STATUS, EXPERIENCE AND FUTURE PROSPECTS FOR THE DEVELOPMENT OF PROBABILISTIC SAFETY CRITERIA

REPORT OF A TECHNICAL COMMITTEE MEETING
ORGANIZED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY
AND HELD IN VIENNA, 27–31 JANUARY 1986
The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.
FOREWORD

This report was prepared by the members of the Technical Committee based on the opinions expressed and on the information available at the time of the meeting.

It should be recognized, however, that some developments and new formulations have emerged since then and are not necessarily reflected in this report.

To consolidate the state-of-the-art knowledge and the international experience in this field and to provide guidance to Member States on the "Role and Use of PSA and PSC in NPP Safety", a document is being prepared for publication in the IAEA Safety Series.

This TECDOC is being used as reference material for the development of the above referred guideline.

Complementary to this, a number of additional publications are also under preparation for publication in the IAEA Safety Series on recognized practises for the conduct of PSA and on specific elements of PSA such as common cause failures, human errors and external hazards.
EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts as submitted by the authors and given some attention to the presentation.

The views expressed in the papers, the statements made and the general style adopted are the responsibility of the named authors. The views do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

Authors are themselves responsible for obtaining the necessary permission to reproduce copyright material from other sources.
PAPERS PRESENTED AT THE MEETING

An integrated safety goal concept ................................................................. 55  
J.H. Sniezek

External safety policy in the Netherlands: an approach to risk management .......... 69  
M.F. Versteeg

Probabilistic safety assessment goals in Canada ........................................... 79  
V.G. Snell

Status of probabilistic safety criteria in France ............................................ 95  
P. Candes

Status of probabilistic safety criteria in Italy ............................................... 105  
A. Ferreli

The Swedish view of probabilistic safety criteria — present status ................ 117  
L. Carlsson

Development of the non-dimensional method of ranking risks ....................... 125  
J.C. Chicken, M.R. Hayns

A method to incorporate uncertainty and degree of compliance in safety goals .... 137  
M.R. Hayns, S.D. Unwin

Prospects for probabilistic safety criteria (PSC) .......................................... 165  
F. Niehaus

The use of probabilistic methods in the licensing of nuclear power plants:  
a recent example ......................................................................................... 177  
U. Bäverstam, C. Wiktorsson

Use of reliability and risk standards as bases for acceptance in licensing and regulation  
of nuclear power plants ........................................................................... 183  
R. Virolainen

Comparison of different societal risks: a new limit-line concept ................... 195  
H.A. Munera

Approach to PSA methods and probabilistic safety criteria in licensing of  
nuclear power plants in the Federal Republic of Germany .......................... 205  
P. Gottschalk

The regulatory use of probabilistic safety analysis in Argentina (Abstract) ........ 211  
A.J. Gonzalez

Prospect theory and limit lines (Abstract) .................................................. 213  
Jya Syin Wu-Chien, G. Apostolakis

Risk aversion in risk acceptance criteria (Abstract) .................................... 215  
Jya Syin Wu-Chien, G. Apostolakis

Risk management application of fire risk analysis (Abstract) ...................... 217  
M. Kazarians, N. Siu, G. Apostolakis
PRISIM — A computer program that makes PRA useful .............................................. 219
   J.B. Fussell, D.J. Campbell, J.C. Glynn, G.R. Burdick

CEC task force on safety goals (Summary) ................................................................. 229
   Commission of the European Communities

Some questions on the development of probabilistic safety criteria .......................... 233
   D.J. Higson

List of Participants .................................................................................................... 239
EXECUTIVE SUMMARY

During 27–31 January 1986 the IAFA held a Technical Committee Meeting on "Status, Experience, and Future Prospects for the Development of Probabilistic Safety Criteria". Participation included representation of essentially all countries with major developments in the area as well as the Nuclear Energy Agency (NEA) of the OECD and CFC (see list of Participants). Though it has to be recognized that in such a short time period it is impossible to resolve or even analyse all aspects of this complex issue, the present situation, the main problems and the directions for future work clearly emerged.

Status of Probabilistic Safety Criteria (PSC)

Detailed information on the status within various countries can be found in individual papers in the body of the report. An overview of proposed PSC and the required levels of a Probabilistic Safety Analysis (PSA) to show compliance is given in Table 1 of Chapter I. There is general agreement that PSC can be used for various objectives. However, their status and use varies. One group of countries is already using them (or is close to a final decision to do so) for safety decisions including design, licensing and operation. Another group of countries is at present debating the basic concepts and their implications. The third group of countries is monitoring the developments for possible use. Across this spectrum of groups, some countries envisage using PSC both at the plant level and the level of public health. Other envisage using PSC only at the plant level.

Radiation protection — nuclear safety

One key issue of the discussions was the relationship between principles for radiation protection and probabilistic criteria for nuclear safety. The meeting took note of the Agency's programme in radiation protection [1], work in the area of radioactive waste disposal [2], the recent ICRP publication 46 [3], and the work of NEA on this subject [4].

ECRP basically proposes:

1a) to extend the radiation protection principles in the context of radioactive waste, implying an overall limit for individual risks with upper bounds assigned to separate sources of risk;

1b) to leave further risk reduction to the optimization process (AIARA) which could utilize a variety of methods including multi criteria analysis or cost-benefit analysis and would also consider societal risk in a way not explicitly specified.

This suggestion has the advantage of consistency between radiation protection and nuclear safety. However, safety engineers propose a different concept.

ad 1a): Because of the uncertainties inherent in PSAs it is claimed that it may be difficult or impossible to demonstrate compliance with limits or upper bounds for individual risk in the legal sense. Therefore, significantly lower levels of individual risks are usually proposed for use as objectives (guidelines, goals, target values, or assessment reference levels), but not as limits or upper bounds. Such a concept allows to demonstrate compliance by explicitly making use of estimated uncertainties.
ad b): Different from the main work and experience in radiation protection, a significant aim in nuclear safety is to put emphasis on reducing the probability of severe accidents which could affect a large number of people from one event. Therefore, it is felt that if PSC are to be established at the public health level, they ought to explicitly, and not implicitly as in radiation protection, include societal risk targets which discriminate against large consequence accidents, rather than leaving this to a not precisely specified concept such as optimization. In order to achieve this goal some approaches use an individual dose boundary line histogram or CCUF with risk aversion as well as or instead of societal risk targets.

Though the numbers proposed in the literature do not vary widely, the main problem at this time is to choose justifiable numerical values and to identify the framework for showing compliance. This includes a common approach in estimating risks. Of major concern is any weighting factor (or exponent) which would represent the relative significance of large consequences. This problem is common to the radiation protection approach of optimization and the nuclear safety approach of probability-consequence relationships. The former needs to establish a (maybe non linear) weighting factor, the latter has to determine as an equivalent the slope of the line representing this relationship.

PSC at the level of public health - PSC at the plant level

The second key issue centres around the question if PSC can and should be established at the public health level i.e. for individual or societal risk. There was general agreement that it is useful to establish PSC at the plant level (e.g. PSC for safety functions) up to core melt PSC including containment. At the level of public health some countries are using or proposing PSC, some countries explore the possibility and others have no such plans at present. There is general agreement that a system of PSC including different levels should be consistent, however, not necessarily in such a way that it can be demonstrated in a strict mathematical statistical sense.

