

Prospects for use of probabilistic safety criteria

F.Niehaus*

International Atomic Energy Agency, Vienna, Austria

1 INTRODUCTION

All industrial installations are sources of routine or potential (accidental) risk to public health and the environment. Whereas in the past more emphasis was given to reduce and limit routine exposure, the recent accidents in the nuclear and chemical industry, in transportation, and in construction (dam failures, impact on buildings from earthquakes) have drawn more attention to the problem of severe accidents. This shift in emphasis is also caused by the trend to build larger and more complex installations. Table 1 shows, however, that severe accidents contribute only a small fraction to the total number of immediate accidental death in a population (Chakraborty, 1986).

Table 1. Comparison of the Mathematical Expectation of Death in the USA (1973)

Type of Hazard	Deaths per year per 100,000 people
Natural catastrophes (global)	1.0
Severe accidents associated with large technical complexes	0.22
Daily (small) accidents caused by transport, work, etc.	58

Design against accidents is so far mainly based on deterministic criteria. Deterministic criteria consist of a set of engineering principles (e.g. defense-in-depth, redundancy, diversity, fail-safe) and design against a set of pre-selected, so-called design base accidents. To analyse the remaining risk and to find optimal ways to reduce risks is called risk management.

The management of risks is based on two principles:

- risk can be reduced below any given level, however, not to zero, and
- the cost of further risk reduction increases with the level of safety achieved.

*The views expressed in this paper do not necessarily reflect the position of the IAEA

It is thus necessary to find a balanced approach for cost-effective risk reduction. There are three paths to reduce risk from accidents both for using prevention and mitigation strategies:

- a) more extended application of engineering principles,
- b) extension of the set of design base accidents to include more unlikely events, and
- c) analysis and quantification of the remaining risk, and risk reduction based on decision criteria (i.e. probabilistic safety criteria).

It is clear that all three options have to be followed and that the deterministic approaches (a and b) and the probabilistic approach (c) have to complement each other. The probabilistic approach also provides a rational tool to check on the balance and risk significance of measures taken based on a) or b). This paper will concentrate on the probabilistic approach especially as it relates to nuclear plants.

2 NEED FOR PROBABILISTIC SAFETY CRITERIA (PSC)

Probabilistic Safety Analysis (PSA) is a tool to evaluate the balance of use of deterministic criteria and to analyse specifically severe accidents, i.e. low probability/high consequence accidents. It is a systematic way, which can be computerized (Wild, 1983), to answer the questions:

- a) What can go wrong?
- b) How likely is it to occur?
- c) If it occurs, what are the consequences?

It is very clear that such an analysis has merits on its own without formal use. It improves the understanding of plant behaviour under abnormal conditions, of man-machine interaction, and of the relative importance of safety functions, systems and components. It is an additional training tool and can be used for many purposes including designing operator computer aids or developing accident scenarios for simulator training. However, in addition to all these qualitative insights gained, it also provides quantitative estimates of the probability of initiating events, accident sequences, core-melt scenarios (level 1 PSA), failure of containment and categories of radioactive releases (level 2 PSA), and consequences for human health and the environment (level 3 PSA). PSA results display uncertainties, which increase with the level of PSA performed. Uncertainties do exist in any approach towards safety and are not introduced by PSA. However, PSA is a method to identify the uncertainties and to rigorously deal with them in the analysis. It can, of course, not substitute for lack of knowledge, but it can help to identify information gaps. It is necessary and desirable that the best use is also made of these quantitative results. However, quantitative results need quantitative criteria against which to judge their implications, i.e. in this case probabilistic safety criteria (PSC). The following gives some more specific reasons why PSC are needed.

2.1 Worldwide use of PSA as a standard tool

More than 30 PSAs have been performed for nuclear power plants including Light Water Reactors, Fast Breeder Reactors and High

Temperature Gas Cooled Reactors. In an interregional technical co-operation programme the IAEA is assisting about 20 Member States from developing countries to perform PSAs for nuclear power plants and research reactors. All these studies are leading to quantitative results, which will be compared (however, with great care). This situation calls for a standardization of the analytical tool (with this objective the IAEA develops PSA guidelines (IAEA, 1986)) and the development of probabilistic safety criteria to judge the results.

