QUANTITATIVE SAFETY GOALS AND CRITERIA AS A BASIS FOR DECISION MAKING

Heinz-Peter Berg.

•

Bundesamt für Strahlenschutz, Salzgitter, Germany

e-mail: hberg@bfs.de

ABSTRACT

Internationally, probabilistic safety analyses represent the state of the art in the licensing process for new industrial facilities, but increasingly also for evaluating the safety level of older industrial plants, e. g. as part of periodic safety reviews of nuclear power plants. Quantitative safety goals have not yet reached the same level of acceptance. However, this depends on the type of industry. Most of the countries consider those criteria as safety targets rather than as sharply defined boundary values. The Netherlands and the United Kingdom are exceptions, they require demonstration of compliance with legally binding safety goals in the licensing procedure.

1 INTRODUCTION

1.1 General

Originated for applications in the nuclear industry, quantified risks and hazard analysis techniques are emerging as powerful tools for the safety management of hazardous plants in the process industry (chemical, petrochemical, petroleum and related industries).

Although the concept remains similar, i.e. is a probabilistic approach to risk quantification, there are apparent variations in methodological practices and particularly in the range of applications, focus and emphasis in the implementation of these tools for the different industries. This probably stems from the fundamental difference between the nuclear industry, essentially a one process industry, and the process industry which is characterized by a multitude of interdependent processes where raw materials undergo physical and chemical changes.

The more apparent variation between quantified risk and hazard analysis in the process industry and probabilistic safety assessment (PSA) in the nuclear industry lies in the relatively narrower range of applications of these tools in the process industry when compared to the more extensive use made use made by the nuclear industry in implementing PSA at the design and operational stages of nuclear power plants including plant changes (Cepin 2004, 2007).

There is much debate about the concept of acceptable risk. The question what level of risk should be tolerated and who determines acceptability is still controversial in the area of safety management. The importance of communicating is illustrated by the differential in willingness to tolerate risks from different sources, independent from benefit considerations, and the differential in willingness to accept types of risks between different groups of individuals.

The concept that some level of risk is tolerable is fundamental to risk assessment and risk management (Kumamoto 2007). Without the definition of such a tolerable risk criterion, risk assessment may be hampered in terms of decision making and formulation of risk management strategies. The setting of and adherence to precise and rigid criteria, however, does not acknowledge the limitation in accuracy of methodologies, nor does it allow for appropriate consideration of the benefits against which the acceptability of the risk may be assessed in each case. Furthermore, the extent of compliance with any risk criteria should not be the sole basis for evaluating the success of risk management measures. Other criteria include: the extent of risk and risk reductions achieved, the cost of risk reductions in social, economic and environmental terms, and the cost effectiveness of control measures.

As such, while debate will probably continue on the appropriateness of quantitative risk criteria as a measure of tolerability, future applications of quantitative risk assessment will greatly benefit from focusing more on the assessment process itself and the interpretation of such criteria as a target guideline.

As demonstrated by the wide spectrum of applications, the fact is illustrated that in the nuclear industry uses of PSA for other than compliance with formal criteria dominate. Some countries which operate nuclear power plants apply numerical safety objectives / criteria / rules / goals. The role and interpretation of such quantitative guidelines vary from country to country. A dominant opinion is that "the safety goals should not be used within a regulatory framework of strict acceptance or non-acceptance criteria but should be considered as one factor in arriving at regulatory judgement".

1.2 Scope and purpose of the paper

The probabilistic safety analysis as already explained is the most powerful approach to quantification of risk and safety where risk is a combination of probability of harm and severity of that harm, while safety is freedom from unacceptable risk (Kumamoto 2007).

Basically, any plant, activity or item should be designed and operated in such a way as to satisfy a given set of safety goals. This is a goal-oriented approach where goals are first specified, and then the plant, activity or item is designed, created, operated and maintained accordingly. However, two problems must be answered for the goal-oriented approach:

1. How safe is safe enough? This requires a set of safety goals to be satisfied.
2. How to deal with uncertainties? The current risk quantification involves significant uncertainties.

The target discussed in this paper is mainly focused on a nuclear power plant. However, the implications can certainly be translated into other fields including process, aerospace, machinery, and automobile industries. Prevention of core damage in a nuclear power plant corresponds in general to prevention of vehicle collision (active safety), and accident mitigation by a containment structure corresponds to collision mitigation by an air bag (passive safety). However, one has to have in mind the more catastrophic consequence of a core damage compared with a vehicle accident. Prevention coupled with mitigation is an indispensable element of the defense-in-depth philosophy to cope with the uncertainty of current risk quantification.

Although the use of quantitative safety goals is sometimes questioned see for example (Aven & Vinnem 2005) and (Hokstad et al. 2004), many industries and countries have introduced such goals or criteria. This is due to the fact that probabilistic safety analysis is part of safety assessment to be submitted to the competent authority or licensing institution. This immediately rises the question how to assess the results, even in case – as in Germany – where no quantitative safety goals are determined.

The main underlying problem is that the quantitative results had to be evaluated together with the content, assumptions, models and data used which normally does not allow an easy comparison with the result of another plant or activity. Therefore, people performing a probabilistic safety analysis have to be aware to provide a very carefully elaborated analysis with high quality because the results may lead to costly technical changes or the shutdown of the respective plant. On the other hand, it is the responsibility of those performing risk assessment not to tailor the numbers used in the analysis to ensure that the results do not exceed the given goals.

2 PROBABILISTIC SAFETY ANALYSIS AND PROBABILISTIC SAFETY CRITERIA FOR THE NUCLEAR INDUSTRY

2.1 Methods and results of PSA

For historical reasons, the safety philosophy in the nuclear industry is mainly based on deterministic principles such as

- A multi-level safety concept ("defense in depth") with engineered safety systems to prevent or control anomalous events,
- ‘Conservative’ design, i. e. preference for proven technology and ample design margins
- Multiple barriers against the release of radioactivity,
- Redundant and diverse safety systems of high reliability.

The safety-related requirements which are the base of the plant safety design, are derived from events which are defined so that they represent in each case a whole class of similar events in an enveloping way.