Outlook

The main benefit of PSA is to provide qualitative and quantitative insights in plant design and performance, including identification of dominant risk contributors and comparison of proposals for reducing risk. In addition PSA is the mathematical and conceptual tool to derive numerical estimates of safety (or safety margins) of nuclear plants and industrial installations in general. PSC provide the means to evaluate the results and to establish a consistent framework for nuclear safety. The future will see a large variety in its use. It is important that Member States take note of this situation. This report is meant to serve this purpose.
1. SUMMARY OF STATUS AND POSITIONS

1.1 Background

In the traditional deterministic approach to safety in the nuclear industry, the safety levels were set by using conservative assumptions based on judgment and experience. However, it became apparent that a more consistent approach could be achieved by incorporating probabilistic concepts and techniques which made it possible to make direct comparisons between different types of plant and take account of the effect of uncertainties. By the time of the TMI-2 accident, the techniques of probabilistic safety assessment were well established (e.g., WASH-1400 and the German Risk Study) but the accident gave added impetus to the use of probabilistic techniques for severe accident analysis. (For a discussion of probabilistic and deterministic approaches to safety see e.g. [5,6]).

PSC are already written into the nuclear regulations of some countries and are being actively considered for implementation in others. Although there is a marked resistance in some countries to the implementation of PSC at the level of public health, the use of lower level PSC (see Table I) makes it possible to set quantitative safety objectives at these levels for the operation of the plant.

<table>
<thead>
<tr>
<th>Level of PSC</th>
<th>Level of PSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety components</td>
<td>Level 0</td>
</tr>
<tr>
<td>safety systems</td>
<td>= reliability studies</td>
</tr>
<tr>
<td>safety functions</td>
<td></td>
</tr>
<tr>
<td>initiating events</td>
<td></td>
</tr>
<tr>
<td>accident sequences</td>
<td>Level 1</td>
</tr>
<tr>
<td>core melt</td>
<td></td>
</tr>
<tr>
<td>containment performance</td>
<td>Level 2</td>
</tr>
<tr>
<td>large release of radioactive materials</td>
<td></td>
</tr>
<tr>
<td>individual risk</td>
<td>Level 3</td>
</tr>
<tr>
<td>societal risk</td>
<td></td>
</tr>
<tr>
<td>cost-benefit (effectiveness)</td>
<td></td>
</tr>
</tbody>
</table>

TABLE 1. LEVELS OF PSC AND REQUIRED LEVEL OF PSA TO SHOW COMPLIANCE
This technical report summarizes the status of PSO and explores likely future developments in this area.

1.2 Basic definitions

It will be noted from the various papers in this report that there is an urgent need to agree on a standard set of definitions of key technical terms as they relate to PSO. A consistent set of definitions regarding radiation protection principles for the disposal of solid radioactive waste is given in Appendix 1. However, this terminology is not generally used in nuclear safety and incomplete as far as many aspects of nuclear safety are concerned. The following addresses some of these problems also exposing conceptual difficulties.

Frequency

refers to the outcome of an experiment of some kind involving repeated trials and is a well defined, objective measurable number. The word experiment should be interpreted rather generously to include thought experiments.

Probability

is a numerical measure of a state of knowledge, a degree of belief, a state of confidence. The probability scale may be defined by using frequency as a standard of reference. (It should be noted that probability is defined differently in Appendix [].)

Uncertainties

is a concept expressing the incompleteness of, or the imprecision in, an estimate or assessment. Distributions are commonly used to describe uncertainties. They can have the form of histogrammes, density functions (for continuous variables) or cumulative density functions indicating confidence levels. If a well-known shape of the distribution is assumed, often uncertainty intervals (e.g. 90% confidence intervals) are displayed.

Risk

is used in the risk assessment literature (see e.g. [7,8]) to describe the set of probabilities and adverse consequences (thus including by definition uncertainties). However, since the word has been borrowed from the non-scientific literature it is often used to describe some aspect of risk only. In radiation protection it is specifically used to denote "the probability of a serious detrimental health effect in a potentially-exposed individual or his descendants" [3].

Individual Risk

is the set of probabilities and adverse consequences as they relate to an individual.

Societal Risk

Societal risk is the set of probabilities and adverse consequences as it relates to society. It is thus the sum of individual risks plus the set of probabilities and additional adverse consequences for society. The latter includes in particular social disruption as might be caused by accidents which result in a large number of immediate deaths at the same time in a small area.
Probability/Density Function (PDF) of adverse consequences

![Figure 1. PDF.](image)

\[ P_{\Delta C} = \int_{C_1}^{C_2} f(c) \, dc \quad (\text{Eq. 1}) \]

\[ E_{\Delta C} = \int_{C_1}^{C_2} c \, f(c) \, dc \quad (\text{Eq. 2}) \]

where

- \( c \) = adverse consequences
- \( f(c) \) = probability density of \( c \)
- \( P_{\Delta C} \) = probability of adverse consequences in interval \( \Delta C \)
- \( E_{\Delta C} \) = expectation value of adverse consequences contributed by interval \( \Delta C \)

A PDF can be approximated by a histogram.

Cumulative Probability Density Function (CDF) of adverse consequences

![Figure 2. CDF.](image)

\[ F(c) = \int_0^c f(c') \, dc' \quad (\text{Eq. 3}) \]

where

- \( f(c) \) = probability of adverse consequences smaller than any given \( c \)
Complementary Cumulative Probability/Density function (CCDF) of adverse consequences

\[ f(c) = 1 - F(c) \cdot \left(1 - \int_0^c f(c') \, dc'\right) \]

where
\[ f(c) = \text{probability of adverse consequences larger than any given } c \]

Risk Curve in CCDF format with point estimates of uncertainty giving confidence intervals (log log scale)

(As e.g. used in [9,10])

Fig. 3. CCDF.

Fig. 4. Risk curve in CCDF format with confidence intervals.
Risk Curve in CCUf format with confidence levels

![Risk Curve Diagram](image)

**Fig. 5. Family of risk curves.**

The cross section A gives the CDH of \( f(c) \) and can be visualized in the 3rd dimension.

**Boundary line (farmer-type limit line):**

As a concept relates frequencies or probabilities to adverse consequences in a direct continuous functional relationship \([3,11,12]\). It can be used to screen point estimates. Since it allows for an infinite number of infinite small consequence categories it cannot be integrated to limit the expected adverse consequences contributed by any interval \( C \) as defined in Equation 2. In order to reach a finite expectation value of adverse consequences, it is necessary to put constraints on the number of permissible point estimates. If the frequency or probability scale of such a boundary line is interpreted to apply to an interval (e.g., 1 decade) of adverse consequences, it is similar to a PDF (or a histogram if not continuous intervals are used).

**Risk Limits and Risk Upper Bound**

Have a specific meaning in radiation protection \([3]\) and are described in Appendix I. The terms are usually avoided in nuclear safety because of the conceptual difficulties of demonstrating compliance.

**Severe Accidents**

Is used to denote accidents beyond design basis.

**Core-melt**

Is defined in different ways ranging from severe core damage, fractions of core destroyed to exceedance of certain temperatures. Also differences have to be considered for different reactor design (e.g., CANDU, H1GR, etc.).
Probabilistic Risk Analysis (PRA) Techniques

are the mathematical framework and set of tools to analyse (in a probabilistic manner) risk. Considering the definition of risk above the use of the word "probabilistic" is redundant, but is kept here for historical reasons.

Probabilistic Safety Criteria (PSC): (qualitative and quantitative)

are probabilistically formulated safety requirements for minimizing public and on site risk. They can be established at the level of public health and/or at the plant level (see Table 1) and complement deterministic safety criteria. In accordance with probabilistic thinking PSC are defined in the form of objectives (goals, targets, guidelines) rather than absolute limits.

Probabilistic Safety Assessment (PSA)

is a field of safety analysis which attempts to delineate what accidents can occur, the likelihood of these accidents, and the specific consequences. It provides a structured logical approach to achieve these aims. Level 1 PSAs analyse possible accident sequences up to core melt. Level 2 PSAs model progression of accidents beyond core melt, including containment failure and releases outside containment. Level 3 PSAs include estimates of impact on public health and other off site effects. Table 1 shows how these levels of PSA relate to different levels of proposed PSC.

