Principles for Nuclear Power Plants. 75-INSAG-3 Rev. 1. INSAG-12; IAEA Safety Series No. 75-INSAG-12. ISBN 92–0–102699–4; IAEA; 1999
IAEA_INSAG-3	IAEA; Basic Safety Principles for Nuclear Power Plants. 75-INSAG-3; IAEA Safety Series No. 75-INSAG-3; IAEA; 1988
IAEA_SRS_12	IAEA; Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards – A Common Basis for Judgement; IAEA Safety Reports Series No. 12, ISBN 92-0-104498-4; IAEA; 1998

IndDep_1183/81	Industridepartementet; Villkor för fortsatt tillstånd enligt 2 § atomenergilagen (1956:306) att driva atomreaktor; Industridepartementet 1183/81 1981-10-15; Industridepartementet; 1981
IndDep_2717/85	Industridepartementet; Villkor för fortsatt tillstånd enligt 5 § lagen (1984:3) om kärnteknisk verksamhet för att driva kärnkraftreaktorerna Oskarshamn I, II och III; Industridepartementet 2717/85 1986-02-27 (dossier 8523); Industridepartementet; 1986
Kahneman-Tversky	Kahneman, D., Tversky, A.; Prospect Theory: An Analysis of Decision under Risk; Prospect Theory: An Analysis of Decision under Risk, Econometrica, XVLII (1979), 263-291.; 1979
NED_185(1998)335	Vaurio, J.K.; Safety-related decision making at a nuclear power plant; Nuclear Engineering and Design 185 (1998) pp 335–345; Imatran Voima Oy, Loviisa Power Station; 1998
NED_93(1986)319	Paté-Cornell, M.E.; Probability and uncertainty in nuclear safety decision; Nuclear Engineering and Design,1986,93() pp 319-327; Standford University; 1986
NKA/RAS-490	Bengtsson, G (editor); Principles for decisions involving environmental and health risks; NKA Report Nord 1989:xx ISBN: 87-7303-363-4; NKS; 1990
NKA/SÄK-1	Dinsmore, Stephen (editor); PRA Uses and Techniques – A Nordic Perspective. Summary Report of the NKA Project SÄK-1, NKA Report, June 1985, ISBN 87-503-5539-2.; NKA SÄK-1; NKS; 1985
NKA_1989:91	Bengtsson, Gunnar (editor); Risk analysis and safety rationale. ISBN: 87-7303-364-2; NKA Report Nord 1989:91; NKS; 1989
NKA_1990:33	Laakso, Kari (editor); Optimization of Technical Specifications by Use of Probabilistic Methods – A Nordic Perspective. Final Report of the NKA Project RAS-450, NKA Report Nord 1990:33, May 1990, ISBN 87-7303-422-3.; NKA Report Nord 1990:33; NKS; 1990
NKA_1990:57	Hirschberg, Stefan (editor); Dependencies, Human Interactions and Uncertainties in Probabilistic Safety Assessment. Final Report of the NKA Project RAS-470, NKA Report Nord 1990:57, April 1990, ISBN 87-7303-445-1.; NKA Report Nord 1990:57; NKS; 1990
NKS(97)FR1	Andersson, Kjell (ed.); Strategies for Reactor Safety. Final report of the Nordic Nuclear Safety Research Project RAK-1; NKS(97)FR1. ISBN 87-7893-021-9; NKS; 1997
NKS-36	Holmberg, J., Pulkkinen, U.; Experience from the comparison of two PSA-studies; Report NKS:36, 2001. Nordisk kernesikkerhedsforskning NKS, Roskilde. ISBN 87-7893-087-1; NKS; 40
NKS-44	Holmberg, J-E, Pulkkinen, U., Rosqvist, T., Simola, K.; Decision criteria in PSA applications.; Report NKS:44, 2002. NKS Secretariat, Roskilde. ISBN 87-7893-097-9; NKS; 2002
NKS-60	Kjell Andersson, Britt-Marie Drottz Sjöberg, Kurt Lauridsen, Björn Wahlström; Nuclear Safety in Perspective. Final Report of the Nordic Nuclear Safety Research Project SOS-1; NKS-60. ISBN 87-7893-115-0; NKS; 2002
NKS-61	Simola, Kaisa (ed.); Advances in Operational Safety and Severe Accident Research; NKS-61. ISBN 87-7893-116-9; NKS; 2002
NUREG-0880	USNRC; Safety Goals for Nuclear Power Plants: A Discussion Paper," U.S. Nuclear Regulatory Commission, February 1982, (Rev. 1); NUREG-0880. Safety Goals for Nuclear Power Plants: A Discussion Paper," U.S. Nuclear Regulatory Commission, February 1982, (Rev
NUREG-1150	USNRC; Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants; NUREG-1150; USNRC; 1991

