Title	Comparison of risk criteria in safety-critical industries
Author(s)	Knochenhauer, Michael; Persson, Anders; Holmberg, Jan-Erik; He Xuhong
Citation	Proceedings of PSAM 10 International Probabilistic Safety Assessment & Management Conference, 7-11 June 2010, Seattle, Washington, USA, pp. Paper 17
Date	2010
Rights	This article may be downloaded for personal use only

Comparison of Risk Criteria in Safety-Critical Industries

Michael Knochenhauer[a*] and Anders Persson[a], Jan Erik Holmberg[b], and Xuhong He[c]
[a]Scandpower – Lloyd's Register, Stockholm, Sweden
[b]VTT Technical Research Centre of Finland, Espoo, Finland
[c]Scandpower – Lloyd's Register, Beijing, PR China

Abstract: The paper describes the results from a sub-project within a Nordic research project dealing with probabilistic risk criteria for nuclear power plants (NPP). In order to provide perspective on the project's detailed treatment of probabilistic risk criteria for NPP:s, and to make it possible to relate these to risk criteria defined and applied in other safety-critical industries, criteria defined and used within the European railway and offshore oil and gas industries have been discussed in some detail and compared to NPP criteria.

Keywords: PSA, Probabilistic Safety Criteria, Safety Targets, Safety Goals

1. INTRODUCTION

The outcome of a risk analysis is a combination of qualitative and quantitative results. Risk criteria are applied to support the assessment of the acceptability of the risk. High level risk criteria are expressed in form of societal risk, group risk or individual risk goals. In some industries, like the nuclear field, lower level system failure risk criteria are in use.

It is of great importance that risk criteria are soundly based, that they can be effectively and unambiguously applied, and that they can be accepted and understood by all parties concerned. The types and levels of the risk criteria differ between different countries and industries. There are also differences in the definition of the risk criteria, and in the formal status of the criteria, i.e., whether or not they are mandatory.

In some countries like the Netherlands and UK same regulatory criteria are applied to all safety-critical industries, but in many other countries the criteria are dependent on the industry practices. This paper gives an overview of risk criteria used in the nuclear industry, European railway and offshore oil and gas industries. A survey of risk criteria has been made within a Nordic project dealing with the use of probabilistic safety criteria for nuclear power plants [1]. The project is performed during the period 2005-2009. It was initiated by NKS (Nordic Nuclear Safety Research) and NPSAG (Nordic PSA Group), and has relations to an OECD/NEA WGRisk task on probabilistic safety criteria in the NEA member countries.

2. SAFETY GOALS IN THE NUCLEAR INDUSTRY

2.1. Introduction

A comprehensive summary of the status of probabilistic safety criteria for nuclear power plants has been published by the OECD/NEA [2].

2.2. Overview of probabilistic safety criteria for nuclear power plants

Basically, three levels of risk criteria exist within the nuclear industry, i.e.:

– at society level (mainly qualitative),

[*] mkn@scandpower.com

- at an intermediate level (quantitative and/or qualitative), and
- at a technical level (quantitative).

The higher level criteria are concerned with the actual risk to society or individuals, or to the environment. Technical criteria are generally quantitative (probabilistic) and mostly on lower levels (subsidiary). They typically concern core damage, unacceptable release, and unacceptable health risks. In later years, some countries have defined separate criteria to address robustness in defence in depth, e.g., by having a separate criterion for reactor containment integrity.

There are considerable differences in the status of the numerical risk criteria that have been defined in different countries. Some have been defined in laws or regulations and are mandatory, some have been defined by the regulatory authority or by an authoritative body, and some have been defined by plant operators or designers. Hence the status of the criteria ranges from mandatory requirements to informal. In most countries that have criteria both for existing and new reactors, the criteria are stricter for new plants. In some cases this is expressed by using the same numerical values for the frequencies, but applying them as limits for new plants and objectives for existing plants.

Regarding consideration of uncertainties, there is consensus that the comparison with probabilistic safety criteria should use the “best estimate” of the results of a probabilistic safety assessment (PSA).
In most cases, risk criteria for operating plants are applied when the PSA is updated, which in done with very differing intervals, as some countries require PSA updates only every 10 year within so-called periodic safety reviews, while others do updates on a yearly basis. Risk criteria are also used to assess the impact on risk of design modifications in the plant.