1.3 Need for PSC

As our level of understanding of the character of safety issues concerning complex systems has increased, the need was recognized for a more comprehensive, coherent and consistent approach to safety than is provided by traditional deterministic methods. PSA is such an approach that has gained considerable acceptance. However, to realize all the potential benefits from PSA, specific PSC are needed.

PSC offer the potential for many applications including:

- determining the level of acceptability and the safety margin with respect to both public and on site safety.

- logically relating the level of safety of many different activities to each other

- allocating more specific safety performance criteria to sub elements of the facility.

- enhancing the public understanding of nuclear safety issues by putting them into perspective.

Specific PSC will also allow evaluation of existing or future deterministic criteria for consistency and completeness.

PSA has now reached a high level of utilization without an internationally accepted basis for guidance with respect to interpretation of the results. A most important aspect of international application of
consistent PSC is a more balanced global allocation of any risk inherent to the endeavours of a nation.

1.4 Summary of Proposed PSC

Member States have developed, and applied, probabilistic safety criteria for various purposes (see body of the report). Also ICRP has developed probabilistic criteria for the disposal of solid radioactive waste [1]. The different levels of PSC are indicated in Fig. 1.

(i) PSC at the Level of Public Health

At the most general level, PSC can be given in terms of risk to an individual or to the population surrounding the nuclear facility. For example, it has been proposed that the time-averaged risk to the most exposed individual should be a small fraction of other industrial risks, or that the time-averaged latent fatality rate (due to the facility) in the surrounding population be a small fraction of the rate due to other causes. Such type of objective allows an immediate comparison of the risk due to the facility, with the risk from industrial activities in general or from other hazards. This requires the use of similar methods and availability of an adequate data base.

Such PSC can be made more restrictive by specifying the shape of the probability vs. consequence curve. Such curves have been developed in form of boundary lines, histograms or CCDFs, both for individual and societal risk. PSC in the form of histograms allow to approximate the mathematical expectation value of individual and societal risk respectively as defined by that histogram within given consequence bands. PSC in the form of CCDFs allow to estimate the total mathematical expectation value as defined by that curve. All actual proposals of this type include an element of risk aversion for high consequences – i.e. a rapid reduction in frequency at the high consequence levels.

PSC at the level of public health are often complemented by cost-benefit or cost-effectiveness criteria.

In many cases, Member States, in exploring use of these PSC at the level of public health, have found it necessary to develop more plant-oriented PSC.

(ii) PSC at the Plant Level

PSC have also been developed and applied at the plant level. These are more specific, and are either derived from PSC at the level of public health or are believed to satisfy such overall objectives by quantifying the more measurable aspects of plant performance.

In order to reduce the probability of accidents it can be useful to place restrictions on the frequency of certain initiating events, which can be repeatedly observed during operation of a plant (e.g. reactor or turbine trip). For more infrequent events reliability studies of design would have to be carried out.

Once an initiating event has occurred, the incident is normally controlled by the plant safety systems [13]. Thus, PSC in the form of reliability objectives can be applied to safety systems and functions and can be substantiated to some degree in practice by testing the safety systems during plant operation.
Another way of achieving this objective is to place restrictions on the probability of certain sensitive accident sequences, especially those leading to core melt. Such sequences are usually chosen from the most significant contributors to public risk.

By establishing a PSC for core melt, one automatically reaches objectives for the risk of prompt fatality for the most exposed individual. Such core melt PSC have been applied by plant designers/owners and are under consideration by the regulatory authority in several countries.

PSC with the objective of mitigating consequences of accidents, e.g. in the form of a reliability target for containment performance to reduce the probability of off-site consequences.

PSC at the plant level can be directly applied during the operation of a nuclear facility to specify the frequency and schedule of inspection, testing, repair and maintenance; to provide an on-line decision-making tool for the owners/operators of a facility to aid in rational decisions when the plant is operating with degraded safety equipment; and finally (although this has not been done in Member States) to set goals for human factors (operator reliability) under accident conditions.

1.5 Range of positions towards PSC

(i) PSC for individual risk

Most approaches in the field of nuclear safety start from the standpoint that risk to an individual of death from radiation should not exceed a small fraction of the risk from other hazards. Many approaches imply the view that the incremental individual risk of death for a member of the public from a single source of radiation exposure should be kept below $10^{-6}$ per year. This is expressed as an objective rather than as an absolute limit. Such PSC have been proposed for early and latent effects [14] based on comparative risk. Another approach identifies a range (e.g. $10^{-6}$ to $10^{-8}$ per year) where risk reduction is desired. A higher risk is unacceptable and a lower risk is acceptable [15]. Limited to the nuclear area such PSC for individual risk is often specified in a more detailed probability-dose relationship. The mathematical concepts include limit-lines [3,16], histograms [17] or CDFs [18].

As described in detail in Appendix I ICRP 46 begins from the established standpoint in radiation protection that continuous exposure of an individual is limited in such a way that, in effect, the incremental probability of death from all sources of radiation (excluding medical and natural radiation) is kept below about $10^{-5}$ per year for a member of the public not occupationally exposed. It should be noted that this statement of implied risk from exposure at the dose limit has a degree of uncertainty attached.

The further step taken in ICRP 46 involves the concept that, in respect of waste management facilities, the incremental individual probability of death from single accidental exposure to radiation should be set at the same level as the incremental probability from continuous exposure, i.e. < $10^{-5}$ per year from all sources.

The intent of ICRP 46 is that regulatory bodies should apply an apportionment procedure so that the incremental frequency of death from single sources of radiation should each be less than, say $10^{-6}$ per year.
Both approaches, nuclear safety and radiation protection, define levels of individual risk from similar thinking and authorities. Because of the history of the topic, ICRP 46 approaches this via the risks from continuous exposure to radiation. In numerical terms, there is little difference, in that the reactor practitioners approach provides the necessary apportionment of risk from a single source e.g. $<10^{-6}$ per year as compared with the ICRP judgment of $<10^{-5}$ per year for all sources.

(ii) PSC for societal risk

In the area of nuclear safety note has also been taken of the common view that for a given mathematical expectation value of consequences a low probability accident potentially involving harm to a large number of people is more serious than an accident of higher probability involving a smaller number of people. This has been converted into PSC for societal risk which place additional restrictions on low probability/high consequence accidents in a probability vs. consequence relationship. This is a controversial issue within the community of nuclear power plant practitioners. While the concept is clear the way it should be applied quantitatively in practice is not. It should be noted that PSC for societal risk can be used for site selection, even if they are not used further in the safety analysis of the plant for licensing or public acceptability.

Proposals include "boundary lines" or CCLMs [19]. Many suggestions have been made to determine the location and slope of such a function in the probability/consequence dimension. Only one Member State is actually using such a PSC for Societal Risk [15].

No directly similar concept can be deduced from radiation protection principles. The nearest parallel is consideration of societal risk as one of the components of the overall optimization process required by ICRP 46.

In this context, the concept of PSC for societal risk may perhaps be seen as an additional restraint, an envelope within which optimization is still pursued, but which itself takes care of the common view that the probability of accidents should decrease overproportionally with the number of potentially affected people.

(iii) Cost-Benefit Criteria

There is a wide spectrum of views. To highlight the position it should be noted that there is an opinion, developing into a practical tool in one country at least, which declares that $\$ 1000 per (expected) person rem averted is a suitable cost level to evaluate safety improvements. An integrated approach, also considering onsite costs, is given in Table 4 of this document [14].