In contrast, it is the essential task of the PSA also to determine the probability of occurrence of event sequences that are not covered by the design base and consequently cannot be assumed to be controlled by the engineered safety systems (Berg 1995). This goal is achieved by means of the accident sequence development analysis, an analysis tool which contains the following essential elements:

- Initiating event analysis,
- Definition of the event sequences and supporting analyses (e.g. thermo-hydraulic model calculations, success criteria analysis),
- Quantification of the probabilities of occurrence of the various event sequences with the aid of fault tree analyses.

Depending upon the nature of the initiating event and the plant status at the time of its occurrence, those functions of the operating and safety systems as well as the manual actions have to be determined that are planned for the control of the event sequence and are required. Inputs are the initiation or trip criteria for the safety systems; manual control actions of the operating staff can be also considered. The different sequences, that result depending on the availability (function or non-function) of these systems are to be represented in the form of event tree diagrams. The availability of a system function is derived quantitatively either from the operational experience or from fault tree analyses, by which the availability of a system is calculated from its logical structure and availability data based on operating experience for sub-units or components, respectively.

It is usual to distinguish three levels of PSA:

- Level 1: The analysis focuses on the responses from operating and safety systems to different initiating events. The end point of the analysis is either the occurrence of a core damage state or the stabilization of the plant state such that a core damage state is prevented.
- Level 2. Starting from the results of level 1 the physical processes of the accident progression post core damage are analyzed. Probabilities are determined for timing and mode of containment failure as well as for the release of radioactivity within the plant as well as for the source term for a release into the environment, determination of the time frame when a certain release is to be expected is of particular importance in this case.
- Level 3: Starting from the probabilities for releases as determined in level 2, the probabilities and extent of damages in the environment of the plant are determined as individual risk, dependent on the distance from the plant, as a complementary frequency distribution of individual risks (counting early fatalities only or including somatic late damages) or as a complementary frequency distribution of the collective dose.

2.2 Quantitative probabilistic safety criteria

In a PSA, safety relevant event sequences and the interaction of the safety systems are modelled for an entire plant. Accordingly, bottom line results do refer to the behaviour of the entire plant, not only to the reliability of single engineered safety systems or components. Those may be subject to design rules or the nuclear safety standards or other technical regulations containing quantitative reliability requirements. The most important of these integral results were:

- Total frequency of core damage states (Core Damage Frequency, CDF),
- Frequency of activity releases due to accidents, most important the Large Release Frequency (LRF). The latter may be defined in different ways as an activity release that requires immediate mitigation measures outside the plant (one typical definition: release of > 0,1 % of the core fission product inventory),
- Frequency of accident-caused damages and/or exposures.

These PSA result formats allow the evaluation of plant safety. They may be used together with results from the deterministic part of a Periodic Safety Review (PSR). Different strategies are followed in different countries (Görtz et al. 2001). The following basic strategies can be distinguished:

1. The PSA results can be used as additional information, without any change of the existing design rules and the regulatory framework which are the base for regulatory decisions in each individual case.
2. In addition to the existing design rules and the code of safety standards, requirements regarding quantitative PSA results are set (Example: The CDF is not to exceed a set limit).
3. Some of the existing design rules and/or safety standards are replaced by requirements that refer to quantitative PSA results.

Implementing these basic modes in national regulatory practice, numerous variants are possible, in particular with regard to the relative weight PSA results are accorded in the safety review process, the specific requirements regarding certification of safety in the review process and the applications of the results. In the chronological course transitions are conceivable between the basic modes. Typical pitfalls encountered when quantitative PSA results are added onto existing deterministic safety standards are shown in Figure 1.

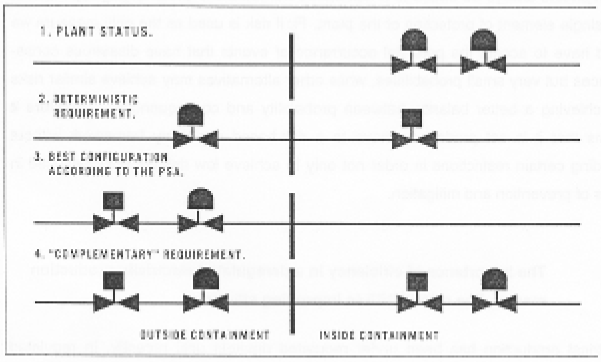

1. PLANT STATUS.
2. DETERMINISTIC REQUIREMENT.
3. BEST CONFIGURATION ACCORDING TO THE PSA.
4. "COMPLEMENTARY" REQUIREMENT.
OUTSIDE CONTAINMENT
INSIDE CONTAINMENT

Figure 1. Possible pitfalls of "complementary" use of PSA-results (Villadóniga 2001).

2.3 International recommendations

2.3.1 IAEA

Quantitative probabilistic criteria were included in (INSAG 1999) and complemented with the annotation that for future plants 'another objective ... is the practical elimination of accident sequences that could lead to large early releases ... '. The recommendations of INSAG were adopted into IAEA Safety Guide No. NS-G-1.2 (IAEA 2001) in a more explicit form:

– 'Core damage frequency: For this, INSAG ... has proposed the following objectives:
–10^{-4} per reactor-year for existing plants,
–10^{-5} per reactor-year for future plants. '

– '... Large radioactive release. The following objectives are given:
–10^{-5} per reactor-year for existing plants,
–10^{-6} per reactor-year for future plants. '

Furthermore, the IAEA recommended in (IAEA 1992) to distinguish three regions as shown in Figure 2.

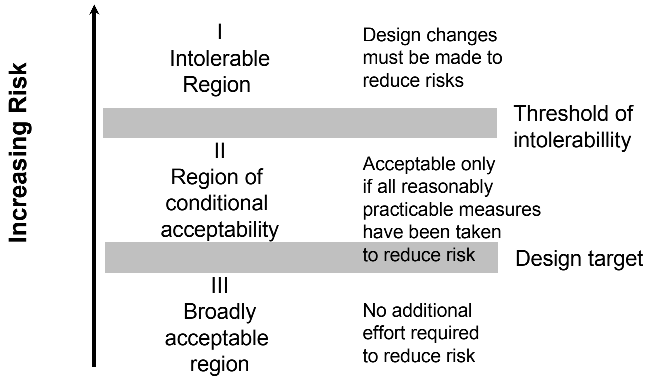


Figure 2. IAEA guidance on acceptance criteria.

