THE VALIDITY OF SAFETY GOALS

Michael Knochenhauer
RELCON AB

Jan-Erik Holmberg
VTT (Technical Research Centre of Finland)

Göran Hultqvist
NPP Forsmark

Ingemar Ingemarson
NPP Ringhals

SUMMARY/ABSTRACT

The paper describes a research project titled “The Validity of Safety Goals” recently initiated by NKS (Nordic Nuclear Safety Research) and NPSAG (Nordic PSA Group) with participants from Finland and Sweden.

Quantitative results from a probabilistic safety assessment (PSA) for a nuclear power plant are typically presented as core damage frequency (CDF) and frequency of radioactive release. In order to judge on the acceptability of results, criteria for the interpretation of results and for the assessment of their acceptability need to be defined.

The risk levels specified by the safety goals differ between organizations and between different countries. There may also be differences in the definition of safety goals. In most countries, safety goals started to be defined in the 1980s, i.e. at a time when PSA models were rather limited in scope. During the 1990s, the PSA models expanded considerably, both regarding operating states and classes of initiating events. In parallel, PSA:s have been expanded to level 2, making it possible to calculate release frequencies. In view of this development, and of current needs, the objective of the project includes looking back and mapping the evolvement of safety goals for PSA.

Defining quantitative goals for reactor safety may have a large impact on both the analysis burden and on requirements for safety improvements at nuclear power plants. It is therefore of great importance that these goals are effective and soundly based, that they can be effectively and unambiguously applied, and that they can be accepted and understood by all parties concerned (analysts, decision makers, the public, etc.). In connection with this, a number of specific issues related to the definition and use of safety goals will also be discussed. Issues, which may become involved in the project, include:

- Reasons for developing safety goals.
- Identification of conditions where safety goals can (and should) be applied.
- Definition of subject of safety goal, i.e., what exactly is meant by “core damage”, “large release”, etc.
- The background to the safety goals developed nationally (Sweden/Finland) and internationally.
- The organizations involved in defining the goals, and the process involved in the formulation of the goals.
- The basis for defining the actual numerical levels used in the safety goals (population risks, etc.)
- Relation of safety goals used for nuclear power plants to safety goals used for other man-made risks.
- The relationship between safety goals defined for level 1 PSA (CDF) and for level 2 PSA (release frequencies)
- Use of the safety goals on results from PSA:s with differing scopes
- Effects on the use of safety goals arising from major PSA uncertainties, including uncertainties related to completeness and the state of knowledge.

The project work was initiated in late 2005, and will be performed mainly during 2006. The paper describes in some detail the background to the initiation of the project, its contents and aims, and also gives some initial comments on the issues related to the use and interpretation of safety goals and on the applicability of safety goals for decision making.

INTRODUCTION

The paper describes a research project titled “The Validity of Safety Goals” recently initiated by NKS (Nordic Nuclear Safety Research) and NPSAG (Nordic PSA Group).

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 Core Damage Frequency (CDF) and frequency of radioactive release, e.g., as Large Early Release Frequency (LERF). In order to judge on the acceptability of results, various criteria for interpretation of results and assessment of their acceptability need to be defined.

Target values for PSA results, both for CDF and for radioactive releases, are in use in most countries having nuclear power plants. In some countries, the safety authorities define the safety goal. In other countries, including Sweden, the goals have been set by the nuclear utilities. In Finland, safety goal are defined by STUK for new plants, and are presently applied for the Olkiluoto 3 plant. The values are also used as a reference value for existing plants. In the U.S.A. the NRC has issued Regulatory Guides [1] defining target values for cases where a utility wants to use PSA results as a basis for deviating from deterministic requirements. The IAEA has issued a number of publications dealing with PSA and judgment of PSA results [2 to 6]. The European Utility Requirements (EUR) document also includes a discussion of probabilistic safety targets [7].

The exact levels of the safety goals differ between organizations and between different countries. There may also be differences in the definition of the safety goal. Ultimately, these safety goals are intended to define acceptable levels of risk from operation of commercial nuclear power plants. The level of 10^{-5} per year seems to have become a consensus target value for CDF, at least in the Nordic countries. For the release frequency, the variety is considerable, both regarding the frequency and the exact definition of what constitutes a “large release”.

Defining quantitative goals for reactor safety may have a large impact on both the analysis burden and on requirements for safety improvements at nuclear power plants. Safety goals can also be used as a basis for relaxation of safety requirements. However, relaxation of deterministic safety requirements based on probabilistic arguments may be a controversial issue.

It is therefore of great importance that these goals are effective and soundly based, that they can be effectively and unambiguously applied, and that they can be accepted and understood by all parties concerned (analysts, decision makers, etc.).