NUREG-1530	USNRC; Assessment of NRC's Dollar Per Person-Rem Conversion Factor Policy; NUREG-1530; USNRC; 1995
OKG_1996-00385	Gunnarsson, Kerstin; Mål och strategi för modernisering avseende reaktorsäkerhet av OKG:s kärnkraftblock; OKG/96-00385; OKG AB; 1997
OKG_2000-03886	Wretås, Ulrika; Test av ny princip för resultatpresentation; OKG Meddelande 2000-03886; OKG AB; 2000
OKG_2005-14190	Lindahl, Pär; Giltighet av probabilistiska säkerhetsmål; OKG/2005-14190; OKG AB; 2005
OKG_2006-09475	Lindahl, Pär; Metodbeskrivning för probabilistisk analys av rumshändelser med avseende på risken för härdskada/bränsleskada; OKG Anvisning 2006-09475; OKG AB; 14
OPB-88/97	; General Safety Regulations for NPPs (OPB-88/97), PN AE G-1-011-89; General Safety Regulations for NPPs (OPB-88/97), PN AE G-1-011-89; 1988
Prop 1980/81:90	Regeringen; Riktlinjer för energipolitiken; Regeringens proposition 1980/81:90; Regeringen; 1980
PSAM8-0162	Knochenhauer, M.; Holmberg, J.; Ingemarsson, I.; Hultqvist, G.; The Validity of Safety Goals; Proceedings of PSAM8 2006, paper 0162; -; 2006
RAB_1723490	Hultquist, Jan-Olof; Appelgren, Lars; VD-direktiv – Reaktorsäkerhet; RAB/ 1723490; Ringhals AB; 2006
RAB_1839723	Jonsson, Dick; Hansson, Åke; VDD-tillämpning – Övergripande mål och förhållningssätt för Reaktorsäkerhet; RAB/ 1839723; Ringhals AB; 2004
RAB_950227045	Vattenfall; Policy för kärnkraftsäkerhet inom affärsområde elproduktion; RAB_950227045; Vattenfall; 1992
RAB_990714068	Jonsson, Dick; Appelgren, Lars; Fackområdesdirektiv – Reaktorsäkerhet; RAB/ 990714068; Ringhals AB; 2006
RESS_36(1992)23	Knochenhauer, M; Hirschberg S; Probabilistically Based Decision Support; Reliability Engineering and System Safety 36 (1992) pp. 23-28; ABB Atom; 1992
RESS_54(1996)91	Apostolakis, G., G. Soares, S. Kondo (eds.); Special Issue on Treatment of Aleatory and Epistemic Uncertainty; Reliability Engineering and System Safety 54 (2-3) pp 91-262.; 1996
RESS_61(1998)11	Vatn, J.; A discussion of the acceptable risk problem; Reliability Engineering and System Safety, Volume 61, Number 1, July 1998, pp. 11-19(9); Norwegian University of Science and Technology; 1998
RESS_61(1998)3	Aven, T., Pörn, K.; Expressing and interpreting the results of quantitative risk analyses. Review and discussion; Reliability Engineering and System Safety, Volume 61, Number 1, July 1998, pp. 3-10; 1998
RESS_75(2002)93	Apeland, S., Aven, T.,Nilsen, T.; Quantifying uncertainty under predictive, epistemic approach to risk analysis; Reliability Engineering and System Safety, Volume 75(2002), pp. 93-102; 2002
RESS_90(2005)15	Aven, T., Vinnem, J. E.; On the use of risk acceptance criteria in the offshore oil and gas industry; Reliability Engineering and System Safety 90 (2005) pp 15-24; University of Stavanger; 2005
RG_1.174	USNRC; An approach for using probabilistic risk assessment in risk-informed decisions in plant-specific changes to the licensing basis; Reg.Guide 1.174; USNRC; 2002
RG_1.175	USNRC; An Approach for Plant-Specific, Risk-Informed Decision making: In-service Testing (ML003740149) (Issued with SRP Chapter 3.9.7) (Draft DG-1062, ML003739158, issued 06/1997); Reg.Guide 1.175; USNRC; 1998

RG_1.176	USNRC; An Approach for Plant-Specific, Risk-Informed Decision making: Graded Quality Assurance (ML003740172) (Draft DG-1064 , ML003739212, issued 06/1997); Reg.Guide 1.176; USNRC; 1998
RG_1.177	USNRC; An Approach for Plant-Specific, Risk-Informed Decision making: Technical Specifications (ML003740176) (Issued with SRP Chapter 16.1) (Draft DG-1065, ML003739150, issued 06/1997); Reg.Guide 1.177; USNRC; 1998
RG_1.178	USNRC; An Approach for Plant-Specific Risk-Informed Decision making for In-service Inspection of Piping (9/98, ML003740181) (Issued with SRP Chapter 3.9.8) (Draft DG-1063, ML003739154, issued 10/1997) (Revision 1, ML032510128, issued 09/2003) (SRP, ML03251
RiskAnal 94 983-991	Holmberg, J., Pulkkinen, U., Pörn, K. & Shen, K.; Risk decision making in operational safety management – experience from the Nordic benchmark study; Risk Analysis Vol. 14, No. 6 (1994) 983–991.; 1994
SG_Semin_2006	Holmberg, J; Knochenhauer, M; Project Seminar NKS Project ”The Validity of Safety Goals”; Thursday November 16, 2006; Relcon MoM 2005126-P-20061116; VTT / Relcon; 2006
SK_1995_Ahlström	Ahlström, Göran; Sydkrafts säkerhetspolicy Kärnkraft; Sydkraft 1995_Ahlström; Sydkraft; 1995
SKI_1994:2	Johansson, G. and Holmberg, J (editors); Safety Evaluation by Living PSA – Procedures and Applications for Planning of Operational Activities and Analysis of Operating Experience. SKI Technical Report 94:2, NKS/SIK-1(93)16, January 1994, ISSN 1104-1374.;
SKI_1996:40	Knochenhauer, Michael; Status and Use of PSA in Sweden; SKI Technical Report 1996:40; Impera-K AB; 1996
SKI_1997:49	Knochenhauer, Michael ; Angner, Anders ; Gunnarsson; Kerstin ; Gunsell, Lars ; Karlsson, Christer ; Wilson, Dan; Resultatpresentation och resultattolkning vid probabilistisk analys av yttre händelser; SKI Technical Report 1997:49; SKI; 1997
SKI_2003:48	Hallman, Anders; Nyman, Ralph; Knochenhauer, Michael; Tillsynshandbok PSA (PSA Review Handbook); SKI Technical Report 2003:48; SKI; 2003
SKI_ASAR80	SKI; ASAR 80, the First Round of Periodic Safety Reviews in Sweden; SKI ASAR 80 – brev; SKI;
SKI_ASAR90	SKI; ASAR 90, the Second Round of Periodic Safety Reviews in Sweden; SKI ASAR 90 – brev; SKI;
SKI_SSI_1985	SKI / SSI; Utsläppsbegränsande åtgärder vid svåra härdhaverier; SKI ref 7.1.24 1082/85; SKI / SSI; 1985
SKIFS 2004:1	SKI; The Swedish Nuclear Power Inspectorate’s Regulations concerning Safety in Nuclear Facilities; SKIFS 2004:1; SKI; 2004
SKIFS 2004:2	SKI; The Swedish Nuclear Power Inspectorate’s Regulations concerning the Design and Construction of Nuclear Power Reactors; SKIFS 2004:2; SKI; 2004
Slovakia-2005	The Nuclear Regulatory Authority of Slovak Republic (UJD),; Application of PSA Methodology in the Regulatory Process; UJD, BNS I.4.2/2005, Bratislava, Slovakia, 2005; UJD; 2005
SOU 1979:86	-; Reaktorsäkerhetsutredningen "Säker kärnkraft?" (Final report from the Reactor Safety Investigation, in Swedish),; SOU 1979:86; -; 1979
STUK_YVL-2.8	STUK; Probabilistic safety analysis in safety management of nuclear power plants; Guide YVL-2.8. ISBN 951-712-786-3; STUK; 2003

STUK_YVL-2.8-1987	STUK; Probabilistic safety analysis in safety management of nuclear power plants; Guide YVL-2.8.; STUK; 1987
STUK_YVL-2.8-1996	STUK; Probabilistic safety analysis in safety management of nuclear power plants; Guide YVL-2.8; STUK; 1996
STUK-YTO-TR 61	Holmberg, J., Pulkkinen, U.; Regulatory decision making by decision analysis; STUK-YTO-TR 61; STUK; 1993
SV_KSÄK_2006	Vattenfall; Vattenfalls policy för kärnkraftsäkerhet; Vattenfall_Kärnkraftsäk_2006; Vattenfall; 2006
SV_PK 301:1	Vattenfall; Koncernpolicy Vattenfall / P-riktlinjer Reaktorsäkerhet; Vattenfall company policy PK 301:1; Vattenfall; 1990
TVO-PSA-ohje	Pesonen, J.; OL1 ja OLl2 – todennäköisyysperustaisen turvallisuusanalyysin (PSA) käyttö ja ajan tasalla pitäminen; O-PSA-OHJE(1.2), ASKI 101320, v. 2.0; TVO; 2006
USNRC SECY-01-0009	USNRC; Modified Reactor Safety Goal Policy Statement; USNRC SECY-01-0009; USNRC; 2001
WASH-1400	USNRC; Reactor safety study : an assessment of accident risks in U.S. commercial nu-clear power plants; WASH-1400 / NUREG-75/01; USNRC; 1975
Vaurio_NKS-99	Vaurio, J.K.; Risk-informed decision making at Loviisa NPP; Proceedings of the NKS/SOS-2 Seminar on Risk Informed Principles. Bergendal,Sweden, 13 – 14 April 1999. Ed. U. Pulkkinen and K. Simola. Nordic Nuclear Safety Research (NKS).NKS-6, ISBN 87-7893-05
VGX-0003-01	VGX; Konstruktionsstyrande säkerhetsprinciper och krav för svenska kärnkraftreaktorer; VGX-0003-01; VGX, Värnamogruppens expertgrupp; 2000
VnP 395/1991	The Council of State, Finland; Decision of the Council of State on the general regulations for the safety of nuclear power plants; Finnish Government Resolution (395/1991); The Council of State, Finland; 1991
VROM-1988	VROM; Omgaan met Risico's (Dealing with risks); Nationaal Milieubeleidsplan; VROM, Den Haag, 1988.; 1988
VTT Publ 146	Holmberg, J., Johanson, G., Niemelä I.; Risk measures in living probabilistic safety assessment; VTT Publications 146; VTT; 1993
YE-asetus 161/1988	Nuclear Energy Decree (161/1988); Nuclear Energy Decree (161/1988); The Council of State, Finland; 1988
YE-laki 990/87	Nuclear Energy Act (990/87); Nuclear Energy Act (990/87); The Council of State, Finland; 1987
YVL-review	Wahlström, B., Sairanen, R.; Views on the Finnish nuclear regulatory guides; http://www.stuk.fi/english/convention/yvl-review.html; VTT; 2001

7 Acronyms and Abbreviations

ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
ASAR	As-operated Safety Analysis Report
BDBA	Beyond Design Basis Accident (Severe Accident)
BSL	Basic Safety Limit
BSO	Basic Safety Objective
BWR	Boiling water reactor
CANDU	CANada Deuterium Uranium, a pressurized heavy water reactor
CDF	Core damage frequency
CEU	Comprehensive uncertainty evaluation
DBA	Design Basis Accident
DID	Defence-in-depth
DSA	Deterministic Safety Analysis
HSE	Health and Safety Executive (UK)
IAEA	International Atomic Energy Agency
LERF	Large early release frequency
LPSA	Living PSA
NEA	Nuclear Energy Agency of OECD
NII	Nuclear Installations Inspectorate
NKA	Nordic liaison committee for atomic energy (now NKS)
NKS	Nordic nuclear safety research
NPP	Nuclear power plant
NPSAG	Nordic PSA Group
OECD	Organisation for Economic Co-operation and Development
PSA	Probabilistic safety assessment
PWR	Pressurised-water reactor
ROAAM	Risk Oriented Accident Analysis Methodology
RPS	Reactor protection system
RSU	Reactor safety investigation (Reaktorsäkerhetsstudien)
SAR	Safety Analysis Report
SARNET	Severe accident research network (EU programme)
SIL	Safety integrity level
SKI	Swedish Power Nuclear Inspectorate (Statens kärnkraftinspektion)
SSI	The Swedish Radiation Protection Authority (Statens strålskyddsinstitut)