This general scheme described has been implemented in various countries (see 2.4).

Figure 3 shows Decision Regions for strategic risk-informed decision making (RIDM) according to (IAEA 2007) The axis is CDFBL-A; it accounts for anticipated routine configurations for activities during the year. The ordinate is ΔCDF, accounting for a change in the CDF, the annual average CDF above CDFBL-0 as a result of a specific activity or situation being evaluated.

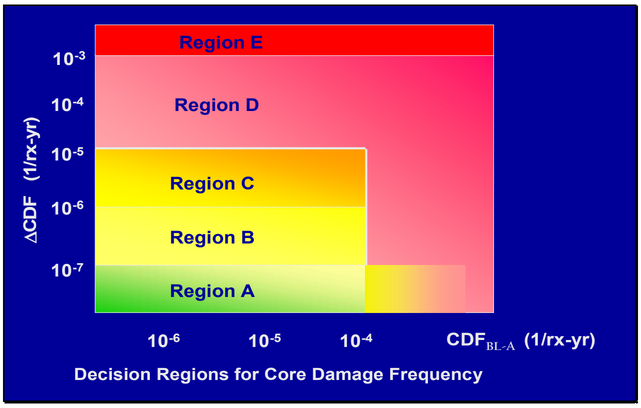


Figure 3. Strategic RIDM Decision Regions for CDF.

There are five decision regions, A to E in Figure 3:

- Results clearly inside Region A are considered to be normal operation and would be within the purview of licensed operators or equivalent.
- Results in Region B would be within the purview of facility management with possibly some regulatory approval depending upon the application, the facility license, and the regulatory structure.
- Results in Region C would require regulatory approval or licensed control depending upon the regulatory structure.
- Results in Region D would not normally be permitted and would always require regulatory approval. The regulatory authority would not normally permit operation in Region D.
- Results in Region E would not be permitted. Immediate action must be taken to remove operation from Region E, or the facility must be immediately shutdown in an orderly manner.

2.3.2 OECD/NEA

In (NEA 2007 a) it is underlined that regulatory bodies have the legal duty and authority to make final safety judgments on all nuclear activities under their responsibility. In a practical sense a nuclear activity is deemed to be safe if the perceived risks are judged to be acceptable. But the regulator can never have a certain quantitative assessment of the risk involved. Therefore, in arriving at its safety judgements, the regulatory body must be guided by the basic safety criteria embedded in its national laws, regulations and policies. One of these criteria is the level of safety protection required by the regulator. There are various statements of the basic level of safety required by OECD/NEA countries, but they all acknowledge that it is not possible to achieve absolute safety (i.e., zero risk) in nuclear activities. Some of these criteria are (see NEA 2007 a):

- no unreasonable risk,
- adequate protection of public health and safety,
- risk as low as reasonably practicable,
- safety as high as reasonably achievable,
- limit risk by use of best technologies at acceptable economic costs.

A related safety criterion is the degree of assurance needed by the regulator that the basic level of safety protection is being met. Here again, there are various formulations of this criterion among OECD/NEA countries.

In 2007 OECD/NEA has published a very exhaustive report on 'The Use, and Development of Probabilistic Safety Assessment (NEA 2007 b), compiled by the Working Group on Risk Assessment (WGRisk) of the Committee on the Safety of Nuclear Installations (CSNI). This report describes the current status of PSA programs in the member states, including general background information, rules and guidelines, different uses of PSA, essential results of recent analyses, brief descriptions of retrofits of plants initiated by PSA results and current topics from R & D in the field. The report is meant as a description of the current state of the art in the member states. A separate chapter, is dealing with quantitative safety criteria. The main statements are summarized in the following.

There are differences in the status of the numerical safety criteria that have been defined in different countries. Some have been defined in law and are mandatory, some have been defined by the regulatory authority (which is the case in the majority of countries where numerical safety criteria have been defined), some have been defined by an authoritative body such as a Presidents Commission and some have been defined by plant operators or designers. Hence there is a difference in the status of the numerical safety criteria which range from mandatory requirements that need to be addressed in law to informal criteria that have been proposed by plant operators or designers for guidance only.

There are a variety of reasons for defining the criteria which includes:

– a change in the law to introduce risk management into the environmental policy,

– the need to define an acceptable level of safety for nuclear power plants following an accident,

– a recommendation from a public enquiry to build a new plant,

– the need for guidance for improving old plants or designing new ones.

In some countries, high level qualitative and quantitative guidance has been defined and the has been used to derive lower level or surrogate criteria than are easier to address and are sufficient to demonstrate that the higher level criteria are met.

In some countries, criteria have been defined for existing plants and for new plants. In general, the expectation is that the target/ objective for the level of risk from a new plant should be about an order of magnitude lower than for existing plants.

In a number of countries no numerical safety criteria have been defined. However, there is a general requirement that the level of risk should be comparable to (or lower than) the risk from existing plants for which a PSA is available.

In most of the countries in which numerical safety criteria have been defined they have been defined as a “target”, an “objective” or a “goal” where the recommendation is that the risk should be lower than the prescribed value with no guidance given on what action needs to be taken if it is exceeded.

The way that the safety criteria have been defined ranges from high level qualitative and quantitative requirements relating to individual and societal risk for members of the public to lower level criteria relating to core damage, a large release or a large early release of radioactivity to the environment, and radiation doses to an individual living near the plant.

The high level qualitative criteria state that the additional health effects to the public from operation of the nuclear power plant should not lead to a significant increase in the risk of death of members of the public. The high level quantitative goals state that the level of increase should be less than about 0.1% of the existing risks.

In some countries the risk criteria are defined for individual members of the public and for societal risks involving 10 or 100 members of the public. The societal risks are sometimes defined as acute fatalities that occur in a short time after the accident or in the longer term.

The most common metrics used are core damage frequency (CDF) and large release frequency (LRF) or large early release frequency (LERF). In some cases these criteria have been defined as surrogates for higher level metrics and some cases they have been defined in their own right.