ICRP 46 takes the view that, while such a figure might be a useful indicator, it should never be used in such a way that commonsense improvements are thereby not undertaken; that the need is rather to "optimize" by balancing overall effort (including cost) against the overall reduction in harm achievable, case by case.

In this area there is no real conflict of views, provided always that commonsense engineering judgment and safety practices rule the day rather than rigid cost guidelines and statistical analysis.
(iv) PSC at the plant level

Whereas some countries have no plans at present to develop PSC at the level of public health, there is general agreement about the usefulness of establishing PSC at the plant level. A number of examples of such proposals are specified in more detail in this report. Such PSC can be derived by propagating a PSC set on core melt (damage) probability to safety functions, systems and components. The other approach begins by setting PSC for safety functions and then proceeds to allocate them to systems and components. Of course, such PSC also imply a PSC for core melt. It is envisaged that the licensing and regulatory authority would be interested only in some fairly high level objectives (e.g. core-melt, safety functions, selected safety systems) and not in criteria at very low level. Such PSC at the plant level are a powerful design tool and have the advantage that it would be easier to demonstrate compliance, though it would also require complex modelling including human error and common mode failure.
2. PSC AT THE LEVEL OF PUBLIC HEALTH

Full scope Level 3 PSAs provide quantitative estimates of individual and societal risk from severe accidents. Based on such information a large variety of proposals has been made to establish PSC at this level. These proposals thus include limits, upper bounds, and objectives for individual risk, and objectives for societal risk. They are usually complemented by optimization criteria either general or using cost/benefit or cost-effectiveness techniques. The position of countries varies greatly. Some countries are using PSC at this level or are very close to a decision to do so. Other countries have no plans at present to establish such criteria.

2.1 Objectives

The list of objectives for nuclear power plants which are perceived for PSC at the level of public health include the following:

(i) To ensure that the public is not exposed to undue risk from nuclear power plants.

(ii) To express requirements in a form which may be used in the siting, design, construction, operation and regulation of nuclear power plants.

(iii) To ensure that disproportionate expense is not incurred in achieving incremental reduction of risk.

(iv) To enhance the public's understanding of the level of safety of nuclear power plants.

2.2 Health Effects

There are many different health effects that have to be considered. These are non-fatal cancers, fatal cancers of various types of different latent periods, serious genetic effects of many types occurring in the next two generations and thereafter, teratogenic effects, acute non-fatal effects and acute fatal effects.

For the purpose of establishing PSC these can be treated in several ways:

(a) All the effects can be kept separate and treated separately.

(b) One or more of the effects can be selected as most important (e.g. latent fatalities).

(c) Those stochastic effects (cancers and genetic effects) considered by ICRP to be equivalent can be combined, and non stochastic (early) effects treated separately.

(d) All the effects can be brought together into some common measure by use of weighting factors, which must be evaluated.

(e) The consideration can be left in terms of dose.
2.3 Individual Risk

In so far as individual risk objectives express the dividing line between a risk that is generally regarded as unacceptable and a risk that might be accepted, they must fundamentally be based on a judgment of society's view. It would not be in society's best interest to set such objectives either too high or too low, but there appears to be no objective means for deciding appropriate levels, since it is not a "scientific" question.

One way in which the view of society about risk can be deduced is by assessing the levels of individual risk inherent in existing practices and activities that are generally accepted. Care must be taken that the risks are of a similar nature, for example it is necessary to distinguish between voluntary and involuntary exposure to risk.

The approach used by ICRP is explained in the Appendix I. Other approaches can be found in the various national developments described in the body of the report. Any individual risk limit, upper bound or objective can be expressed in the following way:

a) probability of death (e.g. $10^{-6}$ per year) or health effect

b) "boundary" line for probability of exposure levels (see e.g. Fig. 6) [20]

c) histogramme for probability of exposure intervals (see e.g. Fig. 7) [17]

d) CCEH for exposure (see e.g. Fig. 8) [8]

![Fig. 6. Criterion curve.](image-url)
Fig. 7. Comparison of safety goals and 'natural' restrictions

Fig. 8. Proposed dose-frequency criterion in form of a CCFD.
To formulate a PSC for individual risk by setting an objective for a probability of death per year has the advantage to be easily comparable to well-known risks to which people are exposed and for which actual frequencies from statistics exist. It does, however, not distinguish between the contribution to that probability from the probability of having an accident and the probability of a given an exposure from that accident (for more details see [21]).

These two contributions to the total probability of death are kept separate if one of the other three approaches is followed. However, the boundary line approach, as discussed in the definition part above, cannot be integrated and thus does not give an objective for total individual risk. Thus, additional restrictions are necessary, e.g. in the form of a requirement to group all possible accident scenarios into a given number of categories. If the probability dimension of such a boundary line is specified to apply to a consequence interval it converts into a PDF. In this case restrictions are only required to limit the contribution from scenarios exceeding the "cut-off" point, i.e. the tail end (e.g. that total probability of accident scenarios leading to higher doses that the cut off value should be less than a given number).

The idea of categorization is followed by the histogram approach which restricts total individual risk in each defined consequence band. The CDF approach allows proper integration over the whole spectrum of doses. It should, however, be recognized that Fig. 8 is meant to only apply to latent effects. Additional objectives would be necessary for early death.

A more detailed description of these approaches is given in the body of this report.

2.4 Societal Risk

Societal risk is the set of probabilities and adverse consequences as it relates to society. The latter includes in particular social disruption as might be caused by accidents which result in a large number of immediate deaths at the same time in a small area (as opposed to e.g. car accidents which cause a large number of deaths per year, however, distributed during the year and over the whole country). It should be noted that, for a given exposure to radiation, also individual risk might increase with the total number of people involved, because of inadequate medical care and disturbance of infrastructure. [Societal risk also includes possible loss of housing, agricultural land and other property damage. This is usually treated separately and considered in cost-benefit analysis.] Thus it is clear that societal risk is not adequately represented by the sum of probabilities times consequences [22] (i.e. the mathematical expectation value of adverse consequences) but that additional restrictions are needed for low probability/high consequence accidents.

The following suggestions have been made:

a) The number of health effects per year representing the sum of the product of consequences and their probability of occurrence, with a weighting factor assigned to large immediate consequences. For work on the "value of a statistical life" see [23]. Sometimes, it has been suggested to scale such a number to a measure of the benefit provided by an industrial activity, e.g. the production of 1 GWa(e) [24].
b) The average risk to society within a given distance around the plant, e.g. the NRC societal goal for latent cancer effects [14]. Such an approach takes no account of the population density and therefore does not relate to the total consequences of accidents unless the population distribution is specified.

c) A graph showing either the probability of accidents of certain consequences, or the cumulative probability usually in form of CCDF of accidents which exceed certain consequences.

Graphical representation has the advantage that the distribution of risk over the spectrum of potential accident consequences is shown. The CCDF is often preferred [12]. The consequences of an accident are often expressed in terms of the number of early deaths as a surrogate for all consequences.

Fig. 9 gives three examples of such graphs in CCDF format [25,26,27] where one example includes a range where risks have to be as low as reasonably practicable [27]. Another example considering ranges for individual and societal risk is displayed in fig. 10 [15]. An individual risk of death larger than $10^{-6}$ per year is considered unacceptable, in the range from $10^{-6}$ to $10^{-8}$ per year risk reduction is desired, and below $10^{-8}$ individual risk is thought to be acceptable. The same principles are applied to derive PSC for societal risks. In order to account for risk aversion a slope of $-2$ was introduced on log-log scale. (It should be noted that often this graph representing societal risk is interpreted as a CCDF). The definition of such ranges explicitly specifies a "de minimis" value for individual and societal risk.