Risk criteria are mostly considered as indicators or orientation values, meaning that no regulatory actions are expected on non-compliance with a probabilistic safety criterion. Practically, there is a consensus on finding the reasons for the non-compliance and identification on the way to overcome it. However, for new builds application of risk criteria would be stricter.
When it comes to the interpretation of the criteria, more work is needed in the definition of the various criteria. Thus, there seems to be a need for a common definition as to what constitutes severe core damage and large release. A strict and common definition would facilitate comparison of risks and results between different plants.

The general experience from the implementation of risk criteria is positive, and various benefits have been recorded. In a number of cases, design weaknesses or procedural weaknesses in NPPs have been identified using PSA and PSA criteria, resulting in the introduction of safety improvements. In many cases, the implementation of risk criteria and safety goals has lead to plant modifications in order to meet the probabilistic risk criteria. The implementation of safety goals often emphasizes the need for more detailed and realistic PSA models, and it appears that the use of safety goals has increased the focus on the correctness and quality of PSA models.

Figures 1 and 2 show the probabilistic criteria that are in use in the countries participating in the OECD/NEA task. Criteria are presented on the levels of core damage and unacceptable release. It is worth noting that the definitions of an “unacceptable” release vary considerably among the countries.

2.3. Conclusions

Safety goals for nuclear power plants are defined in different ways in different countries and also used differently. Many countries are presently developing them in connection to the transfer to risk-informed regulation of both operating nuclear power plants and new designs.

It is far from self-evident how probabilistic safety criteria should be defined and used. On one hand, experience indicates that safety goals are valuable tools for the interpretation of results from a PSA, and they tend to enhance the realism of a risk assessment. On the other hand, strict use of probabilistic criteria is usually avoided. A major problem is the large number of different uncertainties in PSA model, which makes it difficult to demonstrate the compliance with a probabilistic criterion.

Furthermore, it has been seen that PSA results can change a lot over time due to scope extensions, revised operating experience data, method development, or increases of level of detail, mostly leading to an increase of the frequency of the calculated risk. This can cause a problem of consistency in the judgments.

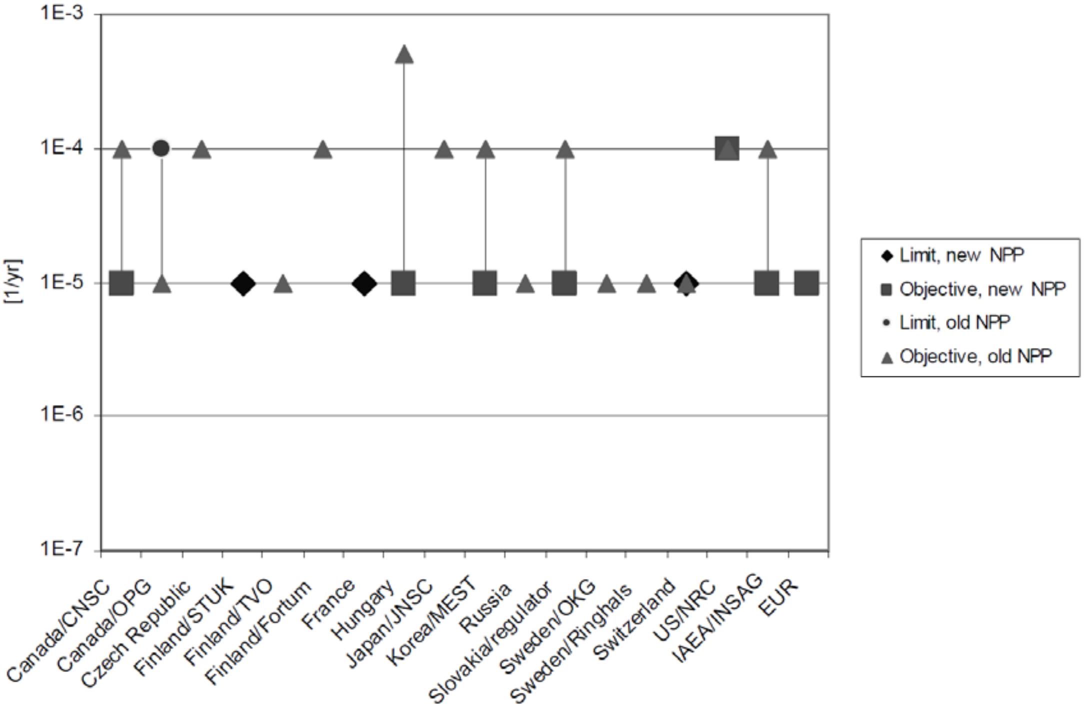

Figure 1. Probabilistic criteria defined for the frequency of reactor core damage accident