2.4 Examples of national approaches

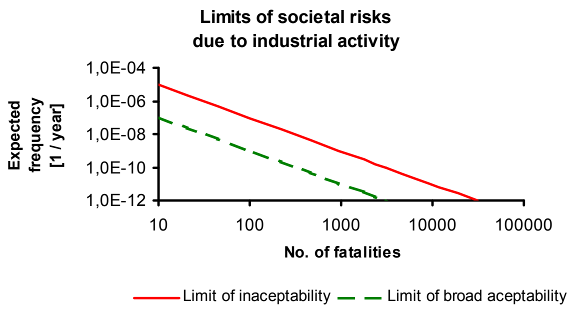
2.4.1 Quantitative safety criteria on level 3

The Netherlands

In the Netherlands risk based criteria were formulated to judge the safety and environmental effects of industrial plants with great hazard potential, nuclear power plants obviously belonging to these. One of these criteria refers to the individual risk, the other one limits the collective risk ('societal risk').

The maximally permissible individual risk, which means the risk of premature death as a result of the plant operation, is 10^{-6} / a. The individual risk is to be calculated according to a rather restrictive rule which postulates that a child one year old at the time of the accident will spend further seventy years at the location of the accident (Eendebak 1995).

According to Figure 4, societal risk is limited in such a way that the probability for ten fatalities is less than 10^{-5} per operating year, for a hundred fatalities less than 10^{-7} per year and so forth. Societal risk refers only to early radiation-induced fatalities, often designated as deterministic radiation-induced damages. In the calculations, accident mitigation measures are not taken into account.



In between: efforts to reduce risk required

Figure 4. Limit of societal risk for any industrial plant in the Netherlands (Directorade 1989).

Although in the Netherlands nuclear power is of minor importance, there being a single NPP in operation providing less than 5 % of the electric power production, PSA is used to a considerable extent including PSA of level 3.

For new plants - NPPs or other nuclear installations - a PSA of level 3 is required in the licensing procedure. There is an official detailed guideline for performing PSAs, also describing the stipulation of specific atmospheric dispersion models and/or programs to be used. (JCSS 2008) gives an overview of the utilization of probabilistic acceptance criteria and the structure of the relevant code of standards, focussing mainly on the chemical industry.

For periodic safety reviews of NPPs, secondary safety criteria for evaluation of PSA results were derived from the above-mentioned societal risk limits. This means that for CDF a probability of < 10^{-4} per year is to be proved, the frequency of large early releases must not exceed 10^{-6} per year.

(Eendebak 1995) states that the PSAs carried out both for Borssele NPP and Doodeward NPP (meanwhile shutdown) show that the associated societal risks are small compared to those of other technical activities and that the Dutch acceptance criteria are unambiguously fulfilled. (Van der Borst & Versteeg 1996) shows this for Borssele NPP and points out the risk reduction effect of retrofitting measures that were initiated based on PSA insights (see Figure 5).

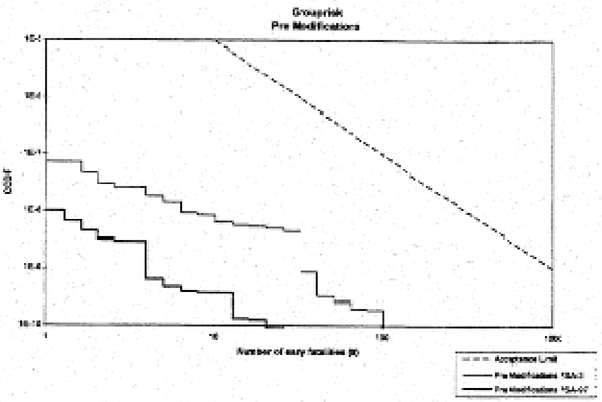


Figure 5. Societal risk of Borssele NPP, before and after AM measures and modifications.

Dutch regulations treat risks from nuclear installations in the same manner as those from non-nuclear installations, e. g. from chemical plants. Thus, an objective evaluation of diverse technical risks is achieved.

In (Vrijling et al. 1996, 2004) a possible extension of the Dutch concept of individual and societal risk is discussed. Application to airports, road traffic and to the transport of dangerous goods frequently shows surprisingly high risk figures compared with nuclear activities.

United Kingdom

The U.K Health and Safety Executive as the British regulatory authority, issued the paper "Tolerability of Risk from Nuclear Power Stations" (HSE 1988) as 'draft for comment'. The proposals contained in this paper became compulsory and were published as "Safety Assessment Principles for Nuclear Power Plants" in 1992. These safety assessment principles have been currently updated (see HSE 2006 a, b).

It must be emphasized that the Nuclear Installation Inspectorate (NII) in its 'Safety Assessment Principles' has a number of different quantitative safety goals. Like in the approach of the IAEA (cf. Fig. 6), there is between the 'broadly acceptable' region (below the Basic Safety Objective, BSO) and the 'unacceptable' region (above the Basic Safety Limit, BSL) an intermediate field in which risk optimization is to be carried out. It should be pointed out that in principle this criterion does not only apply to NPPs, but also to other nuclear installations.

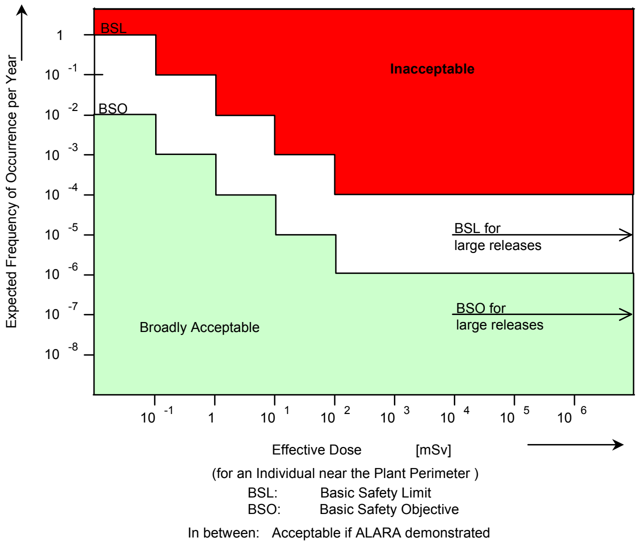


Figure 6. Limits to radiological effects vs. their expected frequencies of occurrence (acc. to HSE 1992). Doses are calculated for a person living approx. 1 km downwind from the plant.