BACKGROUND TO EXISTING SAFETY GOALS

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

During the 1990s, the PSA models expanded considerably, both regarding operating states (inclusion of start-up, shut-down, and outage states) and classes of initiating events (inclusion of area events and external events). The level of detail of the analyses has also increased, especially regarding sub-division of initiating events (definition of common cause initiator events, CCI), inclusion of functional dependencies (signals, power supply, control logics), and modeling of non-safety classified systems. In parallel, PSA:s have been expanded to level 2, making it possible to calculate release frequencies.

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

SCOPE AND AIM OF THE PROJECT

In view of the development described above, and of current needs, the objective of the project is primarily to look back and map the evolvement of these safety goals for PSA. Where do they come from? What do they stand for? What are the experiences using safety targets? What are the needs? Specifically, it will be tried to describe in some detail the reason for developing safety goals and the background to the safety goals developed nationally

(Sweden/Finland) and internationally, as well as describing the organizations involved in defining the goals, and the process involved in the formulation of the goals.

Thus, the project will include a review and description of the current status with regard to definition and application of safety goals. In addition, representatives of the various parties involved (utilities, authorities, etc.) will be interviewed in order to improve the understanding of the role of safety goals and of the expectations on the goals defined. The concept of safety goals, as used in the nuclear industry, will be put in perspective by comparing to goals and application practices in other industries. Based on the information gathered, it will be attempted to provide a basis for improved understanding of a number of crucial problems related to safety goals. The project does not aim at proposing new quantitative safety goals but rather gather information and experiences about the existing ones and to analyze this information.

DESCRIPTION OF CURRENT STATUS

The description of current status will look at existing safety goals in various countries and on current practice regarding application of safety goals internationally. A series of interviews will be held involving a number of key persons at Nordic utilities and authorities, and aim at discussing and documenting current views on the use of safety goals, including both benefits, problems and interpretation. Organizations outside the Nordic countries may also be involved in this phase. The interviews will also include historical issues regarding the definition and application of the safety goals. These activities are in the initial stages, but some comments can be given.

Overview of existing safety goals

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

- No numerical safety goal stated by the regulatory body, but numerical evaluations can be used in regulatory decision making (e.g. Belgium, Canada, Germany, France, Sweden (for core damage frequency)).
- Numerical safety goal defined for nuclear power plants in terms of core damage frequency or large early release frequency (Finland, Switzerland, Sweden (for maximum allowed releases)).
- Numerical safety goal defined for hazardous industry in terms of human mortality risk, safety goal for NPP:s derived from the overall safety goal (the Netherlands, UK, USA).

Table 1 summarizes examples of numerical safety goals applied in different countries.

In addition to the national safety goals, international and national organizations have defined safety goals. The International Atomic Energy Agency (IAEA) defined safety goals already in the 1980s [16]. The report was updated in 1999 [17]. The INSAG-12 target for *existing* nuclear power plants consistent with the technical safety objective is a frequency of occurrence of severe core damage that is below about 10^{-4} events per plant operating year. Severe accident management and mitigation measures could reduce by a factor of at least ten the probability of large off-site releases requiring short term off-site response. Application of all safety principles and the objectives to *future* plants could lead to the achievement of an improved goal of not more than 10^{-5} severe core damage events per plant operating year. Another objective for these future plants is the practical elimination of accident sequences that could lead to large early radioactive releases, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and in time.

European Utility Requirements for LWR nuclear power plants (EUR) defines the following probabilistic design targets [7]:

- a core damage cumulative frequency of less than 10^{-5} per year
- a cumulative frequency of less than 10^{-6} per year of exceeding the criteria for limiting impact (an acceptance criterion, given by a comparison of a linear combination of families of isotope releases, versus a maximum value)
- a significantly lower cumulative frequency to get either earlier or much larger releases.

EUR frequency targets include shutdown states which have been shown to be a significant contributor in assessments of present reactor designs.

Table 1. Safety goals in Finland, the Netherlands, Switzerland, UK and USA [8].