2.2 Use of PSA in design

As mentioned above safety of nuclear plants basically relies on deterministic criteria. PSA is the tool to judge the safety of a certain design, in particular the reliability of safety functions and systems, considering certain categories of initiating events and accident scenarios. The objective is to reach a "balanced" safety design. It also includes the rôle of functions and systems under conditions which would not be covered by the set of design base accidents. These requirements reinforce the need to develop PSC at the level of safety functions/systems (see IAEA 1987b).

2.3 Use of PSA in licensing

A number of IAEA Member States use to a varying degree and in different ways PSA in licensing. For a survey see (IAEA 1987a, 1987b). An example is given in Table 2 (Finnish Centre for Radiation and Nuclear Safety, 1985). It shows that a so-called "Mini-PSA" has to be performed before construction permit application. In the course of the licensing process a level 1 and level 2 PSA is required. If no formal PSC exist to evaluate a design including siting decisions, in fact such criteria will be implicitly used by comparing with PSAs for other plants accepted as "safe designs".

Table 2. Schedule of using PSA in licensing (Finland)

Construction Permit Application	Mini-PSA
Construction Permit	Review of the Mini-PSA in STUK Correction of the Mini-PSA
Operating License Application	PSA of Level 1
Operating License	PSA of Level 2 Review of the PSA of Level 1 in STUK Corrections Conclusions
	Correction of the PSA of Level 2 after the Start-up Testing

2.4 Use of PSA for operation

PSAs are in particular useful, if the analysis is kept as a "living document" which is continuously updated as operational experience becomes available. In this way PSA results can be used in the day-to-day operation of the plant. In this context two types of uses need particular attention.

2.4.1 PSA on personal computer in the control room

The recent advances in computer technology make it possible to store the results of a complete level 1 PSA on a personal computer. In this way it can be more easily updated and information can be retrieved in a short time. Several such systems exist (see e.g. Fussell, 1986; Riley, J. & B. Putney, 1983). They can be used to obtain information about the new risk profile of the plant under certain operating conditions. Typically such information includes new core-melt probability, ranking or probabilities of accident scenarios, or importance ranking of safety systems. Though this information can be used in a qualitative way, any decision based on this information will imply certain probabilistic safety criteria.

2.4.2 Technical Specifications

The type of information mentioned in 2.4.1 can also be used to derive Technical Specifications including optimization of maintenance schedules or Limiting Conditions for Operation. Reliability criteria for safety functions or systems are practicable aids for such decisions.

2.5 Advanced designs

Advanced reactor designs will be based on a set of deterministic criteria, which include smaller size, lower power density, simplification, more inherent safety features and passive systems, standardization and prefabrication. However, given the present state-of-the-art of PSA these designs will also be judged based on reliability of safety functions, core-melt probability (if applicable), probability of radioactive releases and risk to public health and the environment. Thus, implicitly or explicitly PSC will be applied.

2.6 Consistency between radiation protection and nuclear safety

As mentioned in the introduction more emphasis is now given to severe accidents. In the nuclear area it would be important that, if probabilistic safety criteria are used, they would be consistent with those criteria established in radiation protection for routine exposure. This task is very controversial. The dose limitation system in radiation protection cannot easily be transferred to PSC. The similarity between the approach in radiation protection and nuclear safety is indicated in Fig. 1. It should be noted that similar to nuclear safety the original approach in radiation protection was deterministic. PSA now provides the means to obtain a measure of the residual unsafety of a plant. In order to achieve

consistency between the two approaches it would be necessary to reach agreement on how to measure "risk".