2.4.2 Quantitative safety criteria on level 2

The Argentine code of regulations basically does not distinguish between NPPs on the one hand and ‘other nuclear installations’ on the other; rather does it only distinguish between relevant and non-relevant installations based on their associated radiological hazard (Berg et al. 2003). To the first category belong, besides NPPs, also larger test reactors and plants of the fuel cycle, e. g. fuel factories. There exist two criteria: one applicable to the general population near the plant and a second one applicable to the work force (cf. Fig. 7).

The criterion which links the effective dose with the expected frequency of occurrence of the event causing the exposure to a person of the general public outside of the plant boundary (Fig. 7) is defined so that no conceivable accident sequence will give rise to a risk greater than 10^{-7} per year. Together with the further criterion which limits the total plant hazard - the sum over all conceivable accident sequences - to 10^{-6} per year, this provides - at least implicitly - a quantitative criterion indicating whether the plant safety concept is well-balanced.

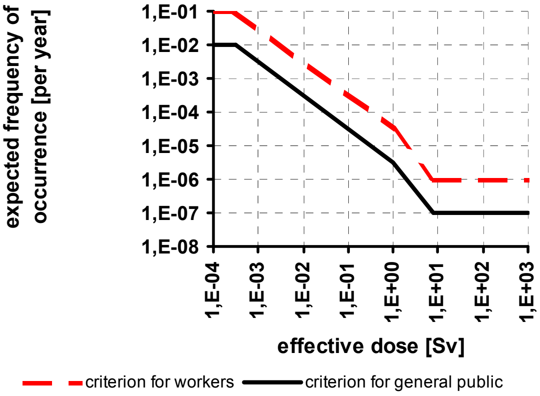


Figure 7. Boundary curves for the work force and for the general public in Argentina. Values to the right and above the curves are not acceptable.

Interpretation of the boundary curve in Figure 7: for effective doses less than 1 Sv, which are expected to yield only stochastic effects, a dose risk rate of 10^{-2} / Sv was used to build the curve. Effective doses larger than 1 Sv will yield non-stochastic effects and higher dose risk rates leading to an increased slope of the curves. Ultimately, effective doses larger than some 7 to 8 Sv (which correspond to the lethal dose in 30 days) may not occur with a probability larger than 10^{-7} per year for the general public (or 10^{-6} per year for workers).

In spite of the definition of the criteria in the form of a dose/frequency curve these are really criteria of level 2 since in the immediate vicinity of the plant the effective dose for the general public (or inside the plant for employees) is simply linearly dependent on the amount of released activity. Far field diffusion and accumulation effects do not play a significant role here, in contrast to criteria regulating collective doses in large areas.

2.4.3 Quantitative safety criteria on level 1

Quantitative safety criteria that are defined on level 1 – e. g. in the format of maximal allowed CDF values – are found less frequently in statutory or regulatory provisions. Some countries, despite having and applying quantitative safety criteria defined on a higher level, also have an explicit statutory or regulatory limitation for CDF.

As a typical example, Finland may be taken: besides limiting the expected frequency of occurrence for large off-site releases, the guideline (STUK 1996) sets a limit which restricts CDF for new plant to less than 10^{-5} per year (the value is designated a design objective).

Furthermore, countries actively promoting the expansion of their nuclear power plant park and the development of advanced NPP designs are known to apply design objectives for CDF like e. g. Canada does with the advanced heavy water moderated reactor type CANDU 9 (IAEA 2002).

In the safety review and for the evaluation of the necessity of back fits for the Ignalina NPP in Lithuania, quantitative probabilistic acceptance criteria were used in one application and more qualitative, quasi-probabilistic criteria in another one.

Given an initiating event (under the assumption that no safety device cuts in to control the event), that scheme combines in a single matrix the scale of possible accident consequences and the number and quality of available safety systems that are available for the control of the considered event sequence according to plant design. In this evaluation, safety systems (with conservative design, nuclear class quality, operational monitoring, single failure tolerance) and other, non safety-grade systems (with lower reliability, e. g. balance-of-plant systems) are distinguished; (Holloway & Butcher 1995) use the terms 'strong' and. 'weak lines of defense' respectively for these.

The former are attributed a failure probability of better than 10^{-2} per challenge, the latter one of between 10^{-2} and 10^{-1} per challenge.

With these roughly estimated values and the accident consequences sorted into four categories according to expected severity, an evaluation diagram is derived that points out broadly acceptable areas, those with long term tolerable safety weaknesses, those with only temporarily tolerable shortcomings safety-wise and, lastly, those areas with safety deficits which are not acceptable, even for limited time periods (Fig. 8).

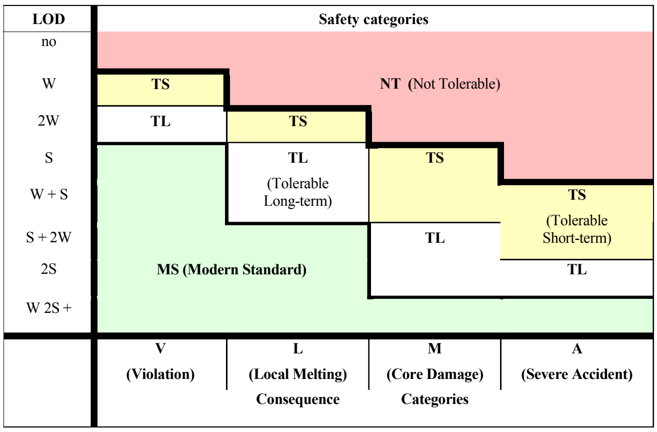


Figure 8. Scheme of the quasi-probabilistic LOD procedure for the evaluation of safety upgrade requirements for NPP Ignalina (acc. to Rimkevicius et al. 2002)
W: weak line of defense; S: strong line of defense

2.5 Discussion and evaluation

The variability of the examples presented in 2.4.1 to 2.4.3 demonstrates how many possibilities exist for the formulation of probabilistic safety criteria. Nevertheless the safety level described by these criteria - expressed either as core damage or large release frequencies - is largely comparable. The yardstick to compare the criteria are accidents leading to large releases. For their investigation, a PSA of at least level 2 is necessary, in the case of the Netherlands and the United Kingdom a PSA of level 3 is required to calculate the accident-caused individual or collective doses. The different criteria can be reformulated directly or implicitly into requirements on the expected frequency of large releases.