![Graph of INDIVIDUAL RISK and GROUP RISK](image1)

Fig. 9. Comparison of proposed collective safety goals.

![Graph of INDIVIDUAL RISK and GROUP RISK](image2)

Fig. 10. Safety criteria in the Netherlands.
For practical reasons, i.e. mainly because of the large uncertainties of consequence modelling at large distances and low doses, the population group considered for application of such criteria is usually limited in some way, for example by distance from the power station or by a cut off specified for individual doses or risks to be included in the sum total.

A risk aversion factor can be built into all of the three possible representations of PSC for societal risk.

ad a) A weighting factor (usually an exponential weighting factor, e.g. $C$) can be assigned to large consequences. Thus the weighted expectation value of consequences would be larger for an accident with a probability of $10^{-6}$ leading to 1000 deaths than with a probability of $10^{-4}$ leading to 10 deaths (in each case the unweighted expectation value would be $10^{-3}$ deaths per year). Such a weighting factor would be a function of the consequences. The problem of demonstrating compliance at very low probabilities is addressed in [28].

ad b) Lower average individual risk could be required for large consequence accidents. This approach needs specification of the population distribution and thus becomes very similar to a).

ad c) Risk aversion can be included by setting the slope of the curve (steeper than -1 on log-log scale).

Two possible methods for finding reference values for setting such criteria are:

- Arbitrary extrapolation from a fixed point such as the individual risk as given in Fig. 10; and
- Comparison with other risks to which society is exposed.

Much of the comment in the previous section on setting individual risk criteria is also relevant to these methods for setting societal risk criteria.

2.5 Parameters which may be needed for approaches to optimization

It is always possible to reduce a risk at additional expenses (however, not to zero). As a rule the marginal cost of risk reduction increase with the level of safety achieved [29]. Thus, if a risk is not unacceptable as determined by one of the previously discussed PSC, it has to be decided whether it is worth the effort to reduce the risk by an incremental amount. In the field of radiation protection any such decision aiding techniques are subsumed under the heading of optimization. Well-known approaches are differential cost-benefit analysis, cost-effectiveness analysis, multi-criteria analysis, etc.

When utilizing an optimization approach there are many factors to be considered in deciding whether to try for an incremental reduction in risk. It has been suggested [23] that this should also include the benefits generated by an activity. One approach would be to consider the offsite monetary impact on the public resulting from radiation (including contamination effects). This would include a variety of health effects, loss of use of land, lost jobs, relocation costs and similar matters. These direct costs could be ascertained only with some difficulty since one would have to take into consideration a wide spectrum of accidents and accident effects, and the specific demography associated with each site.

26
Another approach would be to establish a surrogate such as a set amount of money per person rem. In many cases, using person-rem will to a large degree describe the integral of the magnitude of the accidental release and the demography about the site. However, this is not a satisfactory measure when non-stochastic (i.e., acute) health effects are significant. A further problem in using a surrogate such as this is that it is very difficult to establish a specific monetary value/person-rem which will adequately represent the entire spectrum of effects from the aspect of total monetary impact on the public. Furthermore, the onsite costs are not covered by the person-rem surrogate even though the offsite costs may be adequately covered. One could argue that the onsite costs are borne by the utility and its owners and therefore are not a cost to the public. This is not the case in all countries. In some countries, a substantial portion of the onsite cleanup and replacement power costs is borne by the national or local government and the customers and not only by the nuclear industry. Where that is the case it may be appropriate to include averted onsite costs or some other factor in the optimization approach.

Application of money/person-rem could be viewed as either a good approach or a bad approach depending on one's outlook. Using a statistical value of so many person-rem equating to a fatality would place a monetary value on the averted death of a person. This approach is used in many aspects of society including court decisions for compensation of health damage (and has been applied in some contexts to the nuclear industry). However, it is not generally accepted to refer to averted deaths in monetary terms.

In summary, one must decide how much effort it is worth to reduce risk by an incremental amount. There are several approaches to accomplish this decision but none is perfect. They may include consideration of person-rem, offsite cost to the public, onsite cost or a combination of these or some other parameters appropriate to the specific situation facing the decision-maker. An integrated approach, which considers core melt probability, PSC for early and latent health effects, $1000 per person-rem as a surrogate for off-site impact, and on-site costs, is given in [14].

A further use of PSA in optimization is to identify the main contributions to risk and hence identify the most cost-effective ways of reducing risk. This is most significant in relation to Level 1 and Level 2 PSAs.

2.6 Compliance and Uncertainty

Uncertainties associated with the results of PSA work do exist. Depending on the specific component, system, sequence or event being analyzed, and the method used to conduct the analysis, the uncertainties may be large or small. When one performs a level 3 PSA, the uncertainties associated with the preceding level 1 and level 2 PSAs will be compounded and thus could result in substantial uncertainties in the level 3 PSA results. It should be noted that uncertainties of the same or larger magnitude are present in deterministic decision-making, and that uncertainties are not caused by and are not unique to performance of a PSA. Conduct of a PSA may allow one to reduce some uncertainties, more clearly identify those uncertainties that do exist, and provide a reasonable estimate of their cause and magnitude. This may be considered advantageous to the overall decision making process.

A limit implies a threshold which must not be exceeded. Compliance with limits implies that there is a good degree of precision in demonstrating that the limit is in fact being met. Unfortunately, the present state of the
art for PSA technique does not allow the development of a precise result. The uncertainty band is usually substantial, especially for Level 3 PSA results. Consequently, care must be exercised in establishing limits and, if a limit is established, it should normally take into account the uncertainty band. Because of this situation many countries have utilized the principle of PSC as objectives rather than limits.

Conduct of PSAs have resulted in the identification of areas of interest in the assessment of accident risks which are not readily quantifiable or for which quantititative data do not exist. For example, in the human factors area the response by plant operators to a situation are not readily quantifiable. One has to take into account such things as training, staffing level on shift, adequacy of procedures, and complexity of the operation when assigning the probability of the operator's correct response to the situation. Thus there is clearly a need for expert judgment in all areas of PSA conduct.

2.7 Concluding Remarks

While the interest and activity in the field of probabilistic safety assessments is very high there is to date very limited experience with the use of Level 3 PSA. In particular, the role of Level 3 PSA in the regulatory review and licensing domain has yet to be defined in most, if not all, countries. Given the common objectives of PSC it is not surprising to find a great number of common elements in the approaches being followed in various countries. Neither is it surprising that in this early phase there are significant differences in approach.

(i) Areas of Commonality

A common objective of most approaches is to put constraints on the mortality risk to an individual. While there is some variation in what is being proposed in various countries, the value is generally in the order of an incremental increase of risk of prompt fatality of $10^{-6}$ per year. However, it has to be clearly specified if any such value is to apply to the most exposed person or to an average individual within a given distance, if it is per site or per plant, etc. This is usually expressed as an objective rather than a limit. Indeed, a common feature of most approaches (except LORP 46) is that they do not propose a limit for either an individual or societal risk.

Underlying most proposals for PSC is the recognition that the approach to public safety should include a degree of optimization. This is hardly surprising since one of the objectives of PSC is to ensure that there is no disproportionate expenditure to reduce by a marginal amount the risk to individuals or society as a whole. In a practical sense this requires that designers identify those areas where improvements can be made which would result in a significant reduction in risk or alternatively those improvements which could result in a reduction in risk at a modest cost.

The activity in PSA in the nuclear field is not unique in our current industrial societies. Rather such methods are being applied in conventional industries also. Three examples are the Canvey Island study [30], the COVO study [31] and the recent initiative by the Government of the Netherlands to require a PSA for the most potentially hazardous installations [15]. In the last of these examples, the PSA should indicate individual risk as well as societal risk (early fatalities only). The outcome of these PSAs will be compared with existing PSC at the level of public health.
The disaster at Bhopal plus the escalating liability insurance premiums in many areas are expected to spur further effort to quantify, and where appropriate, reduce the risk from conventional industries.