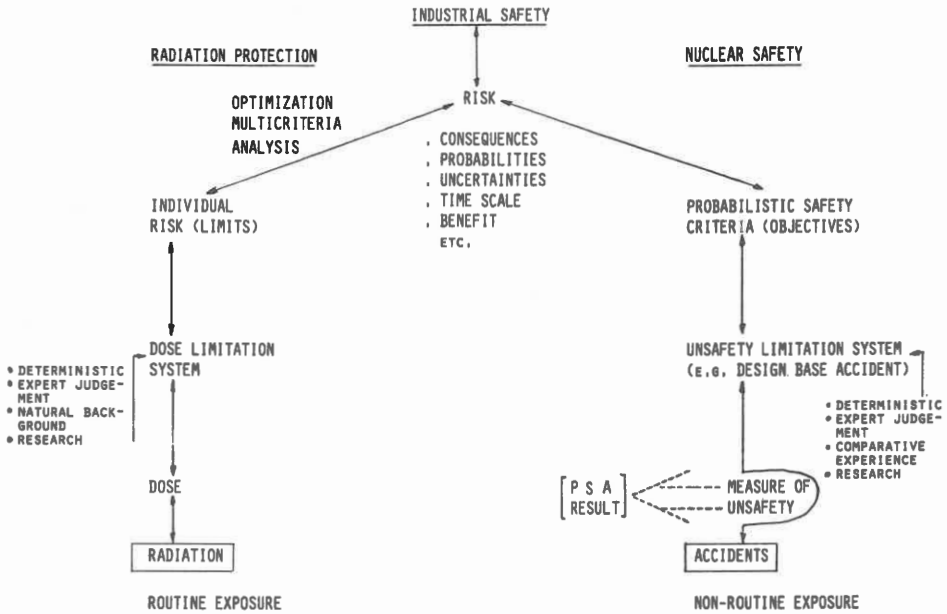


Fig. 1. Comparison of philosophy in radiation protection and nuclear safety.

2.7 Industrial safety

Such an approach also establishes a link to industrial safety in general.

There is no doubt that, in the future, developing and developed countries will place more emphasis on reducing risks from accidents and routine operation of industry in general. To analyse potential accidents PSA is spreading rapidly into the chemical industry (U.K. Health and Safety Executive, 1978; Public Authority Rijnmond, 1982; Seaman, 1986). This spread will be even more rapid if reductions will be given for insurance premiums in case a PSA has been performed for a specific facility (Hicks, A.J. & M. Considine, 1986). Considering both accidents and routine operation, a Joint IAEA/UNEP/WHO Project on Assessing and Managing Health and Environmental Risks from Energy and Other Complex Industrial Systems has been established. This Project calls for a number of regional (region within a country) case studies, collection of an international data base, and training activities. A risk management procedures guide will be prepared based on this experience. This project also reflects the need to develop a consistent approach towards safety for all industries.

3 SUMMARY OF STATUS OF PSC DEVELOPMENT

PSC have been proposed, are under development or are actually being used by countries at various levels. Table 3 summarizes such approaches as they relate to the level of PSA which would be required to show compliance.

Table 3. Levels of proposed PSC and required level of PSA to show compliance.

	LEVEL OF P S C	LEVEL OF P S A
PLANT	SAFETY COMPONENTS SAFETY SYSTEMS SAFETY FUNCTIONS	LEVEL 0 = RELIABILITY STUDIES
	CORE MELT	LEVEL 1
	CONTAINMENT PERFORMANCE	LEVEL 2
PUBLIC HEALTH	INDIVIDUAL RISK SOCIETAL RISK COST-BENEFIT (EFFECTIVENESS)	LEVEL 3

3.1 PSC at the level of public health

3.1.1 Individual risk

The basic approach to formulate PSC for individual risk is to set an objective for the probability of death (e.g. 10^{-6} per year) or of a defined health effect. To set such an objective is of course not a scientific question, but must fundamentally be based on a judgement of society's view. It would not be in society's best interest to set such an objective too high or too low. Too high an objective would mean inadequate protection of the public. Too low an objective would mean hinderance of technological development and waste of society's limited resources on insignificant risk reduction. Therefore, all such suggestions are derived on a comparative basis from other risks to which society is exposed, e.g. low risk groups in society (Versteeg, 1986), total accidental risk and cancer risk in the vicinity of a site of a NPP (USNRC, 1986), or risk implied in standards for radiation exposure (González, 1983, International Commission on Radiological Protection, 1985, Gottschalk, 1986). The last three examples refer to radiation accidents and suggest that one should distinguish between two kinds of probabilities: the probability of having an accident and the probability of death given an exposure from that accident. Such a separation is implicit by using a "boundary" line for the probability of exposure levels (González, 1983), a histogramme for the probability of accidents related to certain exposure intervals (Snell, 1986) or a complementary cumulative distribution function (CCDF) (Gottschalk,

1986). The example using the format of histogrammes is given in Fig. 2. Such an approach implies that the sum of the probabilities of accident sequences, leading to exposures in a given interval, has to be less than the indicated probability.