As conclusions three fundamental dose limits ca be defined, for additive annual doses from normal operation, for non-fatal health detriments (from a single brief exposure, i. e. accident-caused) and for acute fatalities due to large accident releases, determined the corresponding acceptable expected frequencies and thus derived a near-linear complementary cumulative distribution function (CCDF) for a Basic Safety Goal. This CCDF he compared with the BSO- and BSL-curves of the British HSE, the 'Safety Goal' of the USNRC, a safety design criterion for PWR of the ANS, and an ICRP-recommendation (which refers to radioactive waste repositories rather than to NPPs). Figure 9 shows a quite reasonable agreement between these rather differently formulated quantitative criteria (Hakata 2003).

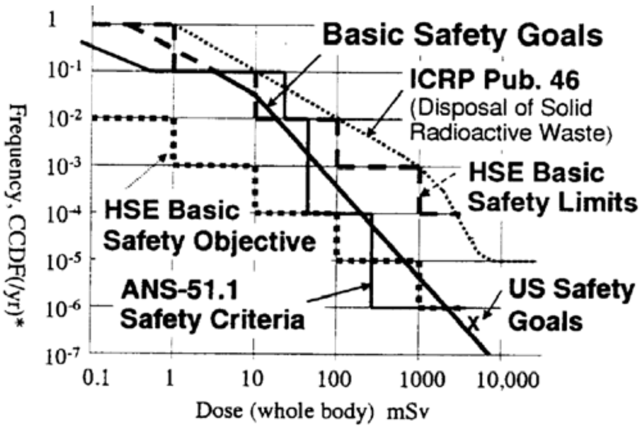


Figure 9. Comparison of different Safety Goals

HSE criteria are CCDF in each decade of doses; ANS and ICRP criteria are frequencies [per year]

3 RISK CRITERIA FOR OTHER INDUSTRIES

In the frame of the EU-project "Safety and Reliability of Industrial Products, Systems and Structures" (SAFERELNET), risk criteria used in the EU for population living in vicinity of hazardous facilities have been investigated. It can be seen from Table 1 that individual risk of 10^{-5} per year represents the upper limit in Europe for existing installations, while in the UK the intolerable limit is 10^{-4} but ALARP is strictly imposed, meaning that in reality the risk is well below the limit. The upper limit for individual risk for new installations in Czech Republic and in the Netherlands after 2010 is 10^{-6} per year. The quoted value for the Netherlands (10^{-5} and 10^{-6}) represent so-called location risk (risk contour), or the individual risk to a person who is permanently at the particular location. In addition, in the case of the Netherlands, the risk value corresponds to one establishment (facility), and the cumulative risks from several establishments are not taken into account.

The negligible risk levels specified in the UK as 10^{-7} per year and in the Netherlands as 10^{-8} per year are not questionable and it will be assumed that 10^{-8} can be a value accepted across the EU for the time being.

Table 1. Comparison of individual risk criteria

IRPA	UK	The Netherlands	Hungary	Czech Republic
10^{-4}	Intolerable limit for members of the public			
10^{-5}	Risk has to be reduced to the level As Low As Reasonably Practicable (ALARP)	Limit for existing installations. ALARA principle applies	Upper limit	Limit for existing installations. Risk reduction must be carried out
3 x 10^{-6}	LUP limit of acceptability (converted from risk of dangerous dose of 3 x 10^{-7})			
10^{-6}	Broadly acceptable level of risk	Limit for the new installations and general limit after 2010. ALARA applies	Lower limit	Limit for the new installations
10^{-7}	Negligible level of risk			
10^{-8}		Negligible level of risk		

In the Norwegian offshore petroleum industry, risk analysis are used for more than decades. These analysis have been closely linked to the use of risk acceptance criteria (see Aven &Vinnem 2005, Aven et al. 2006, Hokstad et al. 2004) as upper limits of acceptable risks.

In order to fulfil the requirements and acceptance criteria for major accidents the NORSOK Z-013 standard is usually applied.

In (Maharik & Vrijling 2002) is explained "If average fatality risk or average individual risk is used in the formulation of risk acceptance criteria, also criteria for areas or groups within the platform personnel shall be formulated. It is not sufficient just to have a platform average value as criterion. The risk estimates shall be considered on a "best estimate" basis, when considered in relation to the risk acceptance criteria, rather than on an optimistic or pessimistic (worst case) basis. The approach towards the best estimate shall, however, be from the conservative side, in particular when the data basis is scarce."

The standard (NORSOK 2001) does not prescribe explicit criteria; however, annex A provides some examples of typical risk acceptance criteria to be used, such as

– The fatality accident rate should be less than 10 for all personnel on the installation, where the fatality accident rate value is defined as the expected number of fatalities per 100 million exposed hours.

– The individual probability that a person is killed in an accident during one year should not exceed 0,1%.

In the railway sector, the European Railway Agency has got in December 2005 the mandate from the European Commission (2005) to develop a first set of common safety targets (CST):

"The CSTs shall define the safety levels that must at least be reached by different parts of the railway system and by the system as a whole in each Member State, expressed in risk acceptance criteria…"

Recommendations of this first set of CST will be available in September 2008 at the earliest.

For the signal technique for railways, safety standards are elaborated as EN 50129 (CENELEC 2003). A complete analysis of the possible hazards is not performed; instead only the hazard H="failure of level crossing to protect public from train" is considered. It is interpreted as covering all situations in which the level crossing should warn the public (of approaching trains), but fails to do so. The objective is now to determine the hazard rate HR [1/time] for H which is acceptable according to certain risk acceptance criteria.

The tolerable hazard rate of 10^{-9} per hour is in the railway area proposed as a target for all safety-critical functions (see Braband 2005). This approach is similar to that in civil aviation. It has been shown from operational experience with large aircraft fleets that the overall level has actually been met in practice. Tolerable hazard rates are correlated here to safety integrity levels (SIL) as shown in Table 2.