(ii) Areas of Differences

A most evident difference in the approach to proposed PSC is the variation in the way in which these criteria are expressed. There are differences in the use of limit lines, histograms or CDFs and in calculating dose, early and latent effects, etc.

A second major difference is the degree to which Level 3 PSA's are being used in different countries. This ranges from full scope Level 3 PSA's in some countries, generic PSA's in others to no immediate plans in other countries. With this variation in use of PSA's there is a commensurate difference in the proposed use which will be made of PSC in the licensing processes. In at least one country firm acceptance criteria have been identified, in another the criteria are intended to be used as guidelines only while in a third no use is planned in the licensing process at this level.

(iii) Direction of further progress

Because it is expected that in the near future a more decisive light will be shed on the source term issue, most countries await these results before committing themselves to specific risk criteria to see if uncertainties can be reduced. Also other uncertain factors, like human factors, influence the attitude of some countries in these matters. Because of all kind of reasons a large number of countries are very cautious in adapting Level 3 PSC in the licensing process in one way or another. Although not averse to the concept of PSC at the level of public health, they lack confidence to some extent in these matters. Accordingly the results of further exploration and/or use in other countries are awaited.

A way to improve the quality of and the confidence in PSA's and PSC is to compare the existing analyses with operating experience.

To get a better understanding, further international consultation on PSA's and PSC is recommended. An international standard problem may be an approach to identify the differences and may help to get a better understanding, how to proceed. Also further exploration of the rationale behind the different approaches may be very helpful for this purpose.
3. PSC AT THE PLANT LEVEL

3.1. Introduction

The purpose of this chapter is to discuss how PSC can be set and implemented at the plant level. Two principal philosophical approaches are identified: one begins by setting criteria on core melt (damage) probability itself, which can be used along with PSC at the level of public health. These criteria, then, have to be propagated to safety functions, systems, and components. The other approach begins by setting criteria on safety functions and then proceeds to allocate them to systems and components. Of course, the implied criteria on core melt frequency can also be calculated. Both these approaches would be based on engineering judgment about adequate safety performance of a plant, eventually derived from a reference facility.

The allocation of PSC to systems and functions is not easy (some work has recently been reported in [32, 33, 34]). Furthermore, the need for allocation is mainly due to design requirements and not necessarily regulatory ones. In fact, it is envisaged that the licensing and regulatory authority would be interested only in some fairly high level criteria (e.g. core melt, safety functions, selected safety systems) and not in criteria at very low level. There is, of course, another philosophical approach that sees the licensing authority comparing with the licensee even at this detailed level.

Whenever criteria are set, the question of demonstrating compliance must be addressed. For probabilistic criteria, the capabilities and nature of the methods used to demonstrate compliance influences the decision making process. At the basic component level, statistical uncertainties of independent component failures are well understood. It must, however, be carefully respected, whether those data are of generic or of plant specific nature, and whether they can be applied in a given situation. As criteria are applied to successively higher levels, that is to systems, to system functions and to higher level quantities, ultimately to environmental impact, the complexity of the problem means that uncertainties not only increase but change in nature to include such difficult areas as human factors, common cause failures, completeness, and the special mathematical difficulties associated with including subjective as well as frequency-based probabilities. At higher levels, judgment plays an important part since empirical data is too scarce to tune the existing rather crude mathematical tools, and, furthermore, higher level mathematical tools for such situations are still in an early stage of development.

In the context of showing compliance with PSC at the plant-level it is important to precisely define what is meant by core-melt (or severe core damage) and by adequate performance of safety functions. Especially core-melt has been defined in different ways.

The LWR design criteria for the fuel temperature is sometimes used as a definition of core melt. However, the core melt does not occur at this temperature (whereas chemical reactions such as hydrogen generation may occur) and other definitions have been proposed.

From the licensees' point of view some countries accept higher temperature for a period of time. This could then be extended to a degraded core and further to a core damage. Different hazard states have been suggested [35] such as significant core damage which is defined as greater than 10% of the noble gas inventory leaking into primary coolant, and large
scale core melt could be when more than 30% of oxide fuel becomes molten. Core damage (core melt) characteristics and criteria are reactor type dependent.

The principle safety functions of a NPP are safe shut down of the reactor, coolability of the core, integrity of the primary system and the integrity of the containment.

3.2 Core melt criteria

One of the earlier proposals is that of the US NRC's Advisory Committee on Reactor Safeguards (ACRS)[35]. As shown on Table 2, there are three "hazard states" characterizing core damage. For each state there are a "frequency goal level" and an "upper limit". In addition, cost-effectiveness criteria are given, as shown in Table 3, which consider delayed cancer death, early death (weighted with an exponent of 1.2), and economic loss over the remaining lifetime (I) of the plant. Detailed explanations are given in the tables.

The USNRC has proposed criteria as displayed in Table 4 and reflects a philosophy of integrating core melt criteria with early and latent health effect criteria and cost-benefit guidelines. A detailed description can be found in the body of this report [14].

When comparing frequencies of core melt it is important to keep in mind the different concepts of defining the conditions which are postulated to lead to core melt. These conditions could, e.g., be defined as an unavailability for minimum numbers of safety system redundancies and intervention times as formally prescribed for license. Here, 'core melt' is a surrogate of exceeding minimal licensing requirements which should not be conceived as a physical plant state with severe core damages (e.g. see definitions of 'core melt' in [10]). Or these conditions could, e.g., be defined on the basis of unavailability of system function minima as derived by best-estimate calculations with or without additional consideration of not safety graded operational systems. Differences in these conditions will result in considerably different numerical values for the proposed core melt criteria.

A third approach uses a comparative concept by which the assessed core melt frequency is compared to that of a reference plant. A detailed description can be found in the body of this report [18].

Core melt, or equivalent accidents for designs like CANDU or HIGOR, are a natural "pinch point" in the progression of accidents. It would, therefore, appear reasonable to set criteria at that level having in mind plant performance. Furthermore, there is a consensus among PSA practitioners that the phenomena up to core damage are better understood than those present after core-melt (with the possible exception of human errors). Demonstration of compliance with such criteria would not be straightforward, because of the many uncertainties in the calculations.
### TABLE 2. LIMITS ON OCCURRENCE OF HAZARD STATES [35]

<table>
<thead>
<tr>
<th>Hazard State</th>
<th>Probability Goal</th>
<th>Decision Rules on Mean Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Goal Level</td>
</tr>
<tr>
<td>Significant Core Damage</td>
<td>Less than 1/100 per reactor lifetime</td>
<td>$f_{cd} &lt; 3 \times 10^{-4}$</td>
</tr>
<tr>
<td>(&gt; 10% of noble gas inventory leaking into primary coolant)</td>
<td></td>
<td>per reactor year</td>
</tr>
<tr>
<td>Large Scale Fuel Melt -LSFM</td>
<td>Less than 1/300 per reactor lifetime</td>
<td>$f_{m} &lt; 1 \times 10^{-4}$</td>
</tr>
<tr>
<td>(&gt; 30% of oxide fuel becoming molten)</td>
<td></td>
<td>per reactor year</td>
</tr>
<tr>
<td>Large Scale Uncontrolled Release from Containment given LSFM</td>
<td>Small, given a Large Scale Fuel Melt</td>
<td>$f_{R/m} &lt; 0.01$</td>
</tr>
<tr>
<td>(&gt; 10% of iodine inventory and 90% of noble gas)</td>
<td></td>
<td>per LSFM</td>
</tr>
</tbody>
</table>

$f_{cd}$ is the frequency of Significant Core Damage per reactor year.