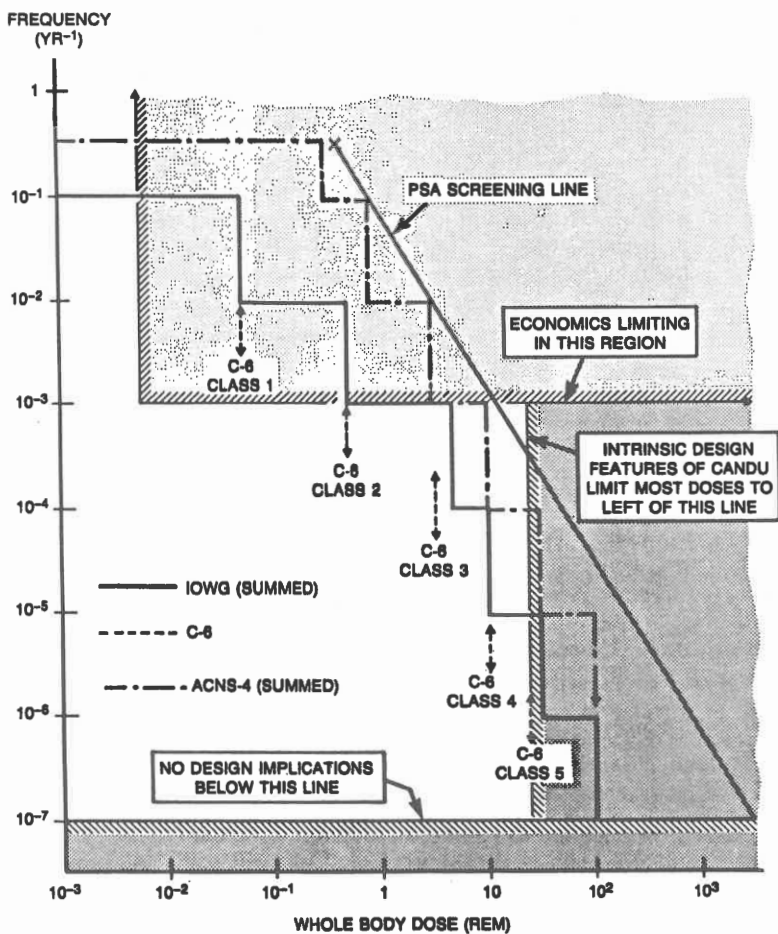


Fig. 2. Comparison of safety goals and "natural" restrictions

3.1.2 Societal risk

Several suggestions have been made to put additional constraints on accidents which affect many people at the same time. This can be achieved by assigning a weighting factor to large consequences (e.g. exponential, Griesmeyer, J.M. & D. Okrent, 1980) or by assigning a slope of less than -1 to a boundary line in a probability/consequence diagramme on log-log scale (Higson, 1986; Levine, 1980; Kinchin, 1978). Fig. 3 gives a recent example (Versteeg, 1986) which includes three areas: acceptable, reduction desired, and unacceptable.

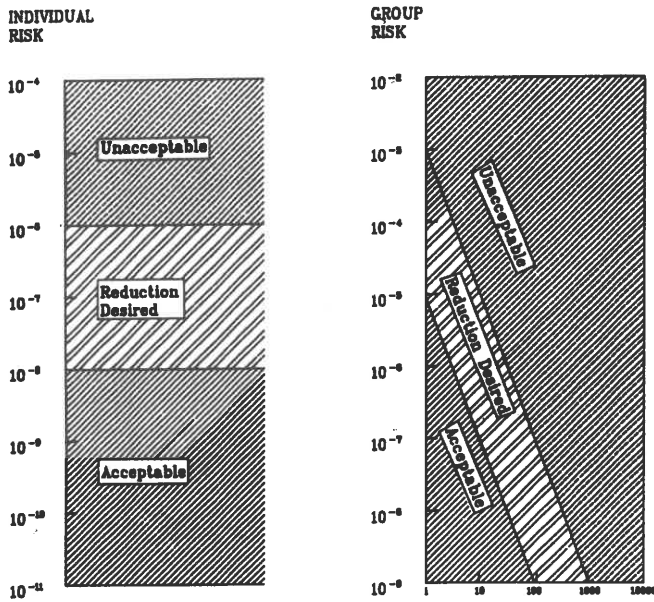


Fig. 3. Preliminary Safety Criteria (Netherlands)

It should be noted that in principle it is also possible to link the acceptable level of individual risk to the number of people exposed to that risk (J. Cohen, 1986).

3.1.3 Cost-effectiveness criteria

Some suggestions have been made to apply cost/benefit or cost-effectiveness criteria below an objective or in a certain range. An example using \$ 1000 per expected man-rem averted, linked to ranges of core-melt probabilities, has been described in (Sniezek, 1986).

3.2 PSC at the plant level

Whereas so far most of the work to develop PSC was concentrated on the level of public health, emphasis is now being given to develop PSC at the plant level, in particular for safety functions/systems. It is expected that such criteria would be more practical and easier to use because the uncertainties are better understood for lower levels of PSA. On the problem of uncertainties reference is made to the benchmark studies of the CEC (Amendola, 1986).

3.2.1 Review of level 1 and 2 PSC at the plant level

PSC which would require a level 2 PSA include probabilities for large releases of radioactive materials (e.g. 10^{-6} per year, USNRC, 1986)

or containment performance criteria (e.g. 10^{-1} to 10^{-2} given a core-melt). The latter poses a specific problem if vented containments are to be included. At the level 1 PSA, typically core-melt criteria (e.g. 10^{-4} to 10^{-6} per year) or probability objectives for accident sequences are being proposed. The latter are usually not in the form of probabilities. Rather it is proposed that a single category of accident sequences should not dominate core-melt, e.g. not contribute more than 10% to total core-melt probability (e.g. Ferreli, 1986). It should be noted that there is no generally agreed definition of core-melt. The use of the word core-melt ranges from fraction of core destroyed to exceedance of certain temperatures of fuel elements, not necessarily resulting in any melting.

3.2.2 PSC at the level of safety functions/systems

Recent effort is concentrated at this level. An example of criteria which are in preliminary use, is given in Table 4 (Virolainen, 1986). A discussion of such concepts can be found in (IAEA, 1987b). It is especially important that the boundaries of safety functions or systems are clearly defined, i.e. which support systems are included.

Three ways have been identified how such PSC can be defined:

- a) logically relating them to higher level objectives
- b) comparison to similar designs which have been accepted as "safe"
- c) removal of peak contributions of certain functions and systems thus leading to a more balanced design.

They can be also related to specific categories of accident sequences. Such safety function/system PSC would be practical tools to derive Technical Specifications including Limiting Conditions for Operation.

Table 4: Examples of Probabilistic Safety Criteria at the Safety Function Level

<u>Safety Function</u>	<u>Unreliability</u>
Making the reactor subcritical	10^{-5}
Isolation of the containment	10^{-3}
Supply of feed-water when the off-site power or the main feed- water supply is lost	10^{-4}
Operation of emergency core cooling in the case of a small reactor coolant leak	10^{-4}
Rapid reactor pressure reduction and long-term pool cooling (BWR)	10^{-4}

Here a 95% confidence concept has been adopted.

4 CONCLUSIONS: TOWARDS INTEGRATED HIERARCHICAL PSC

4.1 Set of consistent PSC at all levels

On one hand the paper has stated that there is a trend, for practical reasons, towards plant-level criteria. On the other hand, it is necessary to provide for a link to radiation protection principles

and to safety of industrial installations in general. The solution to this dilemma of course is to establish a set of consistent PSC at all levels as, e.g. outlined in Fig. 4. Such an approach would also provide for the possibility that countries could choose from such integrated hierarchical PSC the level of criteria which would be best suitable to complement the existing requirements. It should be noted, however, that for a set of lower level criteria, using a PSA for a specific plant, it is always possible to calculate which higher level goals are implied, i.e. ultimately, which level of individual and societal risk is implied.

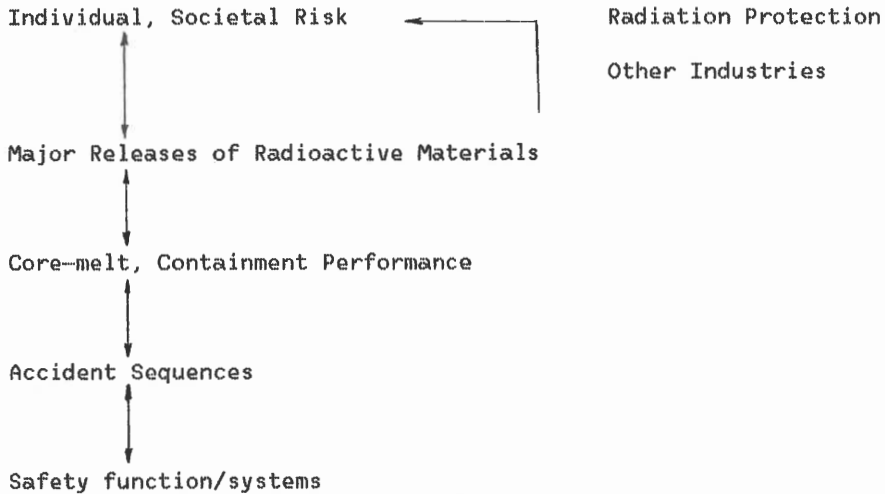


Fig. 4: An integrated hierarchical approach to PSC at all levels

4.2 How to show compliance

Precise definition of how to deal with the uncertainties of PSA-results is the single most important problem in establishing PSC which are of practical use. Suggestions made include use of confidence intervals (e.g. Virolainen, 1986) or compliance indices which could be derived using fuzzy set theory (Unwin, S.D., & M.R. Hayns, 1985). A pragmatic approach which needs to be better explored in the future could be based on a combination of the probabilistic and the deterministic approach. It could have the following features:

1. Standardization of PSA as will be suggested in the PSA guidelines under development by IAEA (IAEA, 1986), including standardized methods for uncertainty and sensitivity analysis.
2. Description of what is technically leading to the tails of the uncertainty distributions exceeding predefined PSC (see also USNRC, 1986).
3. Deterministic approach to exclude or design against the tails of these distributions.

The first point still needs much development work. The last two points still need to be further explored since they also pose serious mathematical and conceptual problems.

REFERENCES

- Amendola, A. 1986. Systems Reliability Benchmark Exercise. Final Report. Part I - Description and Results. Commission of the European Communities, Joint Research Centre Ispra Establishment, Italy. EUR 10696/I EN.
- Chakraborty, S. 1986. Possibilities and limitations of risk comparisons in the light of development of risk criteria for the nuclear fuel cycle (part of an IAEA coordinated research programme on development of risk criteria for the nuclear fuel cycle).
- Cohen, J., 1986. Personal communication.
- Ferrelli, A., 1986. Status of Probabilistic Safety Criteria in Italy. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1987.
- Finnish Centre for Radiation and Nuclear Safety, 1985. Probabilistic Safety Analyses in the Licensing and Regulation of Nuclear Power Plants. Guide YVL 2.8.
- Fussell, J.B., & D.J. Campbell, 1986. PRISIM - A Computer Program That Makes PRA Useful. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1986.
- González, A.J., 1983. The Regulatory Use of Probabilistic Safety Analysis in Argentina, Proc of the Int. Meeting on Thermal Nuclear Reactor Safety, Chicago, Ill., Aug. 29 - Sept. 2, 1982, NUREG 0027, Vol. 1.
- Gottschalk, P., 1986. Approach to PSA Methods and Probabilistic Safety Criteria in Licensing of NPP in the Federal Republic of Germany. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1986.
- Griesmeyer, J.M. & D. Okrent, 1980. Risk Management and Decision Rules for Light Water Reactors. In: An Approach to quantitative Safety Goals for Nuclear Power Plants. NUREG-0739, U.S. Nuclear Regulatory Commission, Washington D.C.
- Hicks, A.J. & M. Considine, 1986. Present and Future Needs for Formal Risk Assessment Procedures - An Insurance Viewpoint. Presented at the First International Conference on Risk Assessment of Chemicals and Nuclear Materials, 22-26 September 1986, Guildford, Surrey, U.K.
- Higson, D.J., 1986. Some Questions on the Development of Probabilistic Risk Criteria. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1986.
- International Atomic Energy Agency, 1986. Guidelines for the Conduct of Probabilistic Safety Analysis of Nuclear Power Plants. Report on an Advisory Group Meeting, 1 - 5 December 1986, Vienna, Austria.
- International Atomic Energy Agency, 1987. Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria. Report on a Technical Committee Meeting, 27-31 January 1986, Vienna, Austria. To be published as IAEA-TECDOC-XXXa.
- International Atomic Energy Agency, 1987. Probabilistic Safety Criteria at the Safety Function/System Level. Report on a Technical Committee Meeting, 26-30 January 1987, to be published as IAEA-TECDOC-XXXb

- International Commission on Radiological Protection, 1985. Radiation Protection Principles for the Disposal of Solid Radioactive Waste. ICRP Publication 46, Annals of the ICRP, Vol. 15, No. 4. Pergamon Press, Oxford, New York, Frankfurt.
- Kinchin, G.H., 1978. Assessment of Hazards in Engineering Work, Proc. Inst. Civ. Eng., Part I: Design and Construction, 64(1):431-438.
- Levine, S., 1980. Various Applications of Probabilistic Risk Assessment Techniques Related to Nuclear Power Plants, presented at the Annual Meeting of the National Safety Council, Chicago, October 1980.
- Public Authority Rijnmond, 1982. Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area. A Pilot Study. D. Reidel, Dordrecht, Holland.
- Riley, J. & B. Putney, 1983. The Risk Management Query System. Presented at the 1983 International Reliability Availability Maintainability Conference.
- Seaman, M.A., 1986. International Experience in Assessment of Risks Due to Oil and Gas Production and Chemicals Manufacture. Paper presented at the Joint IAEA/UNEP/WHO Workshop on "Assessing and Managing Health and Environmental Risks from Energy and Other Complex Industrial Systems", Paris, 13-17 October 1986. To be published as IAEA-TECDOC-XXXX.
- Snell, V.G., 1986. Probabilistic Safety Assessment Goals in Canada. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1987.
- Snizek, J.H., 1986. An Integrated Safety Goal Concept. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1987.
- U.K. Health and Safety Executive, 1978. Canvey: Summary of an Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock Area. U.K. Health and Safety Executive London, U.K.
- Unwin, S.D., & M.R. Hayns, 1985. Rational Quantitative Safety Goals Proc. ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, Vol 1, Sess. 2 (Safety Goals), 11-1 to 11-10, San Francisco, California, February 24-March 1, 1985.
- U.S. Nuclear Regulatory Commission, 1986. Safety Goals for the Operations of Nuclear Power Plants; Policy Statement. 10 CFR PART 50. USNRC, Washington, D.C.
- Versteeg, M.F., 1986. External-Safety Policy in the Netherlands: An Approach to Risk Management. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1987.
- Virolainen, R., Use of Reliability and Risk Standards as Bases for Acceptance in Licensing and Regulation of Nuclear Power Plants. Paper presented at the Technical Committee Meeting "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria", Vienna, 27-31 January 1987.
- Wild, A., 1983. Fault Tree Analysis with Computers. Paper presented at the 1983 International Reliability Availability Maintainability Conference.