Table 2. Definition of safety integrity levels (SILs)

Tolerable Hazard Rate THR per hour and per functions	**Safety Integrity Level**
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

SIL is defined as the reliability to perform the required safety functions under all stated conditions within a stated operational environment and within a stated period of time.

According to the British Rail Safety and Standards Board, railway companies are required to make safety decisions to reduce risk to a level that is as is as low as is reasonably practicable (Dennis 2006). That is their legal duty. What is reasonably practicable must reflect their social duty to delver a railway that society demands and pays for through public subsidy and their commercial duty to shareholders and customers. The ALARP approach is, e.g., applied for risks of train passengers and workers (see Fig. 10).

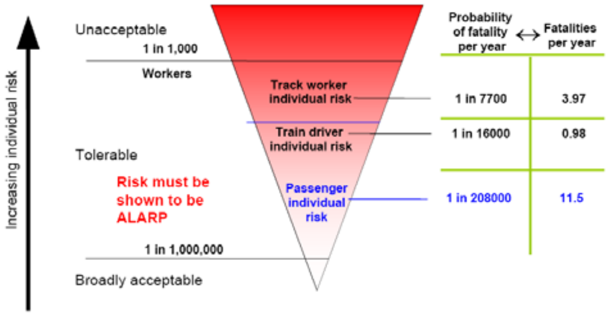

Increasing individual risk
Unacceptable
1 in 1,000
Workers
Tolerable
Risk must be shown to be ALARP
1 in 1,000,000
Broadly acceptable
Track worker individual risk
Train driver individual risk
Passenger individual risk
Probability of fatality per year
↔
Fatalities per year
1 in 7700
3.97
1 in 16000
0.98
1 in 208000
11.5

Figure 10. ALARP for risks of workers and train passengers.

In the maritime sector, international organisations have traditionally been capturing experience and knowledge into prescriptive legislation, thereby endeavouring to prevent past accidents from reoccurring. The current level of safety seems tolerable to the sector, however, the set of rules and regulations is extensive and it is not verified whether individual requirements are in balance with each other.

Thus, the Maritime Safety Committee - senior technical body on safety-related matters of the International Maritime Organisation (IMO) - agreed to further develop goal-based standards using a safety level approach; the task has a five-tier structure: goals (Tier I), functional requirements (Tier II), verification of compliance criteria (Tier III), technical procedures and guidelines, classification rules and industry standards (Tier IV) and codes of practice and safety and quality systems for shipbuilding, ship operation, maintenance, training, manning, etc. (Tier V).

Some reasons for the application of goal-based standards in shipping are seen by the Maritime Safety Committee:

– to assure a uniform minimum acceptable safety level across the merchant fleet;

– to facilitate the comparison between alternative risk control options,

– to facilitate the comparison of accident rates and risk acceptance criteria within the fleet and to other sectors such as aviation or offshore,

– to improve the transparency of the system by the incorporation of rationales; and

– to balance individual requirements with each other.

These goal based standards may use risk criteria as the ‘top’ goal which forms the ultimate goal to be achieved by subsequent IMO rules such as regulations for fire safety, navigation, life saving appliances as well as class society rules and regulations for structures, machinery etc.

4 UNCERTAINTIES IN RISK ASSESSMENT RESULTS

As large-scale accidents occur infrequently and are typically the result of some unique combination of human and system failure, there is inevitably a degree of imprecision or ambiguity associated with the predicted probability of occurrence of such accidents and uncertainty concerning the consequences, should such an accident happen. Procedures for tackling uncertainties when assessing risks are described in (HSE 2001).

These uncertainties 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 shall be reflected when quantitative safety goals are used to judge the results of a probabilistic safety assessment. The requirement may be satisfied in different ways:

– apply more conservation in the risk analysis.

– make sure that probabilistic safety assessment are satisfied with some margin.

Another way to capture uncertainties about a particular risk resulting from a plant, activity or item is to construct an exceedance probability (EP) curve. An EP curve specifies the probabilities that a certain level of losses will be exceeded. The losses can be measured in terms of technical damages, fatalities, financial consequences or some other relevant unit of the respective analysis.

By its nature, the EP curve inherently incorporates uncertainty associated with the probability of an event occurring and the magnitude of losses. This uncertainty is reflected in the 5 % and 95 % confidence interval curves in the EP curve. When determining quantitative safety goals, e.g., the competent regulatory body or institution has to provide guidance how to compare results from probabilistic safety assessments with these goals and how to deal with the uncertainties in the assessment taking into account that the degree of uncertainty in risk analysis increases at lower probabilities, which adds another dimension to the evaluation of potentially disastrous hazards and resulting consequences.

5 CONCLUDING REMARKS

Risk management and safety management, based on the results of risk analysis, support the process of decision making both for the industries and the respective regulatory bodies.

Whenever, on the basis of risk assessments, decision alternatives have been identified and ranked by comparing the expected value of benefits or losses, the risks must be considered in regard to their acceptability. It is suggested to differentiate between tangible and intangible risk, i.e. risks which may be easily expressed in monetary risks and others. Which intangible values should be considered in a given case has to be checked by the risk identification.

Therefore, the need for the development of risk criteria, which would support risk informed decision-making, is expressed worldwide. However, risk acceptance is also correlated to the cultural context, even if, e.g., the European Commission is acting in determining or harmonizing quantitative safety goals.

One way of determining quantitative risk criteria is to consider probabilistic safety assessment. Ideally, such quantitative safety goals are not limited to one type of plants but to any large industrial plant or any industrial activity that requires safety-related systems to ensure safety of aviation, aeronautical (Filip 2007), or railway.

REFERENCES

[1] Aven, T. & Vinnem, J.E. 2005. On the use of risk acceptance criteria in the offshore oil and gas industry. *Reliability Engineering and System Safety* 90: 15 – 24.

[2] Aven, T., Vinnem, J.E. & Røed, W. 2006. On the use of goals, quantitative criteria and requirements in safety management. Risk Management: an International Journal 8: 118 – 132.

[3] Berg, H. P. 1995. On the potential of probabilistic safety assessment. Kerntechnik 60: 71

[4] Berg, H. P., Görtz, R. & Schimetschka, E. 2003. Quantitative Probabilistic Safety Criteria for Licensing and Operation of Nuclear Plants, Comparison of the International Status and Development. BfS-Report, BfS-SK-03/03, Bundesamt für Strahlenschutz, Salzgitter, November 2003.

[5] Van der Borst & M. Versteeg, M. F. 1996. PSA supported severe accident management strategies for the Borssele NPP. Proc. International Topical Meeting on Probabilistic Safety Assessment PSA`96. Vol. 3. Park City, Utah, USA, September 29th – October 3rd, 1996

[6] Braband, J. 2005. Risikoanalysen in der Eisenbahn-Automatisierung. Eurailpress, Hamburg 2005.

[7] CENELEC. (2003). Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling. EN 50129, February 2003.

[8] Cepin, M. 2004. Development of criteria for risk – informed decision – making. Proceedings International Conference Nuclear Energy for New Europe 2004, Nuclear Society of Slovenia, paper 501.

[9] Cepin, M. 2007. The risk criteria for assessment of temporary changes in a nuclear power plant. Risk Analysis 27, No 4: 991 – 998.

[10] Dennis, C. 2006. The use of risk assessment to inform safety decision making. Safety Risk Management as an Input to Business Strategy, Institute of Risk Management, 5th October 2006.

[11] Directorate General for Environmental Protection at the Ministry of Housing, Physical Planning and Environment 1989. Premises for Risk Management – Risk Limits in the Content of Environmental Policy.

[12] Eendebak, B. 1995. The use of probabilistic safety assessment for operating nuclear power plants. Fourth annual Two-Day Conference on PSA on the Nuclear Industry, London, November 29th – 30th, 1995.

[13] European Commission. Mandate to the European Railway Agency. December 16th, 2005.

[14] Filip, Ales 2007. Safety aspects of GNSS based train position determination for railway signalling. UIC GALILEO for Rail Symposium, Paris, October 18th – 19th, 2007.

[15] Görtz, R., Berg, H.P. & Schimetschka, E. 2001. Risk targets and reliability goals. Probabilistic Safety Assessment and Risk-informed Decision Making PSARID EUROCOURSE, Garching, March 2001.

[16] Hakata, T. 2003. Basic considerations on defining safety goals. Nuclear Technology 142: 243 – 249.

[17] Hokstad, P., Vatn, J., Aven, T. & Sorum, M. 2004. Use of risk acceptance criteria in Norwegian offshore industry: dilemmas and challenges. Risk, Decision and Policy, 9: 193 – 206.

[18] Holloway, N. & J. Butcher, P. 1995. Ignalina RSR Task 10: a defense in depth approach to safety assessment for RMBK reactors. Serco Assurance Ltd., UK, December 1995, private communication by S. Simkevicius sigis@isag.lei.It.

[19] Health & Safety Executive (HSE) 1988. The Tolerability of Risk from Nuclear Power Stations. HMSO, London 1988.

[20] Health & Safety Executive (HSE) 1992. Safety Assessment Principles for Nuclear Plants. HMSO, London, 1992.

[21] Health & Safety Executive (HSE) 2001. Reducing Risks, Protecting People. HMSO, Colegate, Norwich.

[22] Health & Safety Executive (HSE) 2006 a. Safety Assessment Principles for Nuclear Facilities. Edition 2006, HSE, Redgrave Court.

[23] Health & Safety Executive (HSE) 2006 b. Numerical Targets and Legal Limits in Safety Assessment Principles for Nuclear Facilities, An Explanatory Note. HSE, Redgrave Court, December 2006.

[24] International Atomic Energy Agency (IAEA) 1992. The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety. IAEA Safety Series No. 106, Vienna.

[25] International Atomic Energy Agency (IAEA) 2001. Safety Assessment and Verification for Nuclear Power Plants. Safety Guide No. NS-G-1.2, Vienna.

[26] International Atomic Energy Agency (IAEA) 2002. Heavy Water Reactors: Status and Projected Development. IAEA Technical Report Series No. 407, Vienna.

[27] International Atomic Energy Agency (IAEA) 2007. Risk-Informed Decision-Making. Draft B, Safety Guide, Vienna.

[28] International Nuclear Safety Advisory Group (INSAG) 1999. Basic Safety Principles for Nuclear Power Plants. 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna.

[29] Joint Committee of Structural Safety (JCSS) 2008. Risk Assessment in Engineering, Principles, System Representation & Risk Criteria. JCSS, June 2008.

[30] Kumamoto, H. 2007. Satisfying Safety Goals by Probabilistic Risk Assessment. Springer Series in Reliability Engineering, Springer-Verlag.

[31] Maharik, H. & Vrijling, J. K. 2002. Lessons from quantitative risk assessment in the Netherlands: national and international perspective. 6th International Conference on Probabilistic Safety Assessment and Management, San Juan, Puerto Rico, USA, June 23rd – 28th, 2002.

[32] NORSOK 2001. Risk and Emergency Preparedness Analysis. Standard Z-013.

[33] Nuclear Energy Agency/OECD 2007 b. Use and Development of Probabilistic Safety Assessment. NEA/CSNI/R (2007) 12, November 2007.

[34] Nuclear Energy Agency/OECD 2007 a. The Regulatory Goal of Assuring Nuclear Safety. Paris.

[35] Rimkevicius, S., Senkin, V. & Brandisauskas, D. 2002. Presentation at IAEA Technical Meeting on Analysis Results and Methods for PSRs of NPPs, Ljubljana, Slovenia, December 2nd – 6th, 2002.

[36] Radiation and Nuclear Safety Authority (STUK) 1996. Probabilistic Safety Analysis (PSA). Guide No. YVL 2.8, issued December 20th, 1996, updated version May 2003.

[37] Villadóniga, J. 2001. Towards the risk-informed approach. Probabilistic safety assessment and risk-informed decision making. PSARID EUROCOURSE, Garching, March 2001.

[38] Vrijling, J. K., van Hengel, W. & van Maanen, S. E. 1996. The application of the concept of societal risk to various activities in the Netherlands. Proceedings of the International Conference Probabilistic Safety Assessment and Management, ESREL 1996 – PSAM III, Springer-Verlag, Volume 2.

[39] Vrijling, J.K. et al. 2004. A framework for risk criteria for critical infrastructures : fundamentals and case studies in the Netherlands, Journal of Risk Research 7 (6): 569 – 579.