$f_{m}$ is the frequency of Large Scale Fuel Melt per reactor year.

$f_{R/m}$ is the frequency of Large Scale Uncontrolled Release per Large Scale Fuel Melt.

The upper non-acceptable limits must be satisfied for extended operation of a new plant or for issuance of a construction permit. Between the upper limits and the goal levels is a discretionary range for case-by-case consideration of uncertainties and competing risk. Once the risk level decision rules have been applied, risk must still be reduced if such reduction is reasonably achievable within the cost-effectiveness criterion of Table 3.
<table>
<thead>
<tr>
<th>Expenditure Limits for Impact Reduction</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$ 1 million per delayed cancer death averted</td>
<td>$ 1 \times 10^6/(\Delta E_d L)</td>
</tr>
<tr>
<td>$ 5 million per early equivalent death averted</td>
<td>$ 5 \times 10^6/(\Delta E_{ed} L)</td>
</tr>
<tr>
<td>2 times the economic loss (due to resource damage) averted</td>
<td>$ 2/(\Delta E_r L)</td>
</tr>
</tbody>
</table>

A particular improvement is "cost-effective" and required if

\[
\text{Cost} \leq \left[2\Delta E_r + (\$ 5 \times 10^6) (\Delta E_{ed}) + (\$ 1 \times 10^6) (\Delta E_d)\right] L
\]

\(\Delta E_d\) is the change (due to the proposed improvements) in the expected value of:
\[
\sum_{\text{accidents}} \text{(Frequency)} \text{(Delayed Cancer Deaths)}
\]
and normal operation

\(\Delta E_{ed}\) is the change (due to the proposed improvements) in the expected value of:
\[
\sum_{\text{accidents}} \text{(Frequency)} \text{(Early Deaths)^1.2}
\]

\(\Delta E_r\) is the change (due to the proposed improvements) in the expected value of:
\[
\sum_{\text{accidents}} \text{(Frequency)} \text{(Economic Losses)}
\]

\(L\) is the remaining lifetime of the plant in units of \(10^{10}\) kWh to be generated and the frequencies are calculated per \(10^{10}\) kWh. This is the amount of electricity generated by a large (1200 MWe) plant operating at full capacity for one year.
### Table 4. Integrated Safety Coal Decision Matrix: Core Melt, Health Effects and Cost Benefit [14]*

<table>
<thead>
<tr>
<th>LARGE-SCALE CORE MELT FREQUENCY (PER RY)</th>
<th>HEALTH EFFECTS 90.1%/RY (EARLY/LATENT)</th>
<th>COST BENEFIT ($1,000/P-R + AVERTED ONSITE COST)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; $10^{-5}$</td>
<td>MEET BOTH DON'T MEET ONE</td>
<td>NO FIX FIX ($1,000/P-R$)</td>
</tr>
<tr>
<td>$10^{-4}$ - $10^{-5}$</td>
<td>MEET BOTH DON'T MEET ONE</td>
<td>FIX ($1,000/P-R + 10% AOSC$)</td>
</tr>
<tr>
<td>$10^{-3}$ - $10^{-4}$</td>
<td>MEET BOTH DON'T MEET ONE</td>
<td>FIX ($1,000/P-R + 100% AOSC$)</td>
</tr>
<tr>
<td>$&gt;10^{-3}$</td>
<td>MEET BOTH DON'T MEET ONE</td>
<td>FIX ($1,000/P-R + 100% AOSC$)</td>
</tr>
</tbody>
</table>

* All values are taken as mean values.

### 3.3 System Function Criteria

(i) Definition of (essential) System Functions

The functions that must be performed to control the potential hazard of a nuclear power plant given an initiating event are called (essential) 'system functions' in the following. Typically, these functions comprise a group of actions that prevent core damage and containment failure. They also keep radioactive releases within permissible limits. The actions may result from automatic or manual actuation of a system or a group of systems, from passive system performance, or from inherent feedback due to the physical characteristics of the plant.

System functions can be considered within a certain hierarchical framework. The most important functions are, e.g.:

- reactivity control
- core cooling control
- overpressure protection of the reactor-coolant system
- heat removal
- containment integrity
- coping with loss of (preferred) power

These essential functions form the basis for grouping accident-initiating events. They also provide the structure for defining and grouping specific actions for each class of initiating events. The last function has a general impact on all other functions. This function might thus be implicitly considered in the other functions. There are good reasons, however, to consider the emergency power case in an explicit way, too.

34
(ii) Objectives of PSC at the System Function level

The required system functions used to prevent accidents or to mitigate their consequences differ with the initiating events and postulated additional boundary conditions (e.g. such as LOCA combined with a loss of preferred AC-Power Supply). The number of postulated initiating events which influence the design of plant systems is, on the other hand, usually limited (in the order of 20). It is the objective of the System Function Criteria to define target values for the availability of those specific system functions which are required to cope with the different initiating events.

To ensure sufficient safety of a plant with respect to system function criteria the unreliability of the function in question should remain below a given target. Front-line systems and support systems, as well as the dependencies between systems and components affecting the reliability of the function in question would be included in demonstrating compliance. It should be clearly stated, whether operational systems (not safety graded) or operational control systems may be taken credit of.

The main justification for these criteria is:

- The System Function Criteria are sufficiently detailed to allow for a quantitative comparison of different plant designs.
- The System Function Criteria are sufficiently general to allow for different technical solutions meeting the same criterion, thus enabling the designer to choose the most appropriate one.
- The System Function Criteria reflect the state of the art in development of modern PSAs, they can therefore be calibrated by a meanwhile large variety of quantitative PSA-results.
- The System Function Criteria address items which are technically complex and which cannot be easily evaluated by other means. They will help to prevent misbalances of system designs.
- The System Function Criteria are effective for broad classes of accident sequences having thus an overall impact on nuclear safety.
- The System Function Criteria focus amongst others on two main principles in reactor safety technology, namely the 'defense-in-depth' and the avoidance of damages by putting emphasis on preventive means.

(iii) Principles for Deriving Numerical Objectives

Quantitative probabilistic safety criteria at the system function level are defined as limits on the unavailabilities of a given system function for given initiating events.

There are two ways to set numerical objectives for system functions. One method is to derive them by analyzing the maximum unavailability of system functions given a maximum value of core melt probability [32-34] or probability for doses from severe accidents received by a defined group of persons [17].
The other method is to derive numerical standards by comparison with results of existing PSAs of modern reactors, thus assuming that the status quo is acceptable and that the frequencies of initiating events are comparable.

For both methods, it is of great importance to clearly define the calculation bases for the system functions unavailabilities. This includes statements such as

- which set of reliability data for components have to be applied;
- which test and maintenance intervals have to be considered;
- whether operational systems (not safety graded systems) which fulfill the same function may be taken credit of (see Example 1 in Table 5);
- how operational control systems (systems limiting the exceeding of certain physical parameters such as power ramps, temperature ramps, etc.) may be taken credit of;
- how human interventions have to be quantified.

Examples of typical unavailabilities at the system function level which also demonstrate the influence of one of the above mentioned definition areas on the numerical values are given in Example 1 of Table 5 [36].