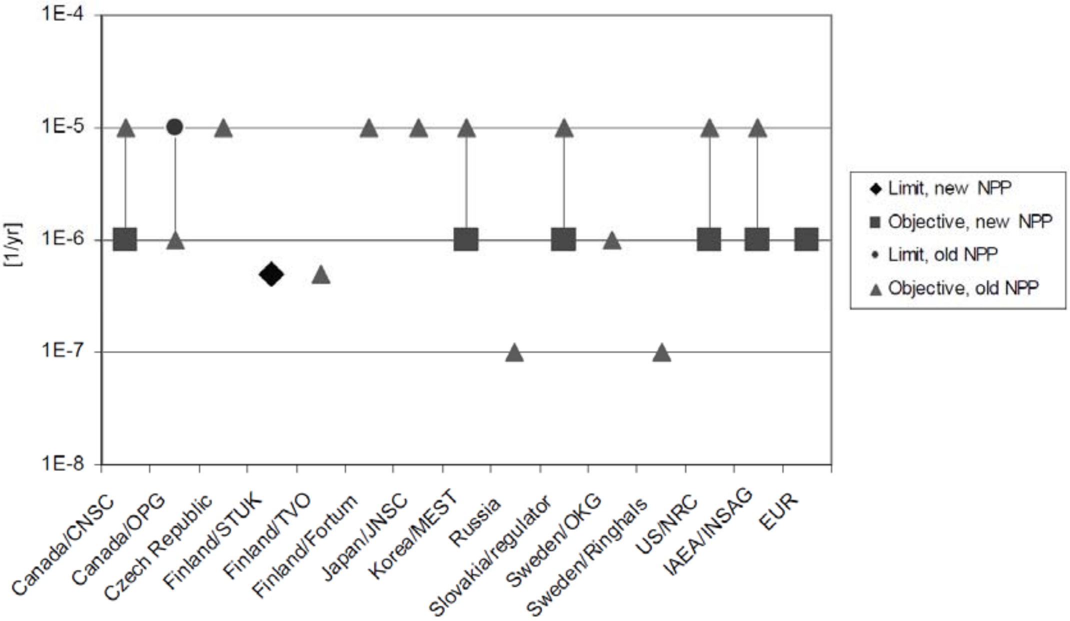

Figure 2. Probabilistic criteria defined for the frequency of large release of radioactivity from a nuclear power plant

3. SAFETY GOALS IN THE EUROPEAN OFF-SHORE OIL AND GAS INDUSTRY

3.1. Introduction

A survey has been made of the regulatory and industry requirements in the Oil and Gas industry for defining Risk Acceptance Criteria (RAC). The focus has been on Norwegian and UK offshore oil industry. RAC may be qualitative or quantitative, and are known variously in the Oil and Gas industry as, e.g., “risk criteria”, “decision criteria”, “screening criteria”, and “tolerability criteria”.

3.2. Risk acceptance criteria in the Norwegian oil and gas industry

The Norwegian Petroleum Safety Authority 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 requires the operator to define acceptance criteria for major accident and environmental risks [3]. RAC shall be defined for personal risk to workers and to third party, loss of main safety functions, and environmental effects from the facility.

The NORSOK standards are developed by the Norwegian petroleum industry, and the NORSOK standard Z-013 presents some general requirements regarding the formulation of RAC [4]. This standard does not provide any guidelines on what actual values to choose for RAC, which is in line with the basic Norwegian PSA requirements, 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 RAC defined should represent a compromise where the following qualities are satisfied as far as possible:

- Suitable for decisions regarding risk reducing measures.
- Suitable for communication.
- Unambiguous in their formulation (no need for extensive interpretation or adaptation for a specific application).
- No favouring of any particular concept solution explicitly or implicitly through the way in which risk is expressed.

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

<u>Individual Risk Criteria for Workers</u>

- The average individual risk, expressed by the fatal accident rate (FAR, number of fatalities during 100 million exposure hours), must meet the criterion FAR < 10.
- For specially exposed groups, the average group individual risk, must meet the criterion FAR < 25.

<u>Individual Risk Criteria for 3rd Party</u>

- 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.

<u>Group Risk Criteria for 3rd Party</u>

- The criterion (limit) for 3rd party societal risk is F(N) = 1/(100*N),
where F(N) is the cumulative frequency for N or more fatalities.
- The ALARP objective is defined at a level two orders of magnitude below the limit.
- This is illustrated graphically in Figure 3.

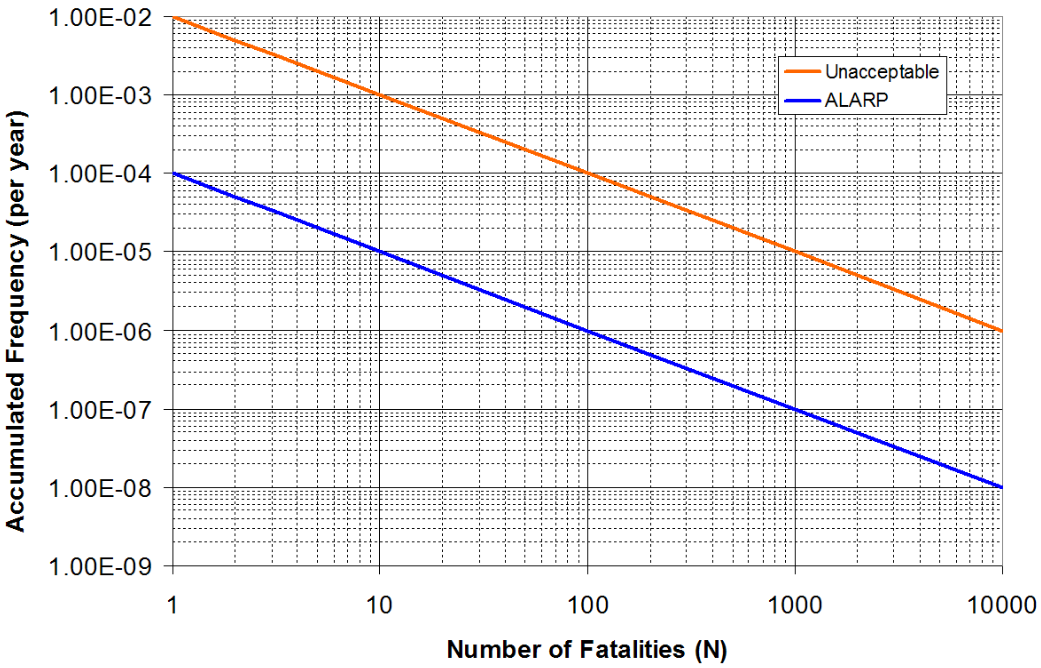

Figure 3. Risk Acceptance Criteria for 3rd party Societal Risk (Norwegian Continental Shelf)

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 1·10-4 per year per safety function and per accident category, see Table 1.

Table 1. Accident categories and main safety functions

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

3.3. Risk acceptance criteria in UK regulations

The risk acceptance criteria used by the UK petroleum industry have mainly been formulated by the UK Health and Safety Executive (HSE) and are embodied in statutory legislation. The Offshore Installations Safety Case Regulations 2005 [5] requires the duty holder 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 are defined as [6]:

- 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.

Temporary Refuge Impairment Criteria (Group risk)
Although there is no specific requirement to estimate group risk, the assessment principles for offshore safety cases [7] indicates a need for a safety case to demonstrate temporary refuge (TR) integrity - this could be considered as a measure of societal risk.

The TR integrity requirement is stated in [8], and requires a demonstration that the frequency with which accidental events will result in a loss of TR integrity, within the minimum stated endurance time, does not exceed the order of 1 in 1000 per year. No ALARP objective is stated, but this frequency is required to be reduced to a lower level wherever reasonably practicable. Where the frequency is close to the limit of 1 in 1000 per year, acceptance that further risk reduction measures are ‘grossly disproportionate’ should be only on the basis of a very rigorous demonstration.

3.4. Discussion

Risk acceptance criteria have been used 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 that they make interpretation of the results of a risk assessment explicit and traceable.

However, there have also been some discussions about the suitability of risk acceptance criteria to assess and control risks [9]. One concern is that the introduction of pre-determined criteria may give the wrong focus to risk assessment activities, i.e., on meeting risk criteria rather than on obtaining overall safe and cost-effective solutions and measures.

Another issue regarding 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 [4] states that the comparison to RAC should usually be made in relation to ‘best estimate’ from the risk analysis rather than to some level of confidence.

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.
- Some of the concerns are similar to the ones encountered in the nuclear field, e.g., that too much focus on meeting strict acceptance criteria may divert attention from an unbiased safety assessment to the “mere” fulfilment of the stated goals.

4. SAFETY GOALS IN THE EUROPEAN RAILWAY INDUSTRY

4.1. Introduction

An overview has been made of the background and status of safety goals in the European railway industry. A railway system can be defined very widely, but in this context the system looked upon is the European Train Control System (ETCS). ETCS is the Automatic Train Protection (ATP) 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.

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. Typically, different countries have recognized different principles. Thus, MEM is mainly practiced in Germany, ALARP in the UK, and GAMAB/GAME in France. The principles are shortly described below.

MEM / Minimum Endogenous Mortality

The basis for 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 $2 \cdot 10^{-4}$ death/person/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 its 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 5% of the MEM, i.e., $1 \cdot 10^{-5}$ death/person/year, which translates to about $1 \cdot 10^{-9}$ death/person/hour.

ALARP / As Low As Reasonable Practicable

According to the ALARP principle, described in a general way in IEC 62278 [10], three areas of risk, divided by certain limits, have to be considered:

The unacceptable region

- The upper bound (limit) defines levels of risk that are intolerable.

- Risks above the limit are so large and their outcomes so unacceptable that they are intolerable and cannot be justified on any grounds.
- If the level of risk cannot be reduced below this bound then the operation should not be carried out.

The ALARP or tolerability region

- The area between the upper and lower bounds is called the ALARP region.
- It is not sufficient to demonstrate that risks are in the ALARP region; they must also 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.

The broadly acceptable region

- The lower bound (objective) of the diagram defines the broadly acceptable region.
- Here, 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.

IEC 62278 does not present any quantitative targets for the ALARP principle but in draft documents for the UNISIG work [11] one can see that the ALARP principle defines target values around the level of 1,14·10-9 death/person/hour as an upper limit (objective), which is similar to the results of applying 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, by the requirement "at least", requires implicitly a progress to be made in the projected system. 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.

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. This brings 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 (ERTMS Safety Requirement and Objective Group) to request safety experts from the German and French railways (DB and SNCF) to set up independent studies to define 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 was the GAMAB/GAME principle, taking into account the performance, operating experience, and accident statistics of existing railway systems. 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 person to suffer an accident with fatal consequences while travelling in a train.
- $\text{TIRF}_{\text{ETCS}}$ = 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.

The work performed by DB AG and SNCF showed quite large differences between the results. These differences were assessed by an Independent Assessment Committee and a number of differences in the approach taken for the calculations were identified. It was agreed within ESROG 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 requirements corresponding to safety integrity level 4 (SIL 4) 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.

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, as defined in the previous section. 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. Thus, when going from TIRF to THR the definition is transferred to be more attached with 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 is set to $2.0 \cdot 10^{-9}$/hour/train. This safety target is defined in the Technical specification for interoperability (TSI) for Control-Command and signalling, and is a legal requirement [12].

4.5. Responsibilities

The responsibility for establishing safety targets for railway systems is described in the standard EN 50129 [13] 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 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.

4.6. Verification

The verification against the THRETCS 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 [14], which qualitatively analyses the top hazard. The fault tree will be adapted by the supplier 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.

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 railway safety authorities will have to perform their own assessments in order to accept a system, or parts of it, even if they have been developed and proven safe in other EU member states.

To allow cross-acceptance of railway systems between EU member states, the methods used for the identification and the management of system hazards and risks need to be harmonised within the EU. In order to promote and improve the compatibility and competitiveness of railways in the EU, the European Railway Agency (ERA) was formed, with defined tasks for interoperability and safety. ERA is in the process of developing measures that concern common safety methods and common safety targets (CST), definition of common safety indicators (CSI) and harmonization of documents related to safety certification [15].

4.8. Conclusions

The following are some general conclusions regarding safety criteria 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 have been proposed by an industry working group, and accepted by authorities.
- Consensus requirements are 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 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). To achieve this, the methods used for the identification and the management of system hazards and risks have to be harmonised.

5. CONCLUSION

In the nuclear energy industry, the scope of risk criteria includes the whole range of risk criteria from societal and individual risk, off-site radioactive release, reactor core damage accident and lower level criteria to numerical criteria used in various risk-informed applications. Risk criteria have variable status in different countries; strict regulatory limits are defined in few countries, while indicative target values are used in most countries. The ALARP principle is sometimes applied, involving a risk criterion with a limit and an objective.

In the offshore oil and gas industry, both qualitative and quantitative 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. It is worth noticing that both the number of precursor events requiring handling, and the number of accidents requiring mitigation is high compared to the nuclear industry, resulting in criteria with a relatively high focus 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. There is also more focus than in the nuclear industry on the different phases of the operation (design, construction, operation, maintenance, decommissioning). Defence in depth aspects are considered in the criteria by stating requirements for different safety functions. Finally, like in the nuclear energy context, the ALARP principle is often applied.

For European rail systems, a standardisation of risk criteria 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 risk criteria, which have then been accepted by authorities. The criteria suggested are consensus requirements based on an amalgamation of national practices, mainly from Germany and France. Basic principles relate to a 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., an agreed common approach on European level for demonstrating the safety levels of the railway system.

Acknowledgements

We thank the NKS (Nordic nuclear safety research) and the members of NPSAG (Nordic PSA Group) and SAFIR-2010 (The Finnish Research Programme on Nuclear Power Plant Safety) for financial support of the project as well as for other input.

References

[1] Holmberg, J.-E. and Knochenhauer, M., 2008, *Probabilistic Safety Goals. Phase 2 Status Report*; Nordic Nuclear Safety Research Report NKS-172, 2008

[2] OECD/NEA WGRISK; *Probabilistic risk criteria and Safety Goals*; NEA/CSNI/R(2009)16 December 2009

[3] NPSA 2002; *Regulations relating to management in the petroleum activities (The Management Regulations)*; Norwegian Petroleum Safety Authority, 2002

[4] NORSOK 2001; *Risk and emergency preparedness analysis*; NORSOK Standard Z-013 Rev.2, 2001-09-01

[5] HSE; *The Offshore Installations (Safety Case) Regulations 2005*; UK Statutory Instrument 2005 No. 3117

[6] HSE; *Reducing Risks, Protecting People. UK HSE's decision making process*; ISBN 071762151-0; HSE 2001

[7] HSE; *Assessment principles for offshore safety cases (APOSC)*; HSE 2006

[8] HSE; *Offshore Installations (Safety Case) Regulations 2005 Regulation 12 Demonstrating compliance with the relevant statutory provisions*; HSE Offshore Information Sheet No. 2/2006

[9] Aven, T. and Vinnen J.-E. (2005); *On the use of risk acceptance criteria in the offshore oil and gas industry*; Reliability Engineering and System Safety, 90 (2005): 15-24.

[10] IEC 62278; *Railway applications – Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*; IEC 1999.

[11] UNISIG (1999); *A number of draft (unofficial) documents produced during work with the UNISIG Class 1 specifications and ESROG Report*; UNISIG 1999.

[12] EC (2006); *Technical specification for interoperability relating to the control-command and signalling subsystem*; 2006/860/EC; EC 2006

[13] EN 50129; *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

[14] UNISIG (2000); *ETCS Application Level 2 – Safety Analysis, Part 1 – Functional Fault Tree*; UNISIG subset-088, part 1

[15] ERA; *ERA recommendation on the first set of Common Safety Targets as referred to in Article 7 of Directive 2004/49/EC*; European Rail Agency; ERA/REC/03-2009/SAF; September 2009