Country	Safety Goal
Finland [11]	The mean value of the frequency of core damage is less than 10^{-5} per year. The mean value of the frequency of a release exceeding the target value defined in section 12 of the Council of State Decision (359/91) must be smaller than $5 \cdot 10^{-7}$ per year. However the containment has to be designed in such a way that its integrity is maintained with a high likelihood in case of both low and high pressure core damage.
Netherlands [8]	For the prevention of major accidents, the maximum permissible level for the individual mortality risk (i.e. acute and/or late death) has been set at 10^{-5} per year for all sources together and 10^{-6} per year for a single source. In order to avoid large-scale disruptions to society, the frequency of an accident in which at least 10 people suffer acute death is restricted to a level of 10^{-5} per year. If the number of fatalities increases by a factor of n, the probability should decrease by a factor of n^2. Acute death means death within a few weeks; long-term effects are not included in the group risk.
Switzerland [12]	For the construction permit for a new nuclear power plant, it must be demonstrated that the core damage frequency is below 10^{-5} per year. This risk criterion is also expected to be fulfilled by the existing plants, to the extent that is reasonably achievable.
UK [13,14]	10^{-4} per year as the limit of tolerability for the risk of death for a worker on a nuclear plant. 10^{-5} per year as the benchmark for the risk of death for a member of the public from a new nuclear power plant. 10^{-6} per year for the broadly acceptable level of risk of death for a member of the public.
USA [15]	The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed 0.1 percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed. The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed 0.1 percent of the sum of cancer fatality risks resulting from all other causes.

DEFINITION AND APPLICATION OF SAFETY GOALS

Defining Safety Goals

There are different reasons for defining safety goals, and the reasons may differ between different types of organizations (utilities, authorities, etc.). Thus, one aim may be to provide a tool to control the risk posed to society by the operation of nuclear power plants by defining a maximum acceptable risk. This risk may be related to the population potentially exposed to the risk, which is the most common case, but may also be related to some other entities, e.g., land contamination. This third party protection aim is always valid to some extent, even if it is not explicitly stated. When relating calculated risks to such a safety goal it can be used in an absolute manner giving the answer *Yes* or *No* to the question of whether the risk is acceptable or not.

However, a relative approach is often also used, where the safety goal constitutes a reference level and the key issue in the analysis of the calculated risk for a plant is the relative deviation from the absolute level, or the degree of change relative to the corresponding results for other plant configurations or designs. In this case the focus is more on using the safety goal as part of a decision criterion.

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

The definition of the risk measure can be a more complex activity, as it should be possible to relate the risk measure to the degree of harm experienced by the population exposed to the risk. As an example, there is no simple connection of this kind between the core damage frequency for a nuclear power plant and the degree of risk experienced by the public. For level 2 PSA criteria (large radioactive release), the connection is more evident, but not necessarily straight-forward and easily interpreted. In contrast, safety goals for other man-made risks are often expressed in terms of frequency and number of fatalities (FN curves), which usually provides safety goals which are easier both to interpret and to apply.

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

Application and Utilization of safety goals

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

Thus, there is a need for defining how to decide that a safety goal has been met, i.e., criteria for accepting a calculated risk. Among other things, it needs to be stated whether it is the mean value of the calculated risk measure that shall meet the goal or if the comparison with the safety goal shall be done for some percentile in the uncertainty distribution of the result. In this context, there may also be a need to consider the risk impact from potential risk contributors not modeled in the plant PSA. This may apply to some categories of initiating events or some plant operating states, e.g., external events and plant shut-down, respectively.

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

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

USE OF SAFETY GOALS IN OTHER INDUSTRIES

It will also be of interest to compare the risks that are associated with PSA safety goals with safety goals related to other man-made risks in society. This was already done in WASH-1400 [18] in 1975. The introduction of the Farmer Curve (FN curve) in 1967 [19] includes a comparison with risks from other activities and a discussion of acceptability as a function of frequency of occurrence and degree of damage. Within OECD/NEA a state of the art report has been developed within WG Risk on the use of safety targets.

To provide perspective on the safety goals used in the nuclear industry, safety goals used in other areas of activity will be studies. The approach will be both descriptive and comparative and focus on the ways safety goals are defined, ways of applying the goals, and the actual maximum acceptable risk levels stated. Some possible areas of comparison include:

- Railway signaling equipment; UNISIG standard defining maximum acceptable hazard frequency
- Offshore industry; criteria for maximum frequency of major platform accidents
- Chemical industry; Seveso directive
- National criteria for population risk from man-made risks, e.g., in the Netherlands, Switzerland and Great Britain
- Programmable electronics; definition of safety integrity levels based on the safety significance of the equipment according to the standard IEC 61508

KEY ISSUES RELATED TO SAFETY GOALS

Based on the activities outlined above it is the aim of the project to provide guidance on a number of problematic issues related to defining and applying safety goals and to the interpretation of the outcome of a safety goal application. The problems may both complicate the use of safety goals and reduce the willingness to accept the outcome of their application. A number of specific issues will be discussed. The following are some issues, which are expected to be covered:

- Definition of subject of safety goal, i.e., what exactly is meant by “core damage”, “large release”, etc.