### Table 5: Examples of Probabilistic Safety Criteria at the Safety Function Level

<table>
<thead>
<tr>
<th>Example 1</th>
<th>System Function</th>
<th>System considered</th>
<th>Unavailability (mean)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Coping with small leaks in the primary circuit</td>
<td>Emergency cooling systems</td>
<td>$4 \times 10^{-3}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency cooling systems plus operational cooling systems</td>
<td>$3 \times 10^{-4}$</td>
</tr>
<tr>
<td></td>
<td>Coping with emergency power case</td>
<td>Emergency power systems</td>
<td>$2 \times 10^{-5}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency power plus operational backup systems</td>
<td>$5 \times 10^{-6}$</td>
</tr>
</tbody>
</table>

### Example 2

<table>
<thead>
<tr>
<th>Safety Function</th>
<th>Unreliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making the reactor subcritical</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td>Isolation of the containment</td>
<td>$10^{-3}$</td>
</tr>
<tr>
<td>Supply of feed-water when the off-site power or the main feed-water supply is lost</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>Operation of emergency core cooling in the case of a small reactor coolant leak</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>Rapid reactor pressure reduction and long-term pool cooling (BWR)</td>
<td>$10^{-4}$</td>
</tr>
</tbody>
</table>
Furthermore, it has to be defined how uncertainty bands are to be treated, so that not only point values will be used.

One of the possibilities is to use 95% confidence values. Other possibilities, such as defining point values for medians/means and allowed uncertainty bands are feasible. Standards for the most important system functions have been drafted by a licensing authority as given in Example 2 of Table 5.

Here a 95% confidence concept has been adopted. Further details can be found in the body of this report [37].

(iv) Comments

The required reliability of the system functions should depend on the frequency for which the function is demanded and on its safety significance.

Typically, a distinction is made between likely initiating events (which could happen up to several times a year) and unlikely events (with a frequency in the range of $10^{-3}$/year or less).

Given the unlikeliness of events such as severe transients (e.g. ALWS) or breaks of high quality coolant pipes (large LOCA) one arrives at the required limits on the unavailability of the necessary system functions with individual or interconnected safety systems, provided the safety systems are designed and maintained according to the present state of the art.

For more likely events, such as loss-of offsite-power or loss-of-main feedwater, the situation is different.

Unavailabilities well below $10^{-4}$ per demand can hardly be realized for individual active systems even with ample redundancy but without partial diversity. It is, furthermore, questionable whether such extremely low system-unavailabilities can be proven analytically or verified by operational experiences.

Thus, either operational systems or operational control systems have to intervene prior (and independently) to the actuation of safety systems, or at least two different safety systems have to be installed, coping independently with the accident sequence and performing the required system function.

For core coolability and decay heat removal a PSC of the order of $10^{-6}$/year (mean per event group) seems to be feasible for modern reactors [36]. This number refers to the unavailability of the system function 'core coolability and decay heat removal' multiplied by the cumulative occurrence frequency of the group of the initiating events.

3.4 Safety System Criteria

(i) Important Safety Systems

Safety systems in this context are engineering means of performing the required functions which are essential for the safety of the plant. They fall into two broad classes, e.g. the so-called front-line systems and the support systems. The boundaries of these systems are not very clearly defined, they also differ from plant to plant. The situation is further complicated by the
The relative importance of plant systems to risk is therefore highly dependent upon plant design, plant operation and site characteristics.

However, several systems have consistently been found important for all PWR plants of present design (in the US) [38]:

- Auxiliary feedwater system
- High pressure injection system
- Low-pressure recirculation system

For US BWR plants, less consistency was found, but some systems often appeared important:

- Power conversion system
- High pressure coolant injection system
- Reactor-core isolation coolant system
- Reactor-protection system
- Residual heat removal system

(ii) Objectives of PSC at the Safety System level

The objective of PSC at the system level is, amongst others, to limit the risk importance of specific systems providing guidance for, e.g.:

- reliability assurance
- operational limitations or requirements
- constraints on allowed outage times
- inspection and enforcement programs
- assessment of weak points in a single system on a comparative basis
- investigations of possible design alternatives

PSC at the system level turn out to be plant specific. They do not provide, in general, a basis for drawing broad generic conclusions.

Necessary prerequisites to establish PSC at the system level are:

(i) performing a plant specific PSA which considers the interactions of front line and support systems at the system function level as well as their demands with respect to the whole spectrum of relevant events and (ii) performing an importance analysis of selected systems and operating modes.

(iii) Discussion of Concepts

Concepts for applying probabilistic safety criteria at the safety system level, which have been used, include

(a) Assigning, based on experience and judgment PSC for major safety systems which are normally dormant, specifically the shutdown systems, the emergency coolant injection system and the active containment systems as well as probabilistic criteria on demands for such safety systems

(b) Deriving, from PSC for safety functions, reliability requirements for all systems contributing to the safety functions.
(c) Deriving, based on a PSC already assigned to an undesirable reactor state (e.g., severe core damage) criteria for major systems whose failure could contribute to the undesirable state.

(d) Assigning reliability requirements to an important safety system, not in a derivative way from a higher level PSC, but based on a more qualitative understanding of the safety importance of the system.

Since PSC for safety systems are generally derived from a higher level concern, they should always be considered in relation to that higher level concern.

Several quantitative methods have been proposed for ranking the relative risk importance of systems. However, there is yet no unique definition of relative importance.

Two kinds of importance measures have been used by several investigators:

- risk reduction worth: This is a measure for judging how the core damage frequency or system function unavailability would be reduced, if the reliability of a selected system was improved. This measure indicates, where system improvements are most appropriate with respect to core damage or safety function availability.

- risk achievement worth: It shows how the core damage frequency or system function unavailability would increase if a selected system were unavailable. This measure shows for which systems maintenance is most important in order not to let the plant deteriorate during its lifetime.

For both measures, the most significant effects are calculated if systems are considered which are involved in coping with many accident sequences.

The conclusions reached depend, however, on the kind of importance measure which is used.

(iv) Principles for Deriving Numerical Objectives

Means of deriving numerical directives for safety system criteria include:

(a) Deriving criteria based directly on public risk considerations.

(b) Deriving criteria for safety systems based on criteria which have already been established for safety functions. They have to be combined with other deterministic criteria to ensure a high level of independence among safety functions.

(c) PSC which have been developed for a safety system can be further allocated to a safety support system, for example, a service water system.

(d) Deriving safety system criteria in a comparative way. For example, if another plant or a group of plants have been assessed and accepted as safe, having an equivalent safety system with a
given reliability, then this system reliability can be assigned as a requirement for new plants.

Normally system reliability requirements lower than \(10^{-3}-10^{-4}\) failures/demand are not specified, as these are very stringent requirements for a single system, and within plant operation compliance cannot be demonstrated to a high level of confidence.

(v) Compliance

Compliance with safety system PSC can be shown by:

(a) Preparing in the design phase a reliability model of the safety system by fault tree analysis or other reliability techniques to show that the system has the capability, during operation, to meet the defined PSC. Such an analysis would typically include considerations of random component failures, component testing and maintenance, operator/maintainer errors, common cause effects and any effects of initiating events for which the system is designed to cater.

(b) In association with a reliability model for the system, periodical testing of the system to show that compliance is being maintained in operation testing of the complete system is the optimal means but, if not practical, overlapping tests of parts of the system are common.

(vi) Uncertainty

Uncertainty can appear in compliance activities in the design and operational phase due to the following reasons:

**Design Phase Compliance**

(a) Assumptions used to define system, component and human success/failure including those related to partial system failure.

(b) Omissions, or incorrect logic in system reliability modelling.

(c) Component and human failure data.

(d) Treatment of common cause failures.

**Operational Phase Compliance**

(a) Lack of the ability to test in the accident environment.

(b) Assumptions used to define success/failure of the test.

These uncertainties can contribute to both optimistic and pessimistic predictions of system reliability.

(vii) Comments

Setting of PSC at the system level has the benefit of stimulating reliability-related activities at the system level in the design phase, contributing to a thorough assessment of the design. This can contribute to achieving higher-level safety objectives when the total plