nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-172
ISBN 978-87-7893-238-9

Probabilistic Safety Goals. Phase 2 - Status Report

Jan-Erik Holmberg, Kim Björkman and Jukka Rossi
VTT, Finland

Michael Knochenhauer, Xuhong He, Anders Persson and Helena Gustavsson
Relcon Scandpower AB, Sweden

July 2008

Abstract

The second phase of the project, the outcome of which is described in this project report has mainly dealt with four issues:

- Consistency in the usage of safety goals
- Criteria for assessment of results from PSA level 2
- Overview of international safety goals and experiences from their use
- Safety goals related to other man-made risks in society

Consistency in judgement over time has been perceived to be one of the main problems in the usage of safety goals. Safety goals defined in the 80ies were met in the beginning with PSA:s performed to the standards of that time, i.e., by PSA:s that were quite limited in scope and level of detail compared to today's state of the art. This issue was investigated by performing a comparative review was performed of three generations of the same PSA, focusing on the impact from changes over time in component failure data, IE frequency, and modelling of the plant, including plant changes and changes in success criteria. It proved to be very time-consuming and in some cases next to impossible to correctly identify the basic causes for changes in PSA results. A multitude of different sub-causes turned out to combined and difficult to differentiate. Thus, rigorous book-keeping is needed in order to keep track of how and why PSA results change. This is especially important in order to differentiate "real" differences due to plant changes and updated component and IE data from differences that are due to general PSA development (scope, level of detail, modelling issues).

Key words

Safety Goals, PSA, Safety Targets, ALARP, Decision criteria, Risk informed decision making

NKS-172
ISBN 978-87-7893-238-9

Electronic report, July 2008

The report can be obtained from
NKS Secretariat
NKS-776
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@nks.org

Probabilistic Safety Goals

Phase 2 Status Report

Jan-Erik Holmberg, Kim Björkman, Jukka Rossi[1]
Michael Knochenhauer, Xuhong He, Anders Persson, Helena Gustavsson [2]

[1]VTT, P.O.Box 1000, FI-02044 VTT, Finland
[2]Relcon Scandpower AB, SE-172 25 Sundbyberg, Sweden

April 2008

Table of contents

ATTACHMENT 1. LEVEL 2 AND 3 PSA CRITERIA USED BY DIFFERENT ORGANISATIONS 1

Tables

Figures

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
CENELEC	Comité Européen de Normalisation Electrotechnique
CEU	Comprehensive uncertainty evaluation
CSM	Common Safety Methods
CST	Common Safety Targets
DB AG	Deutsche Bahn AG (German National Railway Company)
DBA	Design Basis Accident
DID	Defence-in-depth
DSA	Deterministic Safety Analysis
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
ESROG	ERTMS Safety Requirements & Objectives Group
ETCS	European Train Control System
F/N	Frequency / Number of fatalities
FAR	Fatal Accident Rate (fatalities / 10^8 exposed hours)
FTA	Fault Tree Analysis
GAMAB/ GAME	Globalement Au Moins Aussi Bon/Globalement Au Moins Equivalent (Globally at least as good)
GSM-R	Global System for Mobile communications - Railway
HSE	Health and Safety Executive (UK)
IAEA	International Atomic Energy Agency
LERF	Large early release frequency
LPSA	Living PSA
MEM	Minimum Endogenous Mortality
NEA	Nuclear Energy Agency of OECD
NII	Nuclear Installations Inspectorate

NKA	Nordic liaison committee for atomic energy (now NKS)
NKS	Nordic nuclear safety research
NPD	Norwegian Petroleum Directorate
NPP	Nuclear power plant
NPSAG	Nordic PSA Group
OECD	Organisation for Economic Co-operation and Development
PRT	Public Rapid Transport
PSA	Probabilistic safety assessment
PWR	Pressurised water reactor
RAC	Risk Acceptance Criteria
RBC	Radio Block Central
RPS	Reactor protection system
RSU	Reactor safety investigation (Reaktorsäkerhetsstudien)
SAR	Safety Analysis Report
SARNET	Severe accident research network (EU programme)
SIL	Safety integrity level
SIL	Safety Integrity Level
SKI	Swedish Power Nuclear Inspectorate (Statens kärnkraftinspektion)
SNCF	Société Nationale des Chemins de fer Français (French National Railway Company)
SSI	The Swedish Radiation Protection Authority (Statens strålskyddsinstitut)
STUK	Radiation and Nuclear Safety Authority of Finland (Säteilyturvakeskus)
THR	Tolerable Hazard Rate
TIRF	tolerable individual risk of fatality
TRI	Temporary refuge integrity
TSI	Technical Specification for Interoperability
TVO	Teollisuuden Voima Oy
U.S.NRC	United States Nuclear Regulatory Commission
UE	Undesirable event
UNISIG	Union Industry of Signalling
VTT	Technical Research Centre of Finland
WG	Working Group (of OECD/NEA)

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.

The first phase of the project provided a general description of the issue of probabilistic safety goals for nuclear power plants, of important concepts related to the definition and application of safety goals, and of experiences in Finland and Sweden.

The second phase has been more concerned with providing guidance related to the resolution of some of the problems identified. In parallel, additional context information has been provided. This was achieved by extending the international overview by contributing to and benefiting from a new activity related to Safety Goals which was initiated in late 2006 within the OECD/NEA Working Group Risk.

The recently initiated third and last project phase will, to some extent, consist in the continuation of activities initiated during phase 2. This is mainly the case for the international overview (OECD/NEA WGRisk task on safety criteria). In addition, focus will specifically be put on exploring more in detail the relationship between different levels of criteria, and on the utilisation of numerical criteria when using probabilistic analyses in support of deterministic safety analysis. Finally, general guidance will be provided – on the basis of project experiences – concerning the formulation, application and interpretation of probabilistic criteria.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

The work has been financed by NKS (Nordic nuclear safety research) and the members of NPSAG (Nordic PSA Group) and SAFIR2010 (The Finnish Research Programme on Nuclear Power Plant Safety 2007–2010).

1 Introduction

1.1 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 With the aim to discuss and document current views, mainly in Finland and Sweden, on the use of safety goals, including both benefits and problems. The work has clarified the basis for the evolvement of safety goals for nuclear power plants in Sweden and Finland and of experiences gained. This was achieved by performing a rather extensive series of detailed interviews with persons who are or have been involved in the formulation and application of the safety goals. At the end of phase 1, a project report was issued by NKS [NKS-153], and in parallel as an SKI research report (SKI 2007:06). The report presents the project context and a background to safety goal, as well as a historical review describing reasons for defining safety goals, context of goals and experiences. A number of specific issues related to the definition, interpretation and use of probabilistic safety goals were also identified and discussed.

The basic aim of phase 2 has been to increase the scope and level of detail of the project. Based on the conclusions from the first project phase, the following issues were selected for analysis:

- Consistency in the usage of safety goals (finalised during phase 2).
- Numerical criteria when using probabilistic analyses in support of deterministic safety analysis (to be finalised during phase 3).
- Criteria for assessment of results from PSA level 2, including relations to criteria for off-site consequences (finalised during phase 2).
- Addition of a more systematic overview of international safety goals and experiences from their use, including participation in new OECD/NEA WGRisk activity (continued during phase 3).
- Safety goals related to other man-made risks in society, with focus on railway industry and oil and gas (finalised during phase 2).

The results of this project phase was presented at a project seminar in Stockholm in November 2007 [SG_Semin_2007]. The project has also been presented with two papers at PSAM 9, an international conference on Probabilistic Safety and Management [PSAM9-0428 and PSAM9-0443].

This document includes the following parts:

Chapter 1. Introduction
Background; Aim and scope.

Chapter 2. Consistency in the usage of the safety goals
Handling of variations; Consistency over time (for same plant); Consistency between plants.

Chapter 3. Numerical criteria when using probabilistic analyses in support of deterministic safety analysis

Initial description of some activities dealing with the relationship between the levels of defence in depth and PSA or other probabilistic analyses.

Chapter 4. Criteria for assessment of results from PSA level 2

Background to the issue; International overview; Comparison of criteria in level 2 and level 3 PSA, with reference to the Finnish criteria for large release.

Chapter 5. Extension of overview of international safety goals and experiences from their use

Overview of the status within the activity conducted within the OECD/NEA Working Group Risk.

Chapter 6. Safety goals related to other man-made risks in society

Summary of safety goals used in non-nuclear context, with specific focus on safety goals in the areas railway signalling and offshore oil and gas.

Chapter 7. Conclusions

Conclusions, including a summary of planned activities for phase 3 of the project.

2 Consistency in the usage of safety goals

An important issue when dealing with safety criteria is the problem of consistency of judgement in a situation when safety goals are applied to PSA results which change over time, or which are made up of contributors with major differences in uncertainties.

In an ideal situation, the PSA results for a nuclear power plant, e.g., expressed as the core damage frequency (CDF), would exactly mirror the actual safety level of the plant. If the safety is improved, the CDF would decrease, and if the plant safety deteriorates, the CDF increases. In such a situation, the comparison to a safety goal would also be rather uncomplicated.

In practice, it has turned out that there are a lot of challenges involved when attempting to define and make practical use of probabilistic safety criteria. Thus, in many cases changes in PSA results over time are due to scope extensions or increases of level of detail, which will lead to an increase of the frequency of the calculated risk measures (CDF or off-site release). Changes in success criteria, in plant specific data, and in analysis methods will also cause changes over time. This gradual extension and development of plant PSA models may lead to situations where safety goals are violated. The implications of such violations have been under discussion. The problem of consistency in judgement when applying safety goals can appear in two shapes:

- Consistency over time
  This is a situation where the same set of safety goals is applied to a specific plant at different points in time, and where the plant PSA has changed over time.
- Consistency between plants
  This is a situation where the same set of safety goals is applied to different plants. The problem is general, but becomes especially apparent for reactors of similar design.

2.1 Consistency over time

Consistency in judgement over time has been perceived to be one of the main problems in the usage of safety goals. Safety goals defined in the 80ies were met in the beginning with PSA:s performed to the standards of that time, i.e., by PSA:s that were quite limited in scope and level of detail compared to today's state of the art.

In order to investigate this issue more in detail, a comparative review was performed of three generations of the same PSA [Gustavsson_2007]. The PSA for Forsmark 1 was selected, i.e., a BWR of ASEA-Atom design commissioned in 1980. The PSA versions chosen were from the years 1994, 2000 and 2006. During these years, the PSA increased considerably in scope and level of detail. For this reason, the comparison was restricted to a scope (in terms of initiating events) corresponding to the 1994 PSA.

Figure 1 gives an impression of the development of the PSA over these years by presenting the total number of initiating events, fault trees and basic events in the PSA versions.

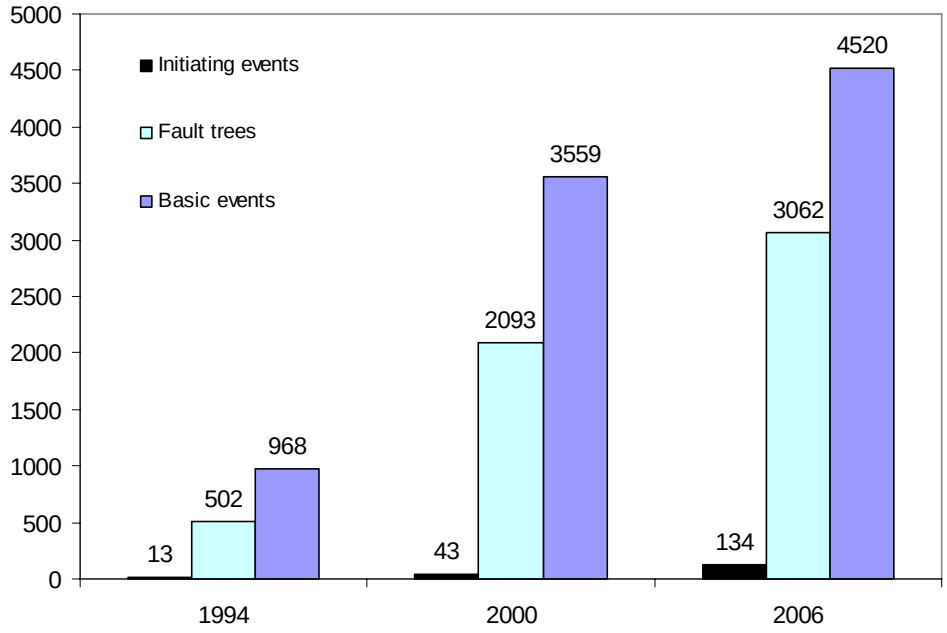

Figure 1. Scope of the Forsmark 1 PSA versions 1994, 2000 and 2006

Looking at the core damage frequency for the internal initiating events, it differed quite considerably over the years, exceeding the CDF safety goal (CDF < 10^{-5}/year) in 2000, but meeting it with a small margin in 1994 and 2006.

- 1994 $8{,}2 \cdot 10^{-6}$/year
- 2000 $2{,}4 \cdot 10^{-5}$/year
- 2006 $7{,}8 \cdot 10^{-6}$/year

If the CDF for years 2000 and 2006 were also to include initiating events that were not modelled in 1994, i.e., CCI events in 2000 and area events (internal fire and flooding) in 2006, the total CDF has been well above the safety goal all the time after 1994.

In order to try better to understand the reason for the changes, the following aspects were analysed:

- Cut-off in PSA quantification
- Changes in component failure data
- Changes in IE frequency
- Changes in conditional CDF (disregarding IE frequency)
- Changes in modelling of the plant, including plant changes and changes in success criteria

2.1.1 Cut-off in PSA quantification

Experiences from other PSA:s have shown that the selection of the absolute and relative cut off in the fault tree quantification can influence the results. A comparison of the PSA quantification results with original cut off and new cut off was performed using the absolute cut off 10^{-12} and the relative cut off 10^{-6}. In some cases this had a noticeable influence, especially for analysis cases with CDF results close to the cut-off limit. However, on total level the cut off only influence the CDF with less than 1 %.

2.1.2 Changes in component failure data

Component failure data are usually updated or changed between PSA generations, and this is an obvious potential cause for changes in total PSA results. In all versions of the Forsmark PSA, component failure data is derived from the T-book, i.e., the Nordic Reliability Data Book. Data was taken from different T-book versions (T-book 3, T-book 5 and T-book 6). In this study, no systematic comparison was made of all differences and their impact on total PSA results. However, data for a number of components were compared, and rather significant differences were found, as illustrated in Figure 2.