- Definition of target of safety goal, i.e., the probabilistic plant model and calculation procedure used in order to calculate the risk level which is to be compared to the safety goal. This is related to problems encountered when applying safety goals to results from PSA:s with differing scopes.
- The basis for defining the actual numerical levels used in the safety goals (population risks, etc.)
- Parallel use of multiple safety goals. This is related to problems encountered when separate safety goals are defined for level 1 PSA (CDF) and for level 2 PSA (release frequencies)
- Effects on the use of safety goals from major PSA uncertainties, including uncertainties related to completeness and the state of knowledge.
- Relation of safety goals used for nuclear power plants to safety goals used for other man-made safety risks.

CONCLUSIONS

The project described is still in its initial stages, and no final conclusions can be presented. However, the project is expected to clarify the concept of safety goals and their application and interpretation, as well as to provide guidance related to a number of issues affecting the formulation and use of safety goals.

In Sweden and Finland there is more than 20 years of experience of performing PSA, which includes several revisions of the studies, a gradual increase of the scope and level of detail of the studies, as well as steadily increasing generalized application of PSA for decision making. In spite of all safety improvements made based on PSA results, a current view is that the safety goals outlined in the 1980s (10^{-5} per year for CDF) are hard to achieve for operating NPP:s. This experience arouses confusion that should be resolved in order to restore the confidence in the PSA methodology. Questions aroused include what safety goals should be applied to the operating plants, whether the risk level of the plants is too high, whether PSA:s are too conservative, an if safety goals are being applied in an incorrect way?

The situation can be somewhat different for a plant for which risk insights have been utilized already from the design phase. Therefore, it is interesting to see how well the Olkiluoto 3 NPP currently being built in Finland will fulfill the safety goals and what influence the safety goals will have on the final design of the plant.

REFERENCES

[1] An Approach for using probabilistic risk assessment in risk-informed decisions in plant-specific changes to the licensing basis, U.S. Nuclear Regulatory Commission, November 2002,Regulatory Guide 1.174, Revision 1

[2] Probabilistic Safety Assessment - INSAG-6, IAEA, 1992, Safety Series No. 75-INSAG-6, ISBN 92-0-102492-4

[3] The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, IAEA, 1992, Safety Series No. 106, ISBN 92-0-101492-9

[4] The Safety of Nuclear Power Plants – INSAG-5, IAEA, 1992, Safety Series No. 75-INSAG-5, ISBN 92-0-100192-4

[5] A Common Basis for Judging the Safety of Nuclear Power Plants Built to Earlier Standards – INSAG-8, IAEA, 1995, INSAG Series No. 8, ISBN 92-0-102395-2

[6] Safety Assessment and Verification for Nuclear Power Plants – A Safety Guide, IAEA, 2001, Safety Standards series, No. NS-G-1.2, ISBN 92-0-101601-8

[7] European Utility Requirement for LWR Nuclear Power Plants; 2002

[8] The Use and Development of Probabilistic Safety Assessment in NEA Member Countries. NEA/CSNI/R(2002)18, OECD, Nuclear Energy Agency, Committee On The Safety Of Nuclear Installations, Paris, 2002, http://www.nea.fr/html/nsd/docs/2002/csni-r2002-18.pdf.

[11] Probabilistic safety analysis in safety management of nuclear power plants, Guide YVL 2.8, Radiation and Nuclear Safety Authority (STUK), Helsinki, 2003 http://www.stuk.fi/saannosto/YVL2-8e.html

[12] Status of PSA programmes in Switzerland. Committee on the Safety of Nuclear Installations (CSNI) working group on risk assessment (WGRISK) sixth annual meeting OECD, Paris 2–4 November 2005.

[13] HM Nuclear Installations Inspectorate Safety Assessment Principles for Nuclear Plants. http://www.hse.gov.uk/nuclear/saps/saps1992.pdf

[14] NII Safety Assessment Principles, 2005 Revision, Numerical Targets Safety Assessment Principles, http://www.hse.gov.uk/nuclear/saps/numtargetint.pdf

[15] Nuclear Regulatory Commission, 10 CFR Part 50, Safety Goals for the Operation of Nuclear Power Plants; Policy Statement; Revision 1, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2001/secy2001-0009/2001-0009scy.html#ATTACHMENT1

[16] Basic safety principles for nuclear power plants, 75-INSAG-3, International Atomic Energy Agency, Vienna, 1988.

[17] Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1 INSAG-12, International Atomic Energy Agency, Vienna, 1999. http://www-pub.iaea.org/MTCD/publications/PDF/P082_scr.pdf

[18] USNRC; Reactor safety study : an assessment of accident risks in U.S. commercial nuclear power plants; WASH-1400 / NUREG-75/014, 1975

[19] Farmer, F.R.; Reactor Safety and Siting: A Proposed Risk Criterion; Nuclear Safety 8(6), 539-548; 1967