STUK	Radiation and Nuclear Safety Authority of Finland (Säteilyturvakeskus)
TMI	Three Mile Island NPP
TVO	Teollisuuden Voima Oy
U.S.NRC	United States Nuclear Regulatory Commission
VGX	Värnamogruppens expert group
VTT	Technical Research Centre of Finland
WG	Working Group (of OECD/NEA)

Attachment 1 Interviews and interview questions

This attachment includes the list of people interviewed within the project and presentes the list of questions used in the interviews.

The following interviews were made:

Sweden

Lars Thuring	EON Energy Trading (previously Barsebäck NPP)
Mauritz Gärdinge	OKG (Oskarshamn NPP)
Lars Fredlund	Ringhals AB
Lennart Carlsson	Swedish Nuclear Power Inspectorate (SKI)
Lars Gunsell	Swedish Nuclear Power Inspectorate (SKI)
Karl-Fredrik Ingemarsson	Vattenfall Nordic Generation
Yngve Flodin	Vattenfall Power Consultant
Nils Olov Jonsson	Westinghouse Electric Sweden
Tomas Öhlin	Westinghouse Electric Sweden

Finland

Kalle Jänkälä	Fortum Nuclear Services
Mika Yli-Kauhaluoma	Fortum (Loviisa NPP)
Jussi Vaurio	Consultant (previously Fortum, Loviisa NPP)
Reino Virolainen	Radiation and Nuclear Safety Authority of Finland (STUK)
Jorma Sandberg	Radiation and Nuclear Safety Authority of Finland (STUK)
Risto Himanen	Teollisuuden Voima Oy (TVO)

International

Gennady Tokmachev	Atomenergoprojekt Russia
Hermann Fabian	AREVA NP, Germany
Gheorghe Raducu	CNSC-CCSN, Canada
Charles Shepherd	HSE NII, Great Britain
Jörn Vatn	Norwegian University of Science and Technology (NTNU)
Terje Aven and Jan Erik Vinnem	University of Stavanger, Norway
Karl-Erik Sundvall	Bombardier Transportation Signal AB, Sweden

General Questions (used in international interviews)

Question

1. What is your general opinion regarding the use of probabilistic safety goals for activities that involve man-made risks?
2. Why should safety goals be used?
3. What should be the main aim with using safety goals?
   Examples: design optimisation, protection of individuals or surroundings, protection of investment, etc.
4. What needs to be considered when defining a safety goal?
   What should be the basis for the numerical value, what issues need to be considered, what is suitable level of detail, etc.?
5. What should be the procedure for applying safety goals ?
   How, when and by whom?
6. How should deviations from safety goals (exceedance) be handled?

Questions Regarding Specific Safety Goals (used in alla interviews)

Question

1. Questions regarding present PSA safety goals and how they are used (or viewed) in your organisation:
   a. How are the PSA safety goals that are applied within your organisation defined?
   b. What is the definition of the subject of the safety goal?
      E.g., what exactly is meant by "core damage", "large release", etc.?
   c. What was the basis for defining the actual numerical levels used in the safety goals?
   d. Are there any additional criteria, e.g., regarding uniformity of risk profile?
   e. What is the role of the safety goals as a decision criterion? *Mandatory, trade-off possibility, just a target, etc.*
   f. What is the procedure for applying the safety goals to PSA results?
   g. What is the procedure (or additional criteria) for judging deviations from the safety goals?
2. Which organizations (or other internal and external parties) were involved in defining the goals and what was the process like that lead to the formulation of the goals?
3. What is (has been) the influence of the safety goals?
   E.g., on decision making, safety management, communication/negotiation between utility and authority, analysis quality, etc.
4. Do you see development needs in safety goals?
   E.g., regarding definition and usage.
5. Do you have any specific expectations for this project?

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se