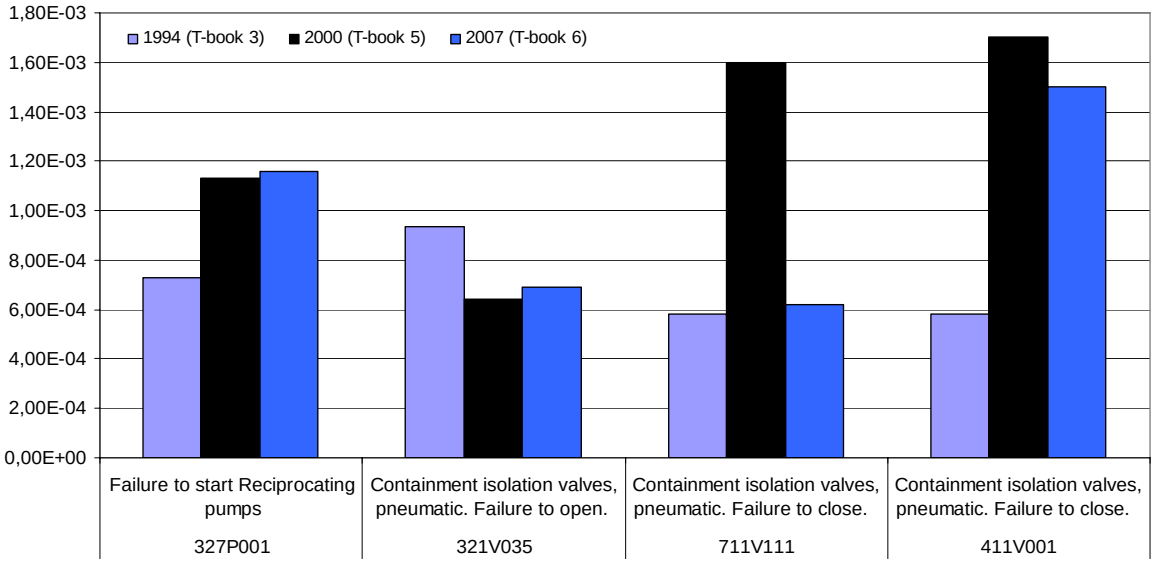

Figure 2. Some examples of changes in component failure data in T-book

2.1.3 Changes in IE frequency

The comparison basically included only transients and loss of coolant accidents (LOCA). Transient frequencies were largely determined by analysis of plant operating experiences (scram statistics), and differed only slightly between the years. The main impact was from the fact that a small part of the transients were modelled as CCI events in the 2000 and 2006 versions of the PSA, and that some of the CCI:s made large contributions to the total CDF. LOCA frequencies were assigned on the basis of WASH-1400 data in 1994. In 2000 and 2006 worldwide LOCA-experience data was used, leading to somewhat lower frequencies for LOCA compared to WASH-1400, at least for large LOCA. In addition, the PSA results differed considerably due to the fact that LOCA events were split up into an increasing amount of more and more detailed break locations, with more specific damage modelling. Finally, loss of external power had very differing total impact in the three PSA:s, due to the fact that the basis for modelling the event was different in the PSA:s.

2.1.4 Changes in conditional CDF

In order to eliminate the impact from differences in IE frequency, a comparison was made also of the conditional CDF for every group of initiating events. Large differences were identified in CCDF for the same IE group between the three PSA:s. In some cases this was due to data changes, but more important were basic changes in analysis

assumptions, such as success criteria for safety systems, or more realistic modelling of the impact of failures or of initiating events.

2.1.5 Conclusion

It proved to be very time-consuming and in some cases next to impossible to correctly identify the basic causes for changes in PSA results. A multitude of different sub-causes were combined and difficult to differentiate.

Thus, rigorous book-keeping is needed in order to keep track of how and why PSA results change. This is especially important in order to differentiate "real" differences due to plant changes and updated component and IE data from differences that are due to general PSA development (scope, level of detail, modelling issues). This requirement was not fulfilled for the analysed PSA, probably partly due to the fact that PSA as a technique was very quickly developing over the studied time period, and that the previous PSA version was always more or less considered to be a draft version of the PSA that was currently being developed.

2.2 Consistency between plants

It might reasonably be expected that PSA:s for identical reactor designs should produce roughly the same results, and that they should give the same conclusions if compared to identical safety goals. However, it has been found on several occasions, that PSA:s for twin plants belonging to different utilities and analysed by different PSA teams show very different results.

In order to investigate this issue more in detail, two PSA:s for nearly identical reactors units (Forsmark 3 and Oskarshamn 3) have been compared [NKS-36]. Two different analysis teams performed the PSA:s, and the analyses became quite different.

A major finding of the comparison study was that the two projects had different purposes and thus had different resources, scope and even methods. It was concluded that comparison of PSA results from different plants is normally not meaningful. It takes a very deep knowledge of the PSA:s to make a comparison of the results and usually one has to ensure that the compared studies have the same scope and are based on the same analysis methods. A PSA is an enormous mathematical model based on technical descriptions of systems, experience and data, interpretations of data, engineering judgements and use of various physical models. The analysis process is sensitive to many factors, not all controllable for the analysis team.

A PSA is never complete. There are always open issues and things that have been excluded that can have great influence on the quantitative estimate of the accident frequency. The results presented and conclusions drawn in one version can be changed in the next version. The history of the analysis and the status of the PSA programme of the plant should be known when reviewing the PSA.

If comparability is considered a desirable property of PSA, the methodology for performing PSA:s should be harmonised. This would also facilitate the review of the studies. Examples of areas for harmonisation are presentation of results, presentation of methods, scope, main limitations and assumptions, definitions for end states (core damage or release categories), definitions of initiating events, and definitions of common cause failures. Harmonisation should follow the experience from the use of studies and results from research and development work. Many real uncertainties can be

identified by comparing PSAs. Generally, comparisons can be recommended as a method to review the quality of a PSA-study and as a method to analyse the uncertainties of the study.

3 Numerical criteria when using probabilistic analyses in support of deterministic safety analysis

This activity is part of the third phase of the NKS project, and the results of this sub-activity are expected to include a presentation of important concepts, and a description of different ways to make use of PSA information for assessing deterministic safety, including status of defence in depth. Some initial information on the subject is given below.

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.

There are on-going activities both nationally and internationally in this field. As an example, the SKI has initiated a research activity related to using PSA information in the assessment of defence in depth. Furthermore, the IAEA has had some initial activities in the area of combining deterministic analysis and PSA, including a technical meeting in September 2006 [IAEA_TM2006].

The aim of the SKI initiated project is to develop methods for using PSA models and results in a way that allows assessment and ranking of the structures, systems, components and operating procedures that form the defence in depth of a nuclear power plant. This whole work is divided into five phases:

1. Mapping of conditions that should be considered for the defence in depth levels.
2. Definition of quantitative measures that should be considered for the defence in depth levels.
3. Method development and adaptation of PSA model.
4. Quantitative analyses.
5. Quantitative and qualitative safety assessment of identified aspects of defence in depth.

Results from the SKI project will be used in the continued development of this activity during phase 3 of the project.

IAEA:s INSAG-10 [IAEA_INSAG-10] guide outlines the general defence in depth principles and measures used to achieve adequate safety in nuclear power plants. The basic definitions of defence in depth (DID) levels are outlined in Table 1.

Table 1. Levels in defence in depth [IAEA_INSAG-10].

DID level	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

The objectives of different DID levels form a chain of consecutive barriers where an event sequence can be stopped to avoid more and more harmful consequences. This description of DID levels is straight-forward to associate with event sequence descriptions used in PSA context, since PSA is also structured in several levels with respect to consequences assessed. In level 1 PSA, the core damage risk is assessed. In level 2 PSA, the risk of radioactive release from the reactor containment is assessed and, in level 3 PSA, the environmental consequences are assessed.

The proceedings of the IAEA technical meeting [IAEA_TM2006] presents a simplified overview of the relationship between the levels of DID and PSA. Table 2 gives an overview of the identified relationships.

Table 2. Simplified overview of the connection between defence in depth levels 1 to 5 and the main elements of PSA levels 1 to 3 [IAEA_TM2006].

<table>
<tr><th>Level of defence in depth</th><th>Level of PSA</th></tr>
<tr><td rowspan="2">1. Prevention of abnormal operation and failures
2. Control of abnormal operation and detection of failures
3. Control of accidents within the design basis</td><td>1 Core damage
Identification of event sequences (initiating events) that may lead to core damage.
Analysis and modelling of the function and reliability of safety systems.
Calculation of core damage frequency.
Assessment of the balance between the frequencies and risk impacts of various initiating events, and of the corresponding barrier strengths.</td></tr>
<tr><td rowspan="2">4. Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents</td><td>2 Release of radioactive substances
Analysis of the occurrence and progression of a core melt within the reactor vessel.
Analysis of core melt behaviour in the containment.
Consideration of accident management systems and of mitigative accident management actions.
Assessment of the balance between the frequencies of various events, and of the corresponding strengths of barriers preventing release.
Calculation of frequency of release categories, i.e., classes of release of radioactive material to the environment</td></tr>
<tr><td rowspan="2">5. Mitigation of radiological consequences of significant releases of radioactive materials</td><td>3 Off-site consequences
Calculation of concentration and composition of the radio-active release at different times and distances from the release, and of the resulting radiation doses.
Assessment of resulting damages to life, health and property.
Calculation of the frequency of various categories of damage.
Assessment of the impact from severe accident management and off-site emergency preparedness measures.</td></tr>
</table>

4 Criteria for assessment of results from PSA level 2

4.1 Background

There is quite good consensus about the definition of a core damage, but 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 [IAEA_INSAG-3, IAEA_INSAG-12]. 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 it 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 addressed 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 mitigation, i.e., “0,1 % of an 1800 MWt core”, corresponding to a release of 100 TBq of Cs-137 [SKI_SSI_1985]. 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.

4.2 Comparison of international criteria

Level 2 and level 3 PSA criteria used by different international organisations are summarized in Attachment 1. There are several differences in the definition of these criteria between different countries. In Canada, Japan, Korea and USA both level 2 and level 3 criteria are specified. In other countries or organisations either level 2 criteria (Finland, Russia, Slovakia, Sweden, IAEA and EUR) or level 3 criterion (the Netherlands, UK) are specified. Criteria can be mandatory (in most cases for new plants or designs) or informal (in most cases for existing plants).

The release for which a numerical criterion is given is also defined in several different ways:

- Large release. This is defined either as absolute magnitude of activity and isotope released, e.g., 100 TBq of Cs-137 or as relative magnitude, e.g., 1 % of the core inventory of Cs-137.
- Large early release. These definitions are more qualitative, e.g., “Large off-site releases requiring short term off-site response,” “Significant, or large release of Cs -137, fission products before applying the offside protective measures,”

"Rapid, unmitigated large release of airborne fission products from the containment to the environment, resulting in the early death of more than 1 person or causing the severe social effect."

- Small release. CNSC from Canada has proposed a criterion both for large and small release. A small release is defined as a release of 1000 TBq of I-131.
- Unacceptable consequence. This is a French definition which is fully open. It should be noted the performance of level 2 PSA is not required in France by the safety authority.
- Containment failure. The Japanese Nuclear Safety Commission proposes a criterion for containment failure frequency. The first version of the Guide YVL-2.8 also defined a probabilistic criterion for containment isolation failure (conditional failure probability). This is a requirement that aims at assuring the robustness of the defence in depth.

Figure 3 summarises numerical criteria defined for large release. As explained above, the definitions for "large release" is not the same for all organisations. However, it can be seen that objectives vary from 10^{-7}/year to 10^{-5}/year, which is a quite large spread, larger than for core damage frequency, where objectives vary between 10^{-5}/year and 10^{-4}/year.

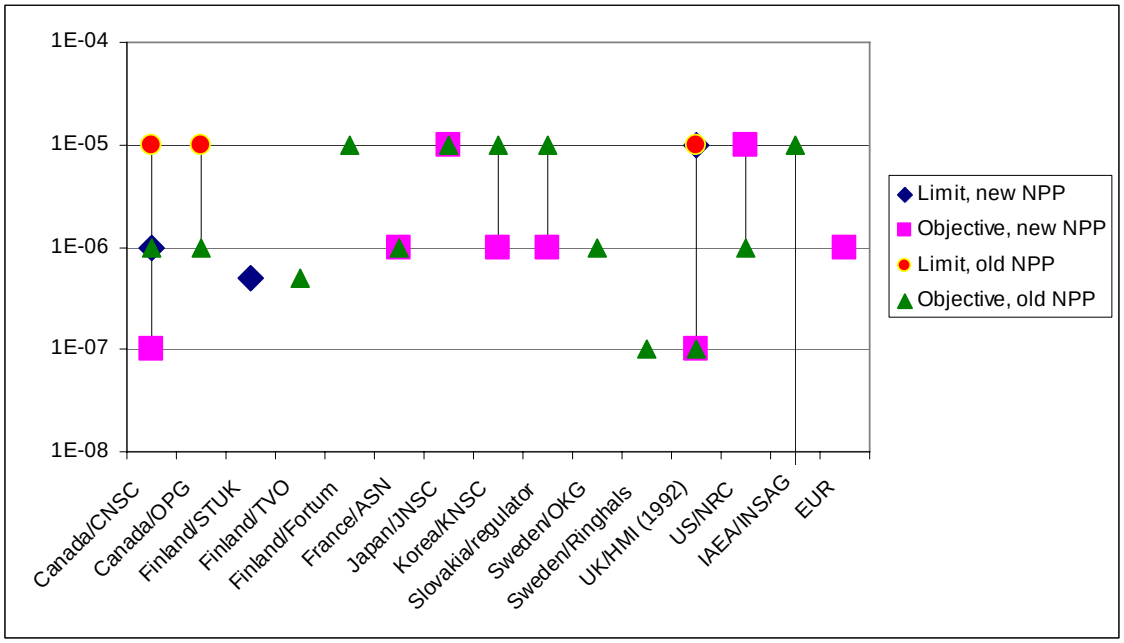

Figure 3. Numerical criteria defined for large release. Definition of "large release" varies (see Attachment 1).

Concerning level 3 there are differences in the definitions of criteria. However, risk is defined in a way or other as a health risk. Mostly risks are divided into fatal acute or fatal late health risks and these can be calculated for an individual or a group. In one case risk is defined as an average risk to members of the public in the vicinity of the site, this excludes the member of a critical group that receives maximum exposure from an accident.

Typically acute health effects have a threshold dose value under which the probability of health effect is zero, but above which the probability of acute health effect is increased with increasing dose. On the other hand most late health effects do not have

threshold values for dose. Based on these assumptions acute health effcets can be expected in the vicinity of the release point, whereas late health effects appear in the public exposed to radiation over larger areas.

4.3 Level 2 vs. level 3 criteria

4.3.1 Basis for comparison

If links between criteria at different levels of PSA are considered, a chain in consequences and associated probabilities should be seen. When transferred from level 1 towards level 3, consequences become more and more severe and probabilities are reduced. Level 2 criteria include probabilities of phenomena from a core damage to the release. This can be the probability of a containment failure or the probability of a sequence resulting in a direct release to the atmosphere. If finally level 3 is considered, criteria are often defined at the level of individual acute or latent fatality risk, making it possible to compare risk from a radioactive release with other risks occurring in normal life.

Level 3 criteria can be qualified in various ways. One is to relate the numerical value to other risks of society. Concerning individual risk of prompt or latent death, statistical data is generally available. This data is often divided into different categories, and in this case the number of premature deaths from accidents and from fatal cancers can be useful as a point of reference. These numbers can be changed to risk values. For example, in general accidental death for an individual is on the level of about 10^{-4} per year. With these numerical values available it needs to be decided how much less the risk from a radioactive release should be. Often the factor of 100 is used, resulting in the value of 10^{-6} per year, i.e., the safety goal for individual risk from radioactive release sould be 10^{-6} per year.

One of the most important factors affecting the off-site consequences is the prevailing weather conditions during the release and dispersion. By means of off-site consequence assessment, various consequences from radioactive releases can be calculated for different weather conditions. Figure 4 illustrates the variability in risk due to the weather, showing the individual risk (early fatality) calculated with a hypothetical level 3 PSA. The figure also shows the safety goal level as specified above.

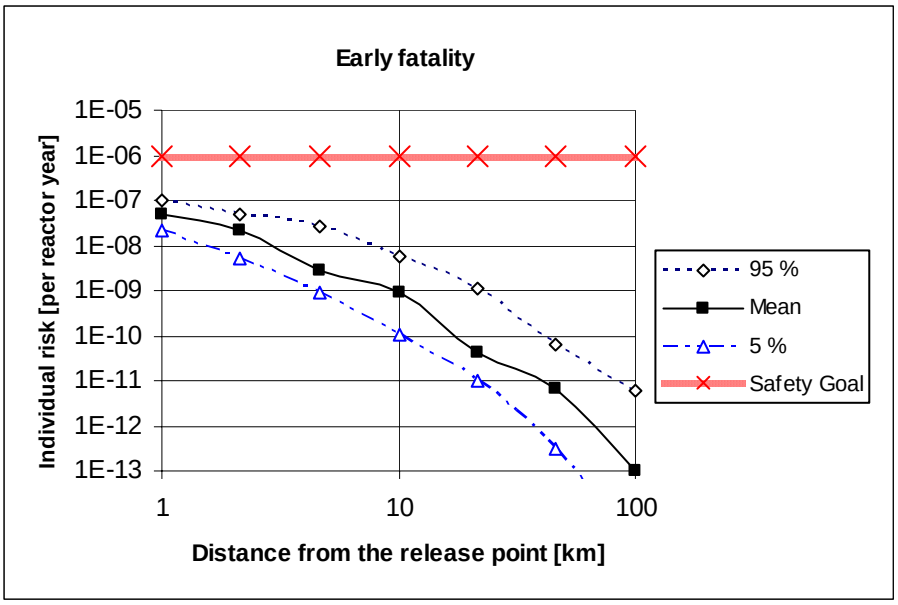

Figure 4. Individual risk of early fatality as a function of distance.

In this case, the effect of the weather variability is illustrated by the percentiles. In a probabilistic consequence model, the consequences are evaluated on an r, θ grid around the release point for each meteorological scenario. Probabilities of different weather sequences are based on on-site measured data. Weather fluctuation causes variation in the calculated risk with two orders of magnitude at most. Figure 4 also shows that in this hypothetical case, individual risk decreases when the distance is increased. The value of the safety goal is clearly at a higher level than the calculated risk values. It should be noticed that the frequency of the release determines the starting point level of the curves.

It is customary to sum up the consequences experienced at each r, θ grid point to show the total consequences observed in the population for each meteorological scenario. Often this is done by presenting the consequence magnitudes and their associated probabilities in the form of complementary cumulative distribution functions (CCDF). Examples from NUREG-1150 are shown in Figure 5.

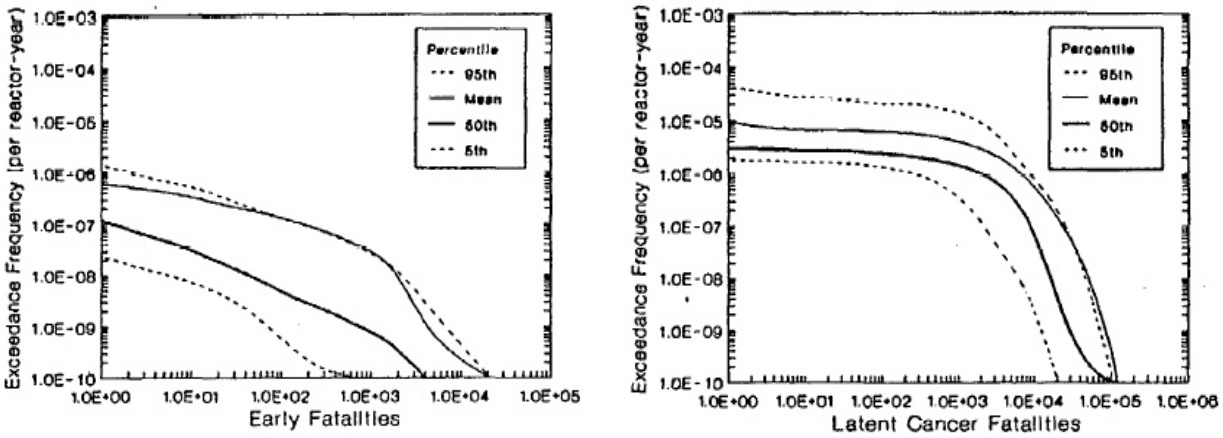

Figure 5. Examples of complementary cumulative distribution functions for early and late health effects from NUREG-1150 [USNRC 1990].

In addition to CCDF curves it is usual to produce expectation values and other percentile values for the CCDF. The expected value (mean) of the CCDF is the integral of the CCDF and it is often used as a summary measure of risk. Values of various percentiles can be obtained from the CCDF. For example in Figure 5 on the left hand side one early fatality would be exceeded in one out of two million releases (probability of $5 \cdot 10^{-7}$), but on the right hand side one latent cancer fatality would be exceeded in one out of 100 000 releases (probability of 10^{-5}), if the mean value is considered.

In addition to weather distribution, there are a number of other aspects that will affect the results, e.g., population distribution and eating habits. In addition, exploitation of countermeasures and other dose mitigating measures can reduce exposure.

Societal risk is often defined as the product of the accident frequency and the magnitude of consequences. If societal risk is considered based on Figure 5, it can be expected to remain very small.

4.3.2 Test application to Finnish site

In a test calculation with environmental data from a Finnish nuclear power plant site [Rossi_2007], the definition of a large release in the Finnish Government Resolution is used as the reference release [VnP 395/1991]. According to the Government Resolution it is required that neither acute harmful health effects nor long-term restrictions for usage of extensive land or water areas in the environment of the nuclear power plant shall be caused by the radioactive release after a severe nuclear power plant accident. Concerning the long-term requirement, the release limit of 100 TBq is assigned for the Cs-137 isotope. In addition it is defined that the combined fallout of other released nuclides shall not cause greater hazard in the long-term, starting three months after the accident, than the defined maximum cesium release. In the Finnish regulatory guide for PSA, YVL Guide 2.8, the numerical objective for a large release is set to $5 \cdot 10^{-7}$/year [STUK_YVL-2.8].

Concerning the release limit of 100 TBq for the Cs-137 isotope, no acute health effects would be expected, but statistical late health effects could be caused. In reality, radiation protection measures both in the early and late phase would certainly be initiated in order to reduce the collective dose, but these measures are assumed not to be applied in this study.

In the following paragraphs, off-site consequences from the reference release are elucidated by calculating various key figures [STUK_YVL-7.2]. Focus is on the assessment of doses and health effects from prolonged exposure. Doses can be converted to late health effects by applying dose response functions.

The exposure pathways considered here are direct external radiation from the fallout (groundshine), and ingestion dose pathways (cow's milk and meat). In addition, inhalation and external radiation from the plume (cloudshine) were included in some calculations to elucidate their significance in long-term exposure. In the ingestion model, Nordic cultivation methods are taken into account in addition to summer-winter seasonal variation. Consumption of berries, mushrooms, game or fish are not considered.

Local shielding conditions are assumed, ingestion rates are taken from the BIOMOVS project[1]. The release altitude is 20 m and the release duration is 1 hour. Dispersion calculations are carried out in different weather conditions measured at the site, and results are weighed with the annual statistical distribution of the conditions [Ilvonen_1994].

4.3.3 Results from the test application

Figure 6 presents individual doses from the reference release of the cesium isotopes. 100 TBq Cs-137 release implies release of other cesium isotopes, which can be scaled in the ratio of the reactor inventory. In this case, the release magnitude of Cs-134 is 148 TBq and it is included in the calculations and the source term is known here as the reference source term or release.

It is concluded that exposure from groundshine is the dominant dose component. The dose from inhalation is one order of magnitude lower than from groundshine, and from cloudshine four orders of magnitude lower. The expectation value of groundshine decreases from 10 mSv to 0,3 mSv along a distance change from 1 to 10 km. The corresponding maximum values change from 100 mSv to 1 mSv.

Expectation values were found not to exceed the ICRP Publication 82's limit value of 10 mSv, but the maximum values exceed this limit value as far as 3 km's distance from the point of release [ICRP_82]. Considering the IAEA's criterion for terminating temporary relocation (set to 10 mSv/month), this criterion would be exceeded even at the distance of 1 km [IAEA_GS-R-2].

[1] BIOMOVS (Biospheric Model Valuation Study) is an international cooperative effort to test models designed to quantify the transfer and accumulation of radionuclides and other trace substances in the environment.

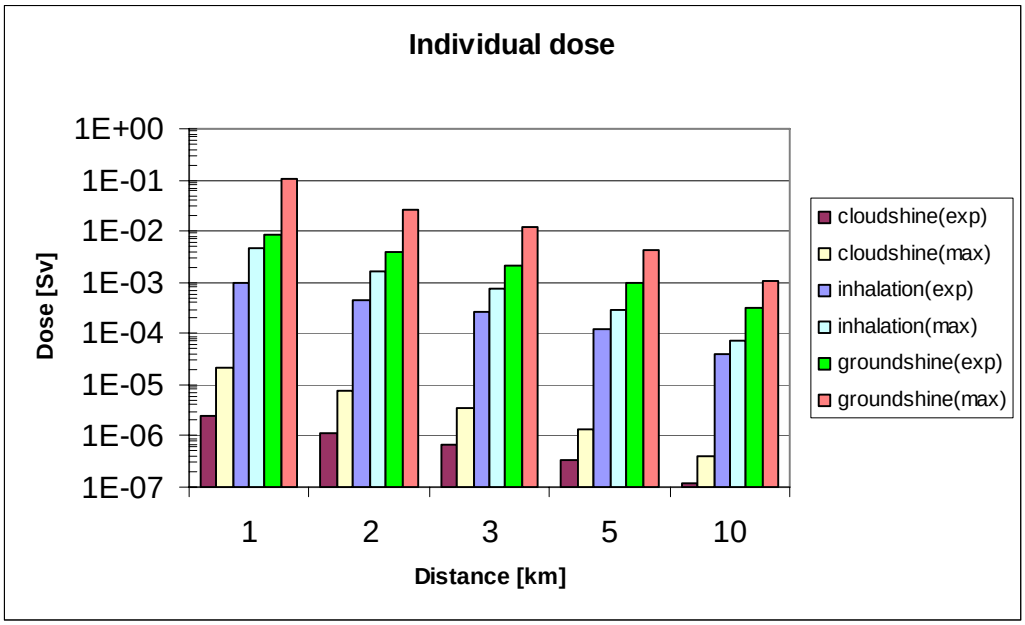

Figure 6. Individual dose caused by the reference release (100 TBq Cs-137 and 148 TBq Cs-134) at the Olkiluoto site.

Only the important ingestion dose pathways from cow's milk and meat are considered here. Due to seasonal variations, results are calculated and presented separately for deposition occurring during the growing and pasturing season and for deposition during the period outside the growing season.

In the analysis, it is assumed that the agricultural production is consumed at the place of cultivation without distribution or mixing with fresh food. Figure 7 illustrates that there is a difference by an order of magnitude in the values if deposition occurs during the growing season or not. The expected values of the dose from cow's milk and meat at the distance of 1 km are in the interval of 100 to 200 mSv. Doses decrease with increasing distance so that at the distance of 10 km the dose values are about two orders of magnitude lower. The expectation value from cow's milk, as well as the maximum value from cow's meat, still reach 10 mSv

Because the first year's dose dominates the ingestion dose during long-term exposure, it is obvious that a food ban would be enforced to avoid or at least reduce exposure.

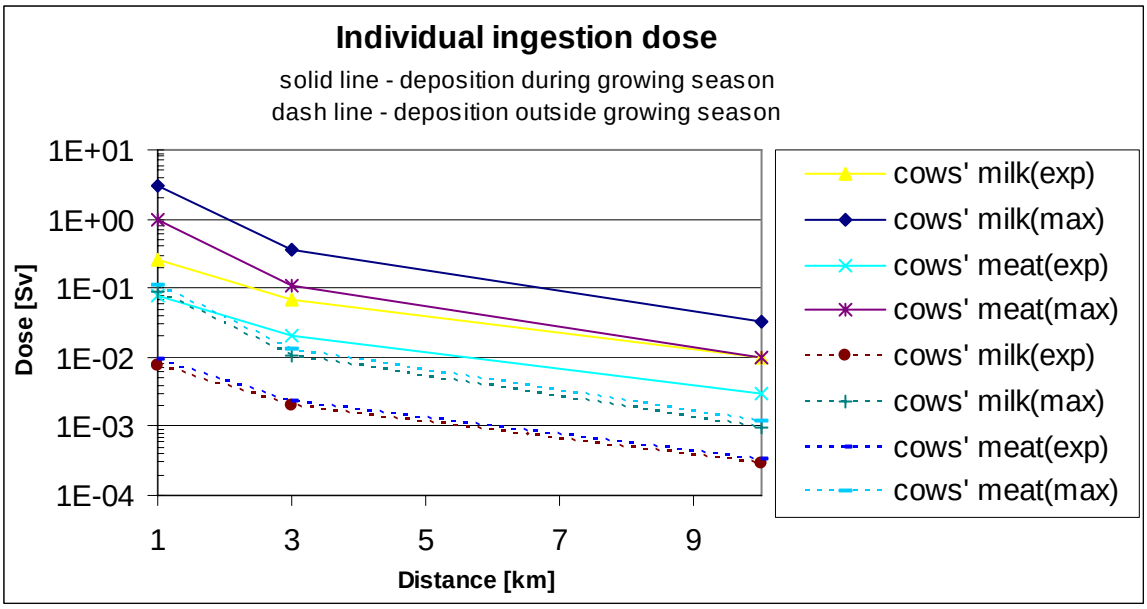

Figure 7. Individual ingestion dose caused by the reference release at the Olkiluoto site.

Contamination areas based on different dose criteria are presented in Table 1. Here the contamination criterion is based on the predicted dose from 30 year's exposure from groundshine and from ingestion of contaminated foodstuffs.

Table 3. Contamination areas[km^2] based on long-term exposure from cow's milk and from groundshine following the reference release.

	Contaminated area [km^2]					
Criterion	0,03 Sv/30a		0,1 Sv/30a		0,3 Sv/30a	
Expected or 99,5 percentile	Exp	99,5	Exp	99,5	Exp	99,5
Milk during growing season	80	350	20	70	6	20
Milk outside growing season	1	7	0,09	2	0,005	0,5
Groundshine	8	40	2	8	0,2	3

The strictest criterion 0,03 Sv/30a (per 30 years) corresponds to the annual dose of 1 mSv, when the global average natural dose is 2,4 mSv/a. If a less rigorous level for protective actions as defined in the ICRP Publication 82 (0,3 Sv/30a corresponding to 10 mSv/a) would be used, the contaminated areas are reduced roughly by an order of magnitude.

If deposition takes place during the growing and pasturing season, the largest contaminated areas are found for doses from cow's milk,. If instead deposition occurs outside the growing season, the external dose from fallout dominates the contaminated area. Then contaminated areas are also strongly reduced compared to the values of the growing and pasturing season.

Figure 8 shows the complementary cumulative probability distribution functions of the collective doses caused by the reference source term at the Olkiluoto site. The highest collective doses are brought about via external exposure from fallout. Ingestion doses are not considered, because no up to date statistical data of production distributions was available. Using the fatal cancer risk factor of 0,05 per manSv, about 25 (0,05·500) or

more fatal cancers would be caused in one out of one-hundred releases (at the 99th percentile). Due to simplified calculation, this interpretation gives a restricted indication of societal risk.

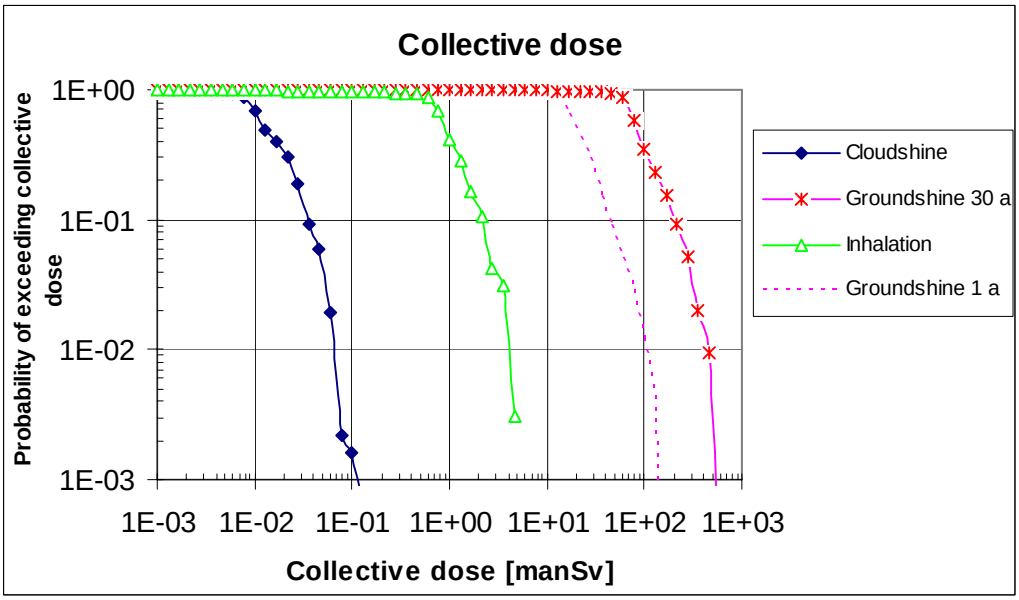

Figure 8. Complementary cumulative distribution functions (CCDF) of the collective doses caused by the reference release in Olkiluoto.

4.3.4 Comparison to safety goal

Finally the feasibility of a safety goal can be assessed by comparing it with the calculated individual fatal cancer risk. Here the reference source term was modified to take into account also other potential nuclides. The release is assumed to be started 24 hours after the shutdown and the iodine release is set to 1500 TBq as I-131 equivalent besides all noble gases are released. In addition, the cesium release is doubled to cover the effect of other nuclides after three month's delay as defined in the reference [VnP 395/1991]. Figure 9 illustrates the individual fatal cancer risk at the distance of 1 km.

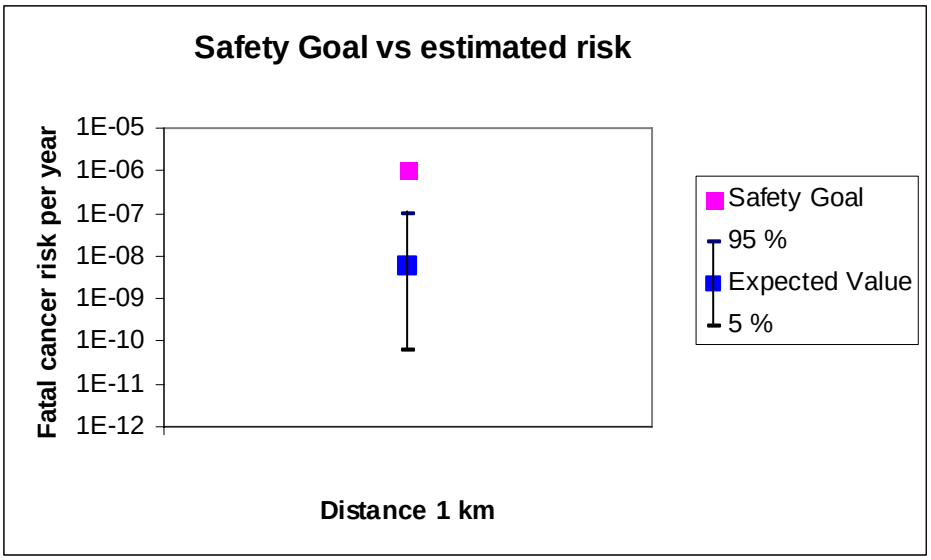

Figure 9. A safety goal compared to the estimated individual fatal cancer risk at the Olkiluoto site.

The calculation includes the release probability of $5 \cdot 10^{-7}$/year and the seasonal variations of agriculture and weather statistic. The value of the safety goal for individual risk is assumed to be 10^{-6}/year as concluded in the beginning of this chapter. It can be seen that the expected value of the calculated individual risk is two orders of magnitude lower than the predefined safety goal value, and that even the 95 % fractile is lower by one order of magnitude. Thus, in this case the requirement of the safety goal is fulfilled.

5 Extension of overview of international safety goals and experiences from their use

OECD/NEA Working group RISK initiated in 2007 a task group on probabilistic safety criteria. The objective of the task is to review the rationales for definition, the current status, and actual experiences regarding the use of probabilistic safety goals and other PSA related numerical risk criteria in the member states.

The scope includes the whole range of safety goals from societal risk, off-site release, core damage and lower level goals. The focus is on experiences from actual use of the safety goals for existing installations, including procedures used, problems related to the technical application of the criteria, and consequences for the status and use of PSA. Both regulatory criteria and criteria defined and used by utilities are covered.

A report presenting the status and trends will be prepared. Rationales used by different regulatory bodies and utilities for setting and defining their safety goals will be compiled, and the relation to acceptance criteria for various risk informed applications will also be reviewed.

During 2007, a questionnaire was prepared and sent to the member countries. In total 19 responses have been received from 13 regulatory bodies and 6 utilities (Canada, Finland and Sweden).

In total 11 different types of criteria were mentioned by the responders of the questionnaire. Large differences can be seen in the status and experience of use of PSA criteria. Two responding countries do not use numerical criteria in the regulatory decision making, while the others use quite different sets of criteria either as strict criteria or as indicators.

The next step of the task is to further analyse the answers and to prepare a report on the issue. The task will be finished in spring 2009, in parallel with the NKS project.

6 Safety goals related to other man-made risks in society

6.1 Introduction

In order to provide perspective on the project's detailed treatment of probabilistic safety goals for nuclear power plants, some information from other areas is provided in this chapter. The aim is two-fold:

- To provide a general overview of the basic rationale for defining safety goals in some countries (section 6.2)
- To provide more detailed information about the safety goals within a two specific industies, railway and offshore oil and gas (sections 6.3 and 6.4).

The information will make it possible to relate safety goals for NPP:s to safety goals defined and applied for other industries.

6.2 National overview

Many societal necessary projects involve risks of fatal accidents. Therefore some sort of regulation is required to ascertain that the risks are not unfairly distributed. Typically the probabilistic safety goals used consider loss of life and economic damage as a consequence. Different probabilistic safety goals are categorised according to the consequences they consider [Jonkman_2003]

- Fatalities
    - individual risk
    - societal risk
- Economic damage
- Environmental damage
- Integrated safety goals
- Potential damage

This section considers some country-sepcific safety goals mainly related to risks to which individuals or a specific group are exposed. The focus is on hazardous installations, such as installations of chemical industry. Another larger entity discussed is safety goals related to transportation. Also some other application areas are mentioned.

6.2.1 The Netherlands

The Netherlands have an officially approved policy for safety goals. It distinguishes between individual risk and societal risk. Furthermore, it distinguishes risks between existing and new activities [Bäckman_2002]. The level of unacceptable risk for an individual from existing activities or industries is chosen from the frequency of death from natural causes. This frequency is lowest for 14-year old girls and is 10^{-5} per year.

The policy states that new industrial activities are not allowed if the total individual risk increases by more than 10 %. Thus, the level for unacceptable individual risk is 10^{-6} per year. The societal risk for existing activities is expressed in a FN-diagram[2]. The criteria for existing and new activities is $10^{-3}/N^2$. The Rijnmond and Schiphol areas are excluded from the new criteria [Trbojevic_2005]. In Netherland the concept of negligible level of risk is no longer used. (Previously for individual 10^{-8} and societal $10^{-5}/N^2$ [Davidson_1997]). Besides criteria for individual and societal fatalities there exisits safety goals for e.g. injuries at the work place, noise pollution and odor nuisance [Beroggi_1997].

The Netherlands have also set safety goals for risks related to transportation of dangerous goods. The safety limit for individual risk is 10^{-6}, which is the same as for stationary installations. The societal risk criteria for transportation of dangerous goods is $10^{-2}/N^2$ per year per kilometre of transport route [Ale_2002, Bottleberghs_2000]. Figure 10 illustrates the unacceptable societal risk limits for installations and transportation. Risk acceptance criteria have also been formulated specifically for rail safety For passengers, individual risk shall be less than 1.5 fatalities per 10^{10} passenger kilometres. For employees the individual risk should be less than 1 fatality per 10 000 employees [Ter_Bekke_2006].

Thus far the only safety limit in the area of air transportation is set for individual risks. In principle, the limit for the probability of death for air transportation is also 10^{-6} per year. Installations with values up to $5 \cdot 10^{-5}$ per year are permitted to continue operating, but they may not be replaced. Installations with larger risk values must cease operating. [Beroggi_1997]

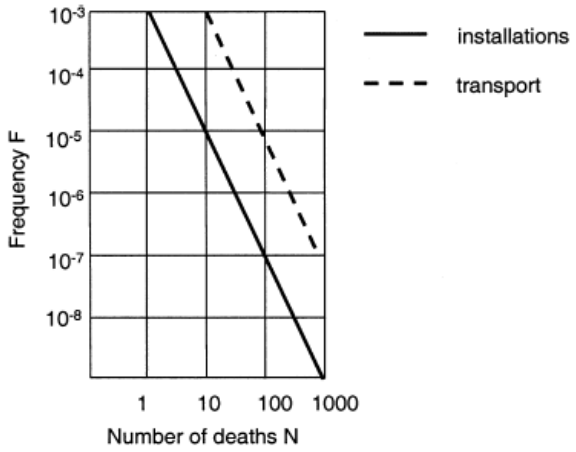

Figure 10. Advisory societal risk limits in the Netherlands [Ale_2002]

6.2.2 The UK

The UK was possibly the first country to use probabilistic regulations. In 1939 England required a 99,999 % reliability for 1 hour of flying time for commercial aircraft. This type of regulation required that the whole aircraft system is examined, along with the influence of its components to reliability [Rechard_1999].

The Health and Safety Executive (HSE) issues statement defining the the risk levels it considers as intolerable or tolerable under certain circumstances. However, these risk

[2] FN = Frequency/Number of fatalities

levels cover all industrial activities in the UK, the primary instrument for risk control is ALARP dynamics [Trbojevic_2005]. The level for unacceptable risk for workers is 10^{-3} per year. The corresponding level for the public is 10^{-4} per year. Risk above these levels is not accepted, i.e., the risk must be reduced or the activity must be stopped. The HSE also uses a limit for broadly acceptable risk, which is set to 10^{-6} per year. Between these limits the ALARP principle applies. HSE also defines risk levels for land use planning, and advises against granting planning permission for any significant development where individual risk of death for the hypothetical person is above 10^{-5} per year, and does not advise against granting planning permission on safety grounds for developments where such an individual risk is less than 10^{-6} per year. [R2P2].

For societal risks the HSE suggests that the risk of an accident causing more than 50 deaths or more in an accident should be regarded as intolerable if the frequency is estimated to be more than one in 5000 years; the associated FN-curve has a slope of -1. The interval between the broadly acceptable region and the tolerable region is set to two orders of magnitude [HSE_2004].

6.2.3 Czech Republic

In the Czech Republic, the Ministry of Environment enacts the principles for the evaluation of risk of major accidents. As in the Netherlands, the Czech Republic has different criteria for existing and new installations. For existing installations the individual risk criterion is 10^{-5} per year and the societal risk criterion is $10^{-3}/N^2$. For new installations, the requirement is 10^{-6} per year and $10^{-4}/N^2$ respectively [Trbojevic_2005].

6.2.4 Switzerland

The societal risk criteria established in Switzerland cover in addition to fatalities also number of people injured, damage to property, as well as contamination of surface water, groundwater, and soil. [Ter_Bekke_2006]

The risk criteria selection depends on the risk dimensions of the material, the product or the waste under consideration. The importance of the consequences is assessed by determination of the separate risk indicators. Figure 11 shows the mapping of damage indicators into three classes. If a disaster value of 0,3 is reached or exceeded for any of the relevant damage indicators, the authority requires the owner to perform and submit a risk study. The criteria also apply to transportation routes used for the shipping of dangerous goods (railway lines, roads, and the river Rhine). [Gmünder]

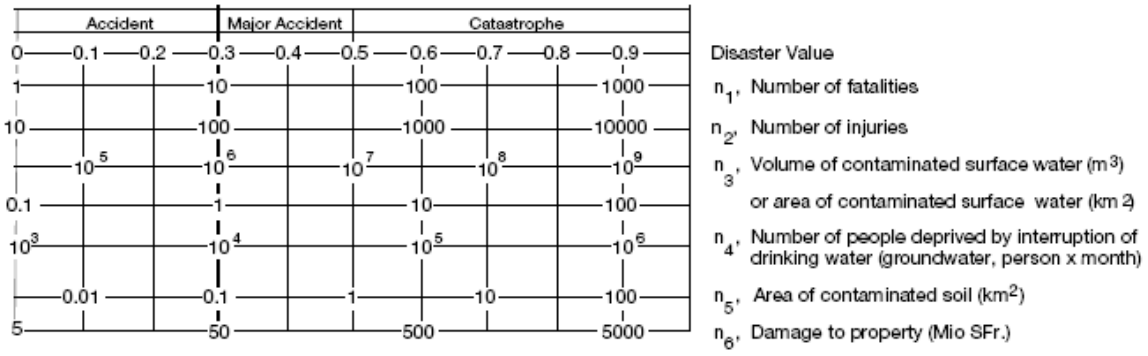

Figure 11. Switzerland – scale of damage indicators (assignment of disaster values)

6.2.5 Germany

In Germany deterministic approaches for risk assessment are extensively used in hazardous plants [Kirchsteiger_1999]. Quantitative methods have not proved suitable or have been unable to establish themselves in the industry. It seems that in Germany two types of criteria are in use [Trbojevic_2004]. Based on the LUP (Land Use Planning) criterion no risk should be imposed to man or the environment outside the installation. The concept of Minimum Endogenous Mortality (MEM) requires that the total risk from all technical systems affecting an individual must not exceed minimum human mortality ($2 \cdot 10^{-4}$ deaths per person per year). Based on the MEM principle the following rule is applied to transportation; "Hazards due to a new system of transport must not significantly augment the Endogenous Mortality Rate". In practice this translates into the following criteria:

- Fatality rate < 10^{-5} per person-year
- Serious injury rate < 10^{-4} per person-year
- Light injury rate < 10^{-3} per person-year

6.2.6 Some other criteria

Some other safety goals used for various technologies:(adopted from [Kafka 1999] and [Pfitzer_2004])

- Marine structures: Failure probability for different accident classes 10^{-3}-10^{-6}
- Aviation, air planes: Catastrophic failure per flight hour, less than 10^{-9}
- Space vehicles: Catastrophic concequence for Crew Transfer Vechicle(CTV) less than 1 in 500 CTV missions.
- Missile range criteria for falling debris: For example, max. acceptable probability for individual fatality (general public) during one mission 10^{-7} and during one year 10^{-6}.

The concept of Safety Integrity Levels (SIL) is introduced in the increasingly important standard IEC 61508, which deals with the functional safety of electrical, electronic and programmable electronic safety-related systems[IEC 61508]. The standard applies quantitative requirements to systems operating on demand and to system operating continuously in order to maintain a safe state. Table 4 illustrates the relationship between the SIL number and the required failure probabilities.

Table 4. Safety Integrity Levels for safety functions operating on demand and in a continuous demand mode [OLF_070]

SIL	**Demand Mode of Operation** (average probability to perform its design function on demand)	**Continuous / High Demand mode of Operation** (probability of dangerous failure per hour)
1	$\geq 10^{-2}$ *to* $< 10^{-1}$	$\geq 10^{-6}$ *to* $< 10^{-5}$
2	$\geq 10^{-3}$ *to* $< 10^{-2}$	$\geq 10^{-7}$ *to* $< 10^{-6}$
3	$\geq 10^{-4}$ *to* $< 10^{-3}$	$\geq 10^{-8}$ *to* $< 10^{-7}$
4	$\geq 10^{-5}$ *to* $< 10^{-4}$	$\geq 10^{-9}$ *to* $< 10^{-8}$

6.2.7 Summary of national criteria

The natioanl criteria for individual and societal (group) risk previously discussed and a few more are summarised in Table 5 and Table 6 below.

Table 5. Comparison of criteria of individual risk

Country	**Application**	**Maximum tolerable risk**	**Negligible level of risk**	**Comment**
The Netherlands	Established plants or combined plants	10^{-5} ALARA principle applies	Not applied	
	New plants	10^{-6} ALARA principle applies	Not applied	
UK	Existing hazardous industries	10^{-4} ALARP principle applies	Broadly accepted limit 10^{-6}	Negligible limit 10^{-7}
	Existing dangerous goods transportation	10^{-4}	10^{-6}	
	New housing areas near existing plants	10^{-5}	10^{-6}	
Czech Republic	Existing installations	10^{-5}		Risk reduction must be carried out
	New installations	10^{-6}		
Hungary	Hazardous facilities	10^{-5} Upper limit	$3 \cdot 10^{-6}$-10^{-6} Lower limit	
Hong Kong	New plants	10^{-5}	Not used	
Australia (New South Wales)	New plants and housing	10^{-5}	Not used	
Australia (Victoria)	Existing installations	10^{-5}	Acceptable limit 10^{-7}	
USA, California	New plants	10^{-5}	10^{-6}	
Germany	Transportation	10^{-5}		

Table 6. Comparison of criteria of societal risk

Country	Application	Maximum tolerable risk	Negligible level of risk	Comment
The Netherlands	Established and new plants	$10^{-3}/N^2$	Not applied	
UK	Hazardous installations	$10^{-2}/N$		
	Existing harbours	$10^{-1}/N$	$10^{-4}/N$	
Hong Kong	Hazardous installations	$10^{-3}/N$	$10^{-5}/N$	Limit for maximum N=1000
USA, California	On-site risk	$10^{-1}/N^2$	$10^{-3}/N^2$	
	Off-site risk	$10^{-3}/N^2$	$10^{-5}/N^2$	
Australia (Victoria)	Hazardous industries	$10^{-2}/N^2$	$10^{-4}/N^2$	
Switzerland	Hazardous installations	$10^{-5}/N^2$ (for N>10)	$10^{-7}/N^2$ (for N>10)	Limit for maximum N=1000. N<10 domain of no serious damage
Denmark	Hazardous installations	$10^{-2}/N^2$		

6.3 Safety goals in the European off-shore oil and gas industry

6.3.1 Introduction

In the Oil and Gas industry, risk acceptance criteria (RAC) are used to express a risk level with respect to a defined period of time or a phase of the activity. RAC may be qualitative or quantitative. RAC are also known variously in the Oil and Gas industry as “risk criteria”, “decision criteria”, “screening criteria”, “tolerability criteria”, etc.

A survey has been made of the regulatory and industry requirements in the Oil and Gas industry for defining Risk Acceptance Criteria [He_2007]. The focus has been on Norwegian and UK offshore oil industry, where the quantitative RAC are mostly used.

6.3.2 Risk acceptance criteria in the Norwegian oil and gas industry

6.3.2.1 Norwegian Petroleum Directorate (NPD) requirements

NPD’s requirements regarding acceptance criteria and their use are presented explicitly in the regulations. Section 6 “Acceptance criteria for major accident risk and environmental risk” of the NPD’s management regulations [NPD_Manreg_2002], requires that the operator shall set acceptance criteria for major accident risk and environmental risk. RAC shall be set for personal risk to workers and to third party, loss of main safety functions and pollution from the facility.NORSOK requirements

NORSOK standard[3] , Z-013 [NORSOK-Z-013], presents some general requirements regarding the formulation of RAC. It is noted that the NORSOK standard does not

[3] The NORSOK standards are developed by the Norwegian petroleum industry as a part of the NORSOK initiative and are issued jointly by OLF (the Norwegian Oil Industry Association) and TBL (Federation

provide any guidelines on what actual values to choose for RAC. This is principally in line with the requirements stipulated by the Norwegian authority, i.e. NPD, which require that the operators should formulate their own risk acceptance criteria.

In order for the RAC to be adequate as support for Health, Environment and Safety (HES) management decisions, Standard Z-013 also requires that the used RAC should represent a compromise where the following qualities are satisfied as far as possible:

- Be suitable for decisions regarding risk reducing measures.
- Be suitable for communication.
- Be unambiguous in their formulation (such that they do not require extensive interpretation or adaptation for a specific application).
- Not favour any particular concept solution explicitly nor implicitly through the way in which risk is expressed.

6.3.2.2 Risk acceptance criteria examples

The following are some examples of risk criteria that have been used by operators on the Norwegian continental shelf.

Individual Risk Criteria for Workers

- The average individual risk, expressed by the fatal accident rate (FAR)[4] - must meet the criterion FAR < 10.
- For specially exposed groups, the average group individual risk, expressed by the fatal accident rate (FAR) - must meet the criterion FAR < 25.

Individual Risk Criteria for 3rd Party

The fatality risk for the most exposed person shall not exceed $1 \cdot 10^{-5}$ per year (limit). An ALARP objective is defined at $1 \cdot 10^{-7}$ per year.

Group Risk Criteria for 3rd Party

The criterion for 3rd party societal risk is:

$$F(N) = \frac{1}{100 \cdot N}$$

where F(N) is the accumulated frequency for N or more fatalities.

The ALARP objective is defined as:

$$F(N) = \frac{1}{100 \cdot N} \cdot \frac{1}{100}$$

This is illustrated graphically in Figure 12. .

---

of Norwegian Engineering Industries). The NORSOK standards are administered by NTS (Norwegian Technology Standards Institution).

[4] FAR = Fatal Accident Rate; number of fatalities during 100 million exposure hours, i.e., FAR = 10 corresponds to a frequency of 10^{-9}/hour.

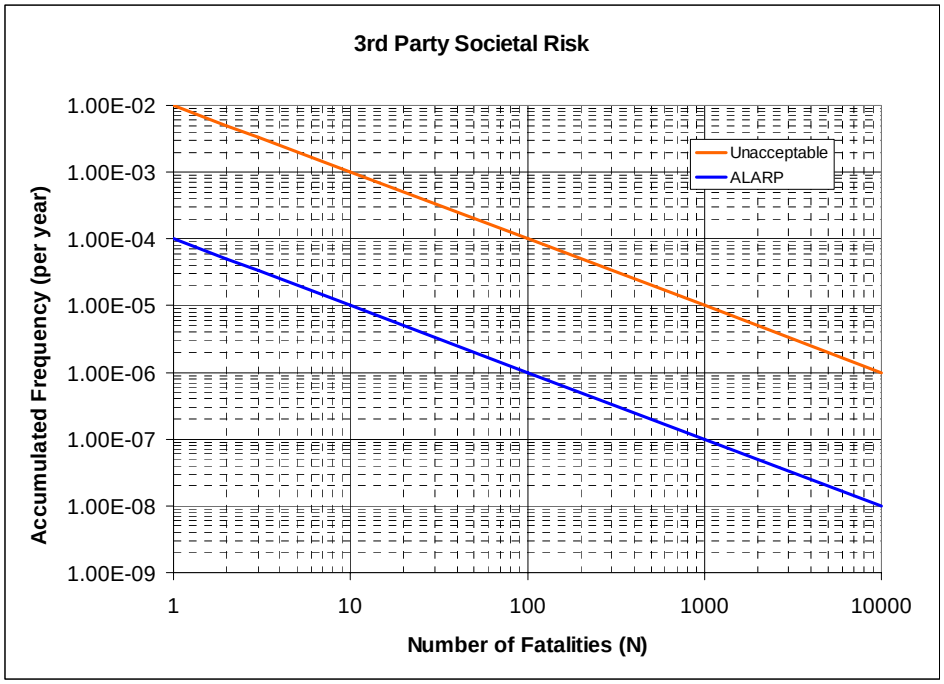

Figure 12. Risk Acceptance Criteria for 3rd party Societal Risk – Example

Loss of Main Safety Functions: Example

For an offshore drilling rig, it is required that the frequency of loss of defined main safety functions on the rig shall be lower than $1 \cdot 10^{-4}$ per year per safety function and per accident category.

The accident categories are:

- Hydrocarbon leak, fire and explosion
- Blow-out
- Helicopter crash on installation
- Collisions
- Falling loads
- Occupational (work) accidents
- Loss buoyancy or stability
- Other accidental events (AEs)

The defined main safety functions include:

- Escape routes from areas outside the area of the initial event
- Evacuation means (lifeboats)
- Safe haven/Living Quarter (LQ)
- Prevention of spreading
- Main load bearing structure and stability
- Fire water system
- Central Control Room

6.3.3 Risk acceptance criteria in UK regulations

ALARP Principle

The risk acceptance criteria used by the UK petroleum industry are mainly those that have been formulated by the UK Health and Safety Executive (HSE) and are embodied in statutory legislation.The Offshore Installations (Safety Case) Regulations 2005 (SCR05), [HSE_SCR_3117], requires the duty holder (i.e. the owner or operator) for each fixed and mobile installation to prepare a safety case, which must be accepted by the HSE before the installation can be operated on the UK continental shelf. It requires, among other matters, a demonstration that:

- All hazards with the potential to cause a major accident have been identified;
- All major accident risks have been evaluated; and,
- Measures have been taken, or will be taken, to control the major accident risks to ensure compliance with the relevant statutory provisions (i.e. a compliance demonstration).

The ALARP (As low as Reasonably Practicable) principle is the basis of the UK Safety Case Regulations , and requires "every employer to adopt safety measures unless the cost is grossly disproportionate to the risk reduction".

Individual Risk Criteria

HSE's risk criteria for individual risk criteria are [HSE_R2P2]:

- Maximum tolerable risk for workers : 10^{-3} per person-year
- Maximum tolerable risk for the public : 10^{-4} per person-year
- Broadly acceptable risk: 10^{-6} per person-year

The ALARP principle is applied for events in the intermediate area. For those near the broadly acceptable limit, the risks are considered tolerable if the cost of risk reduction would exceed the improvement gained. For those near the maximum tolerable limit, the risks are considered tolerable only if risk reduction is impracticable or implementation of risk reducing measures would lead to disproportionate costs compared with safety benefits gained.

It is noted that the above criteria are not official HSE criteria for offshore installations. In the assessment principles for offshore safety cases [HSE_APOSC], HSE also states that:

- An individual risk of death of 10^{-3} per year has typically been used within the offshore industry as the maximum tolerable risk.

Temporary Refuge Impairment Criteria

Although there is no specific requirement to estimate group risk, SCR05 indicates a need for a safety case to demonstrate temporary refuge integrity (TRI) – this could be considered as a measure of society risk.

The assessment principles for offshore safety cases [HSE_APOSC] requires that criteria should exist that describe the TRI and the time over which TRI needs to be maintained against all hazards identified in the risk assessment. The safety case should demonstrate that these criteria are met i.e. that TRI would be maintained for the necessary time.

The typical TRI criterion proposed by HSE [HSE_SCReq_2/2006], is represented as a frequency per year, with an upper bound of no higher than 10^{-3}. In other words no more than once in every 1000 years would there be an event that would prevent the TR from functioning as described in the safety case. ALARP principle should be applied below the upper level, i.e. loss of TRI frequency should be reduced to a lower level wherever reasonably practicable.

6.3.4 Discussions

Risk acceptance criteria have been used in the Oil & Gas industry especially in offshore risk analysis for many years. A common thinking has been that risk analyses and assessments cannot be conducted in a meaningful way without the use of such criteria. The strengths of RAC as a decision support tool are:

- They make interpretation of the results of a risk assessment explicit and traceable.
- They are widely used and discussed in different fields.

In Oil & Gas industry there had been some discussions about the suitability of risk acceptance criteria to assess and control risks [Aven_RESS_90(2005)], such as: the introduction of pre-determined criteria may give the wrong focus—meeting these criteria rather than obtaining overall good and cost-effective solutions and measures.

Another issue about RAC is the influence of uncertainty. The results of risk assessments will always be associated with some uncertainties, which may be linked to the relevance of the data basis, the models used in the estimation, the assumptions, simplifications or expert judgements that are made. This uncertainty will be reduced as the development work progresses. NORSOK Z-013 Standard states that the comparison to RAC should usually be made in relation to 'best estimate' from the risk analysis rather than to an optimistic or pessimistic result of the studies.

In general in the Oil &Gas industry, the use of criteria is widely required and recommended to obtain meaningful results and implementation of relevant measures. Experience is a key factor in this respect both for the personnel performing the study and for the people reviewing the results.

6.3.5 Conclusions

The following are some general conclusions regarding safety goals in the offshore oil and gas industry:

- Compared to the nuclear industry, both the number of precursor events requiring handling and of accidents requiring mitigation is higher, resulting in a relatively high focus in the criteria on consequence mitigation.
- The criteria have a large scope, i.e. they apply to a wide range of accident events and consider a wide range of safety functions.
- The ALARP principle is often applied, involving a safety goal with a limit and an objective.
- Defence in depth aspects are considered in the criteria by stating requirements for different safety functions.
- Criteria are regarded as necessary, but a number of problems are acknowledged.

6.4 Safety goals in the European railway industry

6.4.1 Introduction

An overview has been made of the background and status of safety goals in the European railway industry [Persson_2007]. A railway system can be defined very widely. In this section the system looked upon is the European Train Control System (ETCS), as explained and defined below. Figure 13 shows the main parts of the ETCS system.

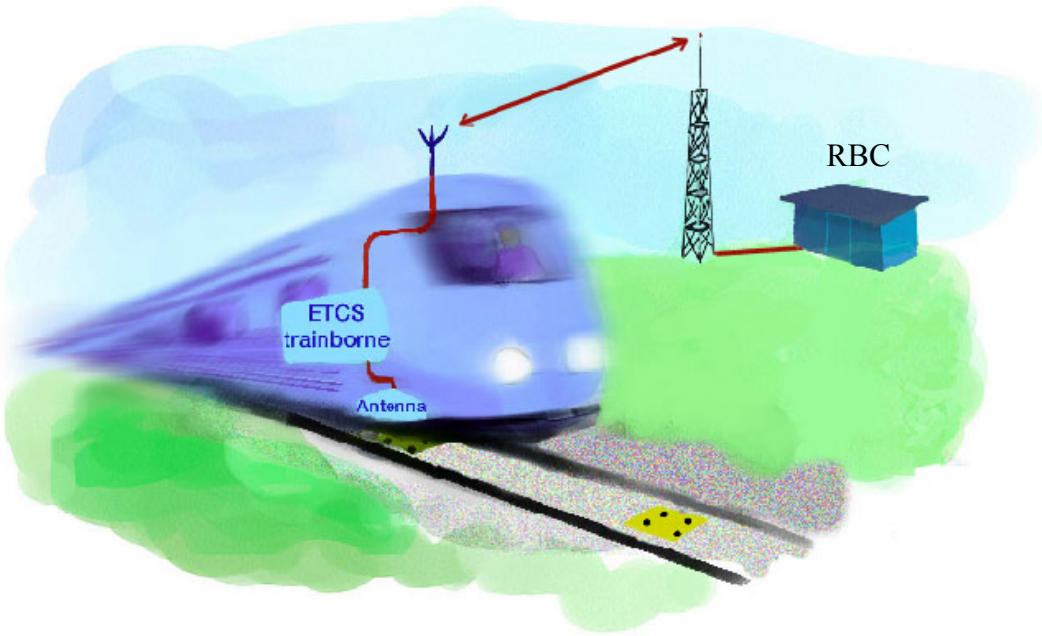

Figure 13. Main parts of the ETCS system

ETCS is the control-command system and GSM-R is the radio system for voice and data communication. Together, they form The European Rail Traffic Management System (ERTMS). The Radio Block Center (RBC) sends movement authority and track profiles to the train via GSM-R. The RBC is the link between the interlocking system, the train traffic control, and the train itself. The train reports its position to the RBC. Balises are read by the on-board antenna, processed by the ETCS onboard (trainborne) equipment and are used as position references for the train, i.e. they determine where the train is.

ERTMS/ETCS is a standardized system that allows trains to cross national borders without the need to change locomotive or driver. The system forms the cornerstone of a common system for train control and traffic management within Europe. It has been developed by Europe's railway and signalling industries (UNISIG) in response to the need for cross-border traffic identified in an EU initiative.

6.4.2 General

There are a number of recognized principles for managing risks and achieve target values for tolerable risks of accidents with injuries or casualties within the railway industry. The principles are somewhat geographically oriented, i.e. different countries have recognized different principles. MEM is mainly practiced in Germany,

GAMAB/GAME in France and ALARP is preferred in the UK. The source for these principles has been [IEC 62278].

MEM
(Minimum Endogenous Mortality)

The main point of the MEM principle is the endogenous mortality caused by natural reasons e.g. illness or natural defects. This value naturally depends on the age of the considered person and on living conditions. In well-developed countries the mortality is at its lowest for the age group 5 years to 15 years resulting in a MEM of:

$$R_{\mathrm{m,total}} = 2 \cdot 10^{-4} \frac{\mathrm{death}}{\mathrm{person} \cdot \mathrm{year}}$$

The MEM principle argues that a human life is exposed to 20 technical systems at the same time, and that a technical system appears acceptable for a society when it's contribution is less or equal to 5 % of the total risk. Railways are one of these technical systems, so the acceptable risk for railway systems would become $1 \cdot 10^{-5} \frac{\mathrm{death}}{\mathrm{person} \cdot \mathrm{year}}$ which translates to $1{,}14 \cdot 10^{-9} \frac{\mathrm{death}}{\mathrm{person} \cdot \mathrm{hour}}$.

ALARP
(As Low As Reasonable Practicable)

According to the (ALARP) principle, described in the yellow book of Railtrack but also in a more general way in [IEC 62278], three areas of risk, divided by certain limits, have to be considered:

<u>The unacceptable region</u>

Some risks are so large and some outcomes so unacceptable that they are intolerable and cannot be justified on any grounds. The upper bound (limit) defines levels of risk that are intolerable. If the level of risk cannot be reduced below this bound then the operation should not be carried out.

<u>The ALARP or tolerability region</u>

The area between the upper and lower bounds is called the ALARP region. It must be stressed that it is not sufficient to demonstrate that risks are in the ALARP region. They must be made as low as reasonably practicable. There are various ways to demonstrate ALARP. It may be sufficient to show that the best available current standards and practices are being applied. For novel operations, or where the adequacy of current standards or practices is in doubt, the concepts of cost benefit analysis and value of life can be introduced.

<u>The broadly acceptable region</u>

The lower bound (objective) of the diagram defines the broadly acceptable region where risks are considered to be so low that strenuous efforts to reduce them further would not be likely to be justified by any ALARP criteria.

In [IEC 62278] no quantitative targets are presented for the ALARP principle but in draft documents [UNISIG_Class1] for the UNISIG work one can see that the ALARP

principle defines target values (objective) around the level of $1.1*10^{-9}$ $\frac{\text{death}}{\text{person} \cdot \text{hour}}$ as an upper limit, which is similar to the results of the MEM principle.

GAMAB/GAME
(Globalement Au Moins Aussi Bon/Globalement Au Moins Equivalent)

The GAMAB/GAME principle is based on comparison with existing systems.

The complete formulation of this principle is as follows:

"All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent existing system".

This formulation takes into account what has been previously done and requires implicitly a progress to be made in the projected system, by the requirement "at least". It does not consider a particular risk, by the requirement "globally". The transport system supplier is free to allocate between the different risks inherent to the system and to apply the relevant approach, i.e. qualitative or quantitative.

6.4.3 Background to risk acceptance criteria

With the introduction of the CENELEC railway standards and the ERTMS/ETCS system, a probabilistic approach was taken to safety analyses within the field of railway safety as it is depicted by those standards and specifications. This makes the approach for safety analyses within railway technology in line with other technology areas such as aviation and nuclear power generation.

Previous attempts for the definition of these safety targets were questioned by different national railways and authorities so a decision was taken within ESROG to request safety experts from DB AG and SNCF to set up an independent study to define the safety targets, represented by a rate for hazards which can be tolerated by railways and national authorities.

The general approach taken to reach these targets were the GAMAB/GAME principle, and by that taking into account the performance of existing railway systems and the operating experience and accident statistics.

The hazardous events considered by SNCF and DB were:

- Derailment
- Collision with other railway vehicle

These efforts resulted in the following definitions for safety targets:

TIRF = tolerable individual risk of a individual person to suffer an accident with fatal consequences while travelling in a train

and restricted to ETCS

$TIRF_{ETCS}$ = tolerable individual risk of an individual person to suffer an accident with fatal consequences while travelling in a train due to a hazardous condition of ETCS

The calculations also considered the contribution of the ETCS system to the overall risk figure. It was concluded that 2.5 % could be related to the ETCS system.

Several reports by DB AG and SNCF were worked on and evaluated by an Independent Assessment Committee. The result of the assessment of the work performed by DB AG and SNCF showed that there were quite large differences between the results. These differences were assessed by the Independent Assessment Committee and a number of differences in the approach taken for the calculations were identified.

From the Independent Assessment Committee's final report it can be read that during an ESROG meeting it was agreed that a value of $2 \cdot 10^{-9}$ Hazards/hour would be acceptable to both SNCF and DB. It is more conservative than the value calculated by DB, but it corresponds well to SIL-4[5] requirements in the CENELEC standards. This is likely the background for the value now established in the TSI for Control-Command and signalling and as such the safety target for all suppliers. It can be noted that the figure was arrived at by negotiation rather than by adherence to criteria such as GAMAB/GAME, although the underlying calculations were made according to that principle.

6.4.4 Hazard definition

During the work with specifying the ETCS, the approach was taken of first trying to quantify the risk of individual fatalities during a train ride. The definition used for that work was:

TIRF = tolerable individual risk of a individual person to suffer an accident with fatal consequences while travelling in a train

Today, suppliers of ETCS equipment do not use TIRF but instead the term Tolerable Hazard Rate (THR), where THR represents the acceptance of risk, i.e. the tolerable rate of hazardous failures. To calculate a relevant THR from the TIRF, additional parameters must be added, e.g. number of passengers on a train, speed, traffic density etc.

When going from TIRF to THR the definition is transferred to be more attached to the technical solution and related to the risk level for a specific function.

It has been agreed within UNISIG for ETCS systems that the undesirable event or Hazard is defined as:

Exceedance of safe speed / distance limits as advised to ETCS

According to the previous discussions it follows that the quantitative target for the top hazard (UE) is set to $2.0 \cdot 10^{-9}$/ hour / train**.** This safety target is defined in the TSI for Control-Command and signaling, [2006/860/EC] and is as such a legal requirement.

6.4.5 Responsibilities

The responsibility for establishing safety targets for railway systems is described in [EN_50129] and is divided between each railway authority (such as Banverket, DB, SNCF, etc) and each supplier (Bombardier, Ansaldo, Siemens, etc.). The principle is that a THR is allocated by the railway authority to the supplier for a specific defined

[5] SIL is a number of defined discrete levels for specifying the safety integrity requirements of the safety function to be allocated to the safety related systems. The Safety Integrity Level with the highest figure has the highest level of safety integrity. Each Safety Integrity Level corresponds to a THR interval according to the Cenelec standards.

hazard. Each hazard and THR is then by the supplier apportioned within their system to each relevant subsystem. This means that the overall risk analysis is mainly the responsibility of the railway authority, and the supplier is responsible for hazard control and to verify their results against the safety target or THR set by the railway authority. The division of responsibilities is illustrated in Figure 14.

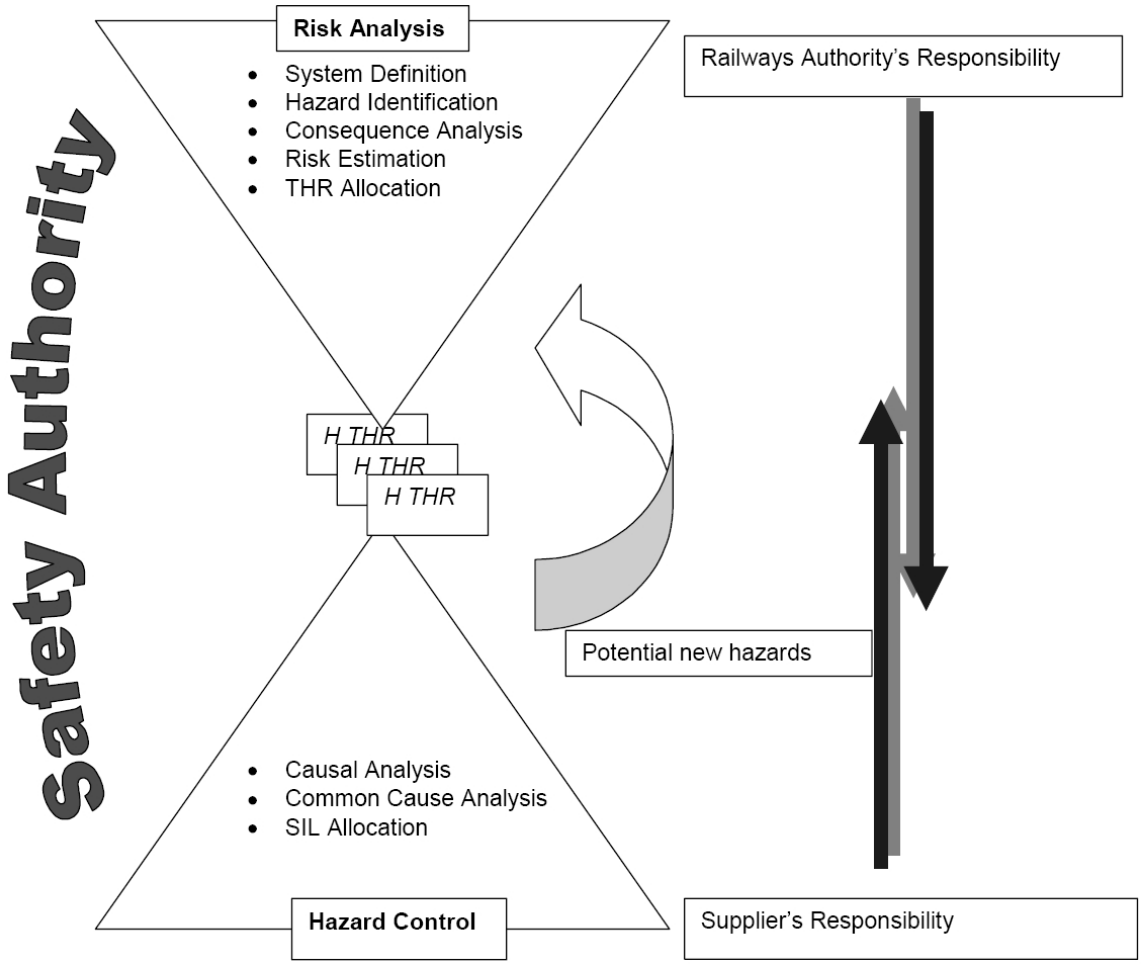

Figure 14 Risk analysis responsibilities from EN 50129

6.4.6 Verification

The verification against the THR_{ETCS} is done by the manufacturer of the system at different levels. Usually it is analysed using fault tree analysis. There is a conceptual fault tree specified by UNISIG in [ETCS_subset-088] that qualitatively analyses the top hazard. The fault tree will be adapted to the specific system being analysed and to the mode of operation. The verification of the safety target will be by comparing the result of the FTA to the THR. If satisfactory results are not achieved, then a re-design would be considered. Verification of safety target is also re-evaluated in case of upgrades and redesign.

6.4.7 Emerging common safety targets

One of the obstacles for the opening of the railway market is the absence of a common approach for demonstrating the safety levels of the railway systems. Without this common approach, the different National Safety Authorities will have to perform their own assessments in order to accept a system, or parts of it, which have been developed

and proven safe in other Member States. To facilitate this cross-acceptance of railway systems/sub-systems between Member States, the methods used for the identification and the management of system hazards and risks have to be harmonised inside all the organisations involved in the development and the operation of the railway systems on the territory of the European Union.

Therefore, in order to promote and improve the compatibility and competitiveness of railways in the Member States the European Union set up the European Railway Agency (ERA), with defined tasks for interoperability and safety.

The Safety Directive 2004/49/EC establishes a framework for railway safety, but leaves certain measures to be gradually developed. ERA will be the driving force to develop these measures. They concern the common safety methods and common safety targets, definition of common safety indicators and harmonization of documents related to safety certification. The task of interest here is the setting up of Common Safety Targets (CST).

The first set of CSTs regarding examination of current safety performances is planned to the 30th of September 2008. The first set are safety targets which will be applicable at the level of the Member States and expressed in term of fatalities by units, like e.g. train km. The first set of CST will not provide detailed risk acceptance criteria (or safety target) like the THR for ETCS. This is planned for the second set of CSMs/CSTs (2009-2010).

6.4.8 Conclusions

The following are some general conclusions regarding safety goals for European rail systems:

- A standardisation of safety goals has been prompted by the expressed aim of making it possible for trains and personnel to cross national borders.
- Safety goals proposed by an industry working group, and accepted by authorities.
- Consensus requirements based on an amalgamation of national practices, mainly from Germany and France.
- Systematic procedure in place for creating subsidiary goals, this is done by defining a tolerable hazard rate (THR) for each subsystem forming part of the overall system.
- Basic principles are based on comparison to general health risk (MEM principle) and a requirement for continuous improvement of safety (GAMAB).
- A framwork for cross-acceptance is under development, i.e., development of an agreed common approach for demonstrating the safety levels of the railway system (in addition toi the common risk criteria already in place). To achieve this, the methods used for the identification and the management of system hazards and risks have to be harmonised.

7 Conclusions

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 large 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. The three phases of the project "The Validity of Safety Goals" will deal with a number of different aspects on the definition and application of probabilistic safety criteria. The results from the project can be used at the utilities as a platform for discussions 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 are expected to support on-going activities concerning risk-informed applications.

The second phase of the project, the outcome of which is described in this project report has mainly dealt with four issues:

- Consistency in the usage of safety goals
- Criteria for assessment of results from PSA level 2
- Overview of international safety goals and experiences from their use
- Safety goals related to other man-made risks in society

Some conclusions from these activities will be summarised below.

Consistency in the usage of safety goals

Consistency in judgement over time has been perceived to be one of the main problems in the usage of safety goals. Safety goals defined in the 80ies were met in the beginning with PSA:s performed to the standards of that time, i.e., by PSA:s that were quite limited in scope and level of detail compared to today's state of the art. This issue was investigated by performing a comparative review was performed of three generations of the same PSA, focusing on the impact from changes over time in component failure data, IE frequency, and modelling of the plant, including plant changes and changes in success criteria. It proved to be very time-consuming and in some cases next to impossible to correctly identify the basic causes for changes in PSA results. A multitude of different sub-causes turned out to combined and difficult to differentiate. Thus, rigorous book-keeping is needed in order to keep track of how and why PSA results change. This is especially important in order to differentiate "real" differences due to plant changes and updated component and IE data from differences that are due to general PSA development (scope, level of detail, modelling issues).

Criteria for assessment of results from PSA level 2

Goals related to CDF and LERF are surrogates to societal risk level criteria. To fully validate these goals, calculations of environmental consequences of release sequences would need to be made. The on-going international survey conducted by the OECD/NEA WG Risk shows that acceptance criteria for results from level 2 PSA differ considerably between countries. Both definitions for large release and probability

values differ. Further, the status of criteria differs from mandatory requirements to informal targets. Some countries do not use probabilistic criteria at all.

The probability limits used in level 2 PSA vary from 10^{-7}/year to 10^{-5}/year. The highest criteria (10^{-5}/year) have been defined for old reactors only. For new reactors, targets between 10^{-7}/year and 10^{-6}/year have been defined. These numbers can be compared with risks experienced or accepted otherwise in society. From the individual risk point of view, these numbers are acceptable. To validate the target values from the societal risk point of view, level 3 PSA assessments need to be made. Results from such assessments are strongly dependent on population data, weather data, and whether or not countermeasures are accounted.

The aim of the definition for large release of the severe reactor accident is such that, first of all, the release magnitude shall be reduced to such an amount that no acute health effects are caused in the environment. It follows from this requirement that only stochastic late effects can be expected. The criterion “100 TBq Cs-137” used in Finland and the differently worded but almost identical criterion “0,1 % of the core inventory of Cs-137 in an 1800 MWt BWR” used in Sweden are examples of criteria fulfilling the above requirement. Test calculations with environmental data from a Finnish nuclear power plant site shows that this particular release limit would not cause acute heath effects and that late effects would be minor.

Overview of international safety goals

The on-going OECD/NEA Working group RISK task group on probabilistic safety criteria has the objectives to review the rationales for definition, the current status, and actual experiences regarding the use of probabilistic safety goals and other PSA related numerical risk criteria in the member states. The NKS project participates actively in the task. At present, responses have been received to a questionnaire and processing and compilation of answers has been initiated. The activity has already provided valuable input to the NKS projcet, and is expected to provide further valuable input during the third and final project phase.

Safety goals related to other man-made risks in society

In order to provide perspective on the project’s detailed treatment of probabilistic safety goals for nuclear power plants, some information from other areas has been collected, with the focus on the use of probabilistic risk criteria in European offshore oli and gas operations and in the European railway industry.

In offhore oil and gas operations both the number of precursor events requiring handling and of accidents requiring mitigation is high compared to the nuclear industry, resulting in a relatively high focus in the criteria on consequence mitigation. Criteria have a large scope, i.e. they apply to a wide range of accident events and consider a wide range of safety functions. Defence in depth aspects are considered in the criteria by stating requirements for different safety functions. Finally, the ALARP principle is often applied, involving a safety goal with a limit and an objective.

For European rail systems, a standardisation of safety goals has been prompted by the expressed aim of making it possible for trains and personnel to cross national borders. The harmonisation has been achieved by by letting an industry working group propose saety goals, which have then been accepted by authorities. The goals suggested are consensus requirements based on an amalgamation of national practices, mainly from Germany and France. Basic principles are based on comparison to general health risk (MEM principle) and a requirement for continuous improvement of safety (GAMAB). Systematic procedures are in place for creating subsidiary goals, which is done by defining a tolerable hazard rate (THR) for each subsystem forming part of the overall system. Finally, it is woth noting , that a framwork for

cross-acceptance is under development, i.e., development of an agreed common approach for demonstrating the safety levels of the railway system (in addition to the common risk criteria already in place).

Continued work during phase 3

To some extent, phase 3 of the project will consist in the continuation of activities initiated during phase 2. This is mainly the case for the international overview (OECD/NEA WGRisk task on safety criteria). In addition, focus will specifically be put on exploring more in detail the relationship between different levels of criteria, and on the utilisation of numerical criteria when using probabilistic analyses in support of deterministic safety analysis. Finally, general guidance will be provided – on the basis of project experiences – concerning the formulation, application and interpretation of probabilistic criteria.

Thus, the project includes the following main parts:

- Participation in OECD/NEA WGRisk task on use of probabilistic criteria
- Use of subsidiary criteria and relations between these
- Numerical criteria when using probabilistic analyses in support of deterministic safety analysis
- Guidance for the formulation, application and interpretation of probabilistic safety criteria (harmonization of approaches)

8 References

2006/860/EC	Technical specification for interoperability relating to the control-command and signaling subsystem, 2006/860/EC
Ale_2002	Ale, B.J.M.; Risk assessment practices in The Netherlands; Safety Science, Volume 40, Number 1, February 2002, pp. 105-126(22).
ASN_1977	The letter 1076/77 of the French Nuclear Safety Division published in 1977
Aven_RESS_90(2005)	Terje Aven, Jan Erik Vinnen; On the use of risk acceptance criteria in the offshore oil and gas industry; Reliability Engineering and System Safety, 90 (2005): 15-24.
Bäckman_2002	Bäckman, J.; Railway Safety – Risks and Economics; PhD thesis, Royal Institute of Technology, Stockholm, 2002.
Beroggi_1997	Beroggi, G.E.G., Abbas, T., Stoop, J., Aebi, M.; Risk Assessment in the Netherlands; Akademie für Technikfolgenabschätzung in Baden Württemberg, No. 91, November 1997, ISBN 3 932013-14-x, ISSN 0945-9553.
BNS I.4.2/2006	Requirements for PSA performance.
Bottleberghs_2000	Bottleberghs, P. H.; Risk analysis and safety policy developments in the Netherlands; Journal of Hazardous Materials, Volume 71, Number 1, 7 January 2000, pp. 59-84(26).
CNSC_968790	Safety Goals for S-337. CNSC reference 968790
Davidson_1997	Davidson, G., M., Lindgren, M., Mett, L.; Värdering av risk (Valuation of risk); Räddningsverket – Risk- och miljöavdelningen, Karlstad, Report no. P21 – 182/97.
Dinnie_2004	Dinnie, K.S., Experience with the Application of Risk-Based Safety Goals, 25th Annual Conference of the Canadian Nuclear Society, June 2004. Specific guidance of using "risk" information and criteria have been developed in OPG Nuclear Safety Policy, N-POL-0001 R00 and OPG Risk and Reliability Program, N-PROG-RA-0016 R05.
EN 50129	EN 50129, Railway applications – Communication, signaling and processing systems – safety related electronic systems for signaling
ETCS_subset-088	ETCS Application Level 2 – Safety Analysis, Part 1 – Functional Fault Tree, subset-088, part 1
Gmünder	Gmünder, F.K., Meyerm P., Shiess, M.; The Control of Major Chemical Hazards in Switzerland in the framework of sustainable development – Liquefied Petroleum, Ammonia and Chlorine as Examples.
Gustavsson_2007	Gustavsson, H; Consistency in Usage of Safety Goals – A case study involving Forsmark 1 PSA; Relcon Scandpower; Relcon Scandpower report 32.800.003-R-003; Relcon Scandpower; 2007
He_2007	He, X; Risk Acceptance Criteria in the Offshore Oil and Gas Industry; Relcon Scandpower; Relcon Scandpower report 32.800.003-R-002; Relcon Scandpower; 2007
HSE_2004	Guidance on 'as low as reasonably practicable' (ALARP) decision in Control Of Major Accident Hazards (COMAH), SPC/Permissioning/12
HSE_APOSC	Assessment principles for offshore safety cases (APOSC); HSE 2006
HSE_R2P2	Reducing Risks, Protecting People. UK HSE's decision making process [R2P2]; http://www.hse.gov.uk/risk/theory/r2p2.htm
HSE_SAP_2006	The HSE's Safety Assessment Principles, SAPs http://www.hse.gov.uk/nuclear/saps/saps2006.pdf
HSE_SCR_3117	The Offshore Installations (Safety Case) Regulations 2005; UK Statutory Instrument 2005 No. 3117
HSE_SCReq_2/2006	Offshore Installations (Safety Case) Regulations 2005 Regulation 12 Demonstrating compliance with the relevant statutory provisions; HSE Offshore Information Sheet No. 2/2006

IAEA_GS-R-2	Preparedness and response for a nuclear or radiological emergency. International Atomic Energy Agency. Safety Standards Series No. GS-R-2. IAEA, 2002, Vienna.
IAEA_INSAG-10	IAEA; International Nuclear Safety Advisory Group, INSAG-10 Defence in Depth in Nuclear Safety, IAEA, Vienna, 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_TM2006	IAEA; Technical Meeting on Effective Integration of Deterministic and Probabilistic Analysis in Plant Safety Management in Barcelona_4-8 September 06;IAEA; 2006.
ICRP_82	Protection of the Public in Situations of Prolonged Radiation Exposure. ICRP Publication No. 82, Pergamon Press, Oxford, 2000, New York.
IEC 62278	IEC 62278, Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
Ilvonen_1994	M. Ilvonen, Software development of models that simulate the dispersion of atmospheric radioactive releases and predict the resulting radiation doses. 119 p. Thesis of diploma, HUT, Information technology, 1994, Espoo. (In Finnish)
Jonkman_2003	Jonkman, S.N., van Gelder P.H.A.J.M., Vrijling, J.K.; An overview of quantitative risk measures for loss of life and economic damage; Journal of Hazardous Materials, Volume 99, Number 1, 4 April 2003, pp. 1-30(30).
Kafka_1999	Kafka, P.; How safe is safe enough? – An unresolved issue for all technologies; Safety and Reliability, Proceedings of ESREL99, Rotterdam, 1999.
Kirchsteiger_1999	Kirchsteiger, C.; On the use of probabilistic and deterministic methods in risk analysis; Journal of Loss Preventation in the Process Industries; Volume 12, Issue 5, September 1999, pp. 399-419
NKS-153	Holmberg, J.-E., Knochenhauer, M.; Probabilistic Safety Goals; Phase 1 – Status and Experiences in Sweden and Finland; Nordic Nuclear Safety Research Report NKS-153, 2006 (issued in parallel as SKI research report 2007-06).
NKS-36	J.-E. Holmberg, U. Pulkkinen; Experience from the Comparison of two PSA Studies; Nordic Nuclear Safety Research Report NKS-36; ISBN 87-7893-087-1; March 2001
NORSOK-Z-013	NORSOK Standard Z-013; Risk and emergency preparedness analysis; Rev.2, 2001-09-01
NPD_Manreg_2002	Regulations relating to management in the petroleum activities (The MANAGEMENT REGULATIONS); http://www.npd.no/regelverk/r2002/frame_e.htm
NSC_2006	NSC, “Report on Performance Goals for Light Water Power Reactors, - on performance goals consistent with safety goals - (in Japanese)”, Special Committee on Nuclear Safety Goals of NSC, March 2006.
OLF_070	OLF 070; Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry; 2004.
Persson_2007	Persson, A; Risk Acceptance Criteria) in the European Railway Industry; Relcon Scandpower; Relcon Scandpower report 32.800.003-R-001; Relcon Scandpower; 2007
Pfitzer_2004	Pfitzer, B., Hardwick, M., Pfitzer, T.; A Comparison of QRA Methods used by DOD for Explosives and Range Safety with Methods used by NRC and EPA; Presentation at the 22nd International System Safety Conference, August 2004.

PSAM9-0428	Knochenhauer, M, Holmberg, J.-E., Gustavsson, H.; Consistency of judgment in usage of safety goals Proceedings of PSAM9 2008, paper 0428; 2008
PSAM9-0443	Holmberg, J.-E., Knochenhauer, M, Rossi, J.; Criteria for assessment of results from level 2 PSA; Proceedings of PSAM9 2008, paper 0443; 2008
R2P2	Reducing risks, protecting people; HSE's decision making process, HSE Books 2001, ISBN 0 7176 2151 0.
Rechard_1999	Rechard, R. P., Historical relationship between performance assessment for radioactive waste disposal and other types of risk assessment; Risk Analysis 19 5 (1999), pp. 763-807.
Rossi_2007	Rossi, J. Evaluation of the level 3 PSA safety goal. Espoo: VTT, 2007, 16 p. (Report VTT-R-04585-07)
SG_Semin_2007	Holmberg, J; Knochenhauer, M; Project Seminar NKS Project "The Validity of Safety Goals, phase 2"; Wednesday November 21, 2007; Relcon Scandpower MoM 32.800.003-P-20071121; Relcon Scandpower; 2006
SKI_SSI_1985	SKI / SSI; Utsläppsbegränsande åtgärder vid svåra härdhaverier; SKI ref 7.1.24 1082/85; SKI / SSI; 1985
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-7.2	Assessment of radiation doses to the population in the environment of a nuclear power plant. Guide YVL 7.2. ISBN 951-712-530-5, STUK 1997, Helsinki.
Ter_Bekke_2006	Ter Bekke, E.C.A.; Risk Criteria – Background Information for Maritime Decision Makers, 2006, TU Delft, Delft.
Trbojevic_2004	Trbojevic, V.M.; Risk Criteria in the UK and EU; Workshop on ALARP and Societal Risk, Loughborough University, 15 September 2004.
Trbojevic_2005	Trbojevic, V.M.; Risk Criteria in EU, ESREL'05, Poland, 27-30 June 2005.
UNISIG_Class1	A number of draft (unofficial) documents produced during work with the UNISIG Class 1 specifications and ESROG Report.
USNRC 1990	Reactor Risk Reference Document, Final Summary Report, NUREG-1150, Vol. 1.
USNRC SECY-01-0009	USNRC; Modified Reactor Safety Goal Policy Statement; USNRC SECY-01-0009; USNRC; 2001
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

Attachment 1. Level 2 and 3 PSA criteria used by different organisations

"limit" = strict criterion, *shall* be fulfilled
"goal" = "target" = "objective" = not strict criterion, *should* be fulfilled

Country	PSA level 2	PSA level 3	Comment
Canada Canadian Nuclear Safety Commission [CNSC_968790]	Small Release: 1000 TBq of I-131 limit f < 10^{-5} per plant (multiple reactors sharing at least one safety system) year goal f < 10^{-6} per plant year Large Release: 100 TBq of Cs-137 limit f < 10^{-6} per plant year goal f < 10^{-7} per plant year		Draft Regulatory Document RD-337. The criteria are the same for any plant (existing or future). However, the numerical values for the frequencies are expected to be one decade higher for existing plants. The definition of "small release" is due to the CANDU technology, where accidents involving a single fuel channel are possible.
Canada Ontario Power generation [Dinnie_2004]	Large release: 1 % of core inventory of Cs-137 limit f < 10^{-5} per reactor year target f < 10^{-6} per reactor year	Latent health effect A hypothetical individual living at a fixed location close to the facility boundary 24 hours per day, 365 days per year and is calculated conservatively as a rate of exposure in Sv/year to the individual multiplied by the probability of a latent health effect/Sv. limit f < 10^{-4} per site per year target f < 10^{-5} per site per year	Utility goals for existing plants
Finland Radiation and Nuclear Safety Authority [STUK_YVL-2.8]	Large release: 100 TBq Cs-137 limit f < $5 \cdot 10^{-7}$ per year		Numerical objective for construction license and operating license of a new unit
Finland Teollisuuden Voima	Large release > 100 TBq Cs-137 Informal objective f < $5 \cdot 10^{-7}$ per year		Utility goal for existing units
Finland Fortum	Large release: 100 TBq Cs-137 Informal target f < 10^{-5} per year derived from the CDF criterion 10^{-4} per year and 10 % value of the CDF applied in the planning of SAM-strategies		Utility goal for existing units

Country	PSA level 2	PSA level 3	Comment
France The French Safety Authority (ASN) [ASN_1977]	Unacceptable consequences: Objective: $f < 10^{-6}$ per year		This criterion has been presented in an authority position paper for 1300 MWe plants. It is an orientation value which is not binding. "Unacceptable consequences" are not specified by legislation or regulation.
Japan The Japanese Nuclear Safety Commission [NSC_2006]	Containment Failure: target $f < 10^{-5}$ per reactor year	Average individual risk, early fatality Members of the public in the vicinity of the site boundary target $f < 10^{-6}$ per year Average individual risk, cancer fatality Members of the public within a certain distance from a nuclear facility target $f < 10^{-6}$ per year.	Proposal. Criteria should be generally applied as reference levels in regulatory activities.
Korea The Korean Nuclear Safety Commission	Tentative regulatory decision until the official issuance of the Criteria Large early release: The rapid, unmitigated large release of airborne fission products from the containment to the environment, resulting in the early death of more than 1 person or causing the severe social effect. for existing plants and life extension: $f < 10^{-5}$ per reactor year for new plants : $f < 10^{-6}$ per reactor year	Policy on Severe Accident in 2001 Average individual risk, early fatality An individual in the vicinity of a NPP target 0,1 % sum of those risks resulting from other accidents Population risk, cancer fatality target 0,1 % sum of cancer fatality risks resulting from all other causes	Proposed target values
Netherlands Law [VROM-1988]		Individual risk (all sources) Limit $f < 10^{-5}$ per year Individual risk (single sources) Limit $f < 10^{-6}$ 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.
Slovakia Nuclear Regulatory Authority of the Slovak Republic [BNS I.4.2/2006]	Large early release: Significant, or large release is defined through the release of Cs -137. Early release is the release of fission products before applying the offside protective measures. Target $f < 10^{-5}$ per year		For existing plants. Criteria for the new plant are lower by one order of magnitude
Sweden SKI [SKI_SSI_1985]	Unacceptable release: > 0,1 % of the inventory of Cs-134 and Cs-137 in a 1800 MWt core excluding noble gases f < extremely unlikely		"Extremely unlikely" interpreted as 10^{-7} per year
Sweden OKG	Release: > 0,1 % of the inventory in a 1800 MWt core excluding noble gases (= SKI definition) f considerably lower than 10^{-5} per year		"considerable lower" can be interpreted as factor 10, i.e., $f < 10^{-6}$ per year

<table>
<tr><th>Country</th><th>PSA level 2</th><th>PSA level 3</th><th>Comment</th></tr>
<tr><td>Sweden
Ringhals</td><td>Release: > 0,1 % of the core inventory of substances causing ground contamination (= SKI definition)
f < 10^{-7} per year</td><td></td><td></td></tr>
<tr><td>UK
HMI
[HMI_SAP_1992, HSE_SAP_2006]</td><td>Large release: > 10 000 TBq I_{131}, > 200 TBq Cs-137
Limit 10^{-5} per year
Objective 10^{-7} per year</td><td>Individual risk
Limit 10^{-4} per year
Objective 10^{-6} per year
Frequency dose targets [1/year]<table><tr><th>On site, mSv</th><th>Off-site, mSv</th><th>Limit</th><th>Objective</th></tr><tr><td>2–20</td><td>0,1–1</td><td>10^{-1}</td><td>10^{-2}</td></tr><tr><td>20–200</td><td>1–10</td><td>10^{-2}</td><td>10^{-4}</td></tr><tr><td>200–2000</td><td>10–100</td><td>10^{-3}</td><td>10^{-5}</td></tr><tr><td>>2000</td><td>>100</td><td>10^{-4}</td><td>10^{-6}</td></tr></table>Societal risk: total risk of 100 or more fatalities
Limit 10^{-5} per year
Objective 10^{-7} per year</td><td>Large release criterion does not appear in the revised version of the document published in 2006.

The targets are not mandatory but, rather, they are guides to inspectors to indicate where there is the need for consideration of additional safety measures.</td></tr>
<tr><td>USA
U.S.NRC
[USNRC SECY-01-0009]</td><td>Large early release:
Existing plants objective f < 10^{-5} per year
New plants objective f < 10^{-6} per year (proposed)</td><td>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.</td><td>Goals on Levels 1 and 2 are subsidiary objectives intended to achieve the same intent as the quantitative health objective (level 3)</td></tr>
<tr><td>IAEA
[IAEA_INSAG-12]</td><td>Large early release: Large off-site releases requiring short term off-site response
Existing plants f < 10^{-5} per year
New plants “Practical elimination”</td><td></td><td></td></tr>
<tr><td>EUR
[EUR_2002]</td><td>Criteria for limiting impact (CLI): An acceptance criterion, given by a comparison of a linear combination of families of isotope releases, versus a maximum value. Each criterion is associated with a specific kind of limited consequence to the public.
f < 10^{-6} per year
Large early release: Earlier or much larger release than CLI
Significantly lower frequency than 10^{-6} per year</td><td></td><td>New plants. Targets established by the utilities. Should be more demanding than current regulatory limits, but that are considered reasonably achievable by modern, well designed plants.</td></tr>
</table>

Bibliographic Data Sheet **NKS-172**

Title	Probabilistic Safety Goals. Phase 2 - Status Report
Author(s)	Jan-Erik Holmberg, Kim Björkman, Jukka Rossi (1) Michael Knochenhauer, Xuhong He, Anders Persson, Helena Gustavsson (2)
Affiliation(s)	(1) VTT, P.O.Box 1000, FI-02044 VTT, Finland (2) Relcon Scandpower AB, 172 25 Sundbyberg, Sweden
ISBN	978-87-7893-238-9
Date	July 2008
Project	NKS-R / Safety Goals
No. of pages	46+3
No. of tables	6
No. of illustrations	14
No. of references	57

Abstract

The second phase of the project, the outcome of which is described in this project report has mainly dealt with four issues:

- Consistency in the usage of safety goals
- Criteria for assessment of results from PSA level 2
- Overview of international safety goals and experiences from their use
- Safety goals related to other man-made risks in society

Consistency in judgement over time has been perceived to be one of the main problems in the usage of safety goals. Safety goals defined in the 80ies were met in the beginning with PSA:s performed to the standards of that time, i.e., by PSA:s that were quite limited in scope and level of detail compared to today's state of the art. This issue was investigated by performing a comparative review was performed of three generations of the same PSA, focusing on the impact from changes over time in component failure data, IE frequency, and modelling of the plant, including plant changes and changes in success criteria. It proved to be very time-consuming and in some cases next to impossible to correctly identify the basic causes for changes in PSA results. A multitude of different sub-causes turned out to combined and difficult to differentiate. Thus, rigorous book-keeping is needed in order to keep track of how and why PSA results change. This is especially important in order to differentiate "real" differences due to plant changes and updated component and IE data from differences that are due to general PSA development (scope, level of detail, modelling issues).

Goals related to CDF and LERF are surrogates to societal risk level criteria. To fully validate these goals, calculations of environmental consequences of release sequences would need to be made. The on-going international survey conducted by the OECD/NEA WG Risk shows that acceptance criteria for results from level 2 PSA differ considerably between countries. Both definitions for large release and probability values differ. Further, the status of criteria differs from mandatory requirements to informal targets. Some countries do not use probabilistic criteria at all.
The probability limits used in level 2 PSA vary from 10-7/year to 10-5/year. The highest criteria (10-5/year) have been defined for old reactors only. For new reactors, targets between 10-7/year and 10-6/year have been defined. These numbers can be compared with risks experienced or accepted otherwise in society.

From the individual risk point of view, these numbers are acceptable. To validate the target values from the societal risk point of view, level 3 PSA assessments need to be made. Results from such assessments are strongly dependent on population data, weather data, and whether or not countermeasures are accounted. The aim of the definition for large release of the severe reactor accident is such that, first of all, the release magnitude shall be reduced to such an amount that no acute health effects are caused in the environment. It follows from this requirement that only stochastic late effects can be expected. The criterion “100 TBq Cs-137” used in Finland and the differently worded but almost identical criterion “0,1 % of the core inventory of Cs-137 in an 1800 MWt BWR” used in Sweden are examples of criteria fulfilling the above requirement. Test calculations with environmental data from a Finnish nuclear power plant site shows that this particular release limit would not cause acute heath effects and that late effects would be minor.

The on-going OECD/NEA Working group RISK task group on probabilistic safety criteria has the objectives to review the rationales for definition, the current status, and actual experiences regarding the use of probabilistic safety goals and other PSA related numerical risk criteria in the member states. The NKS project participates actively in the task. At present, responses have been received to a questionnaire and processing and compilation of answers has been initiated. The activity has already provided valuable input to the NKS project, and is expected to provide further valuable input during the third and final project phase.

In order to provide perspective on the project’s detailed treatment of probabilistic safety goals for nuclear power plants, some information from other areas has been collected, with the focus on the use of probabilistic risk criteria in European offshore oil and gas operations and in the European railway industry.
In offshore oil and gas operations both the number of precursor events requiring handling and of accidents requiring mitigation is high compared to the nuclear industry, resulting in a relatively high focus in the criteria on consequence mitigation. Criteria have a large scope, i.e. they apply to a wide range of accident events and consider a wide range of safety functions. Defence in depth aspects are considered in the criteria by stating requirements for different safety functions. Finally, the ALARP principle is often applied, involving a safety goal with a limit and an objective.
For European rail systems, a standardisation of safety goals has been prompted by the expressed aim of making it possible for trains and personnel to cross national borders. The harmonisation has been achieved by letting an industry working group propose safety goals, which have then been accepted by authorities. The goals suggested are consensus requirements based on an amalgamation of national practices, mainly from Germany and France. Basic principles are based on comparison to general health risk (MEM principle) and a requirement for continuous improvement of safety (GAMAB). Systematic procedures are in place for creating subsidiary goals, which is done by defining a tolerable hazard rate (THR) for each subsystem forming part of the overall system. Finally, it is worth noting, that a framework for cross-acceptance is under development, i.e., development of an agreed common approach for demonstrating the safety levels of the railway system (in addition to the common risk criteria already in place).

Key words Safety Goals, PSA, Safety Targets, ALARP, Decision criteria, Risk informed decision making

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@nks.org, www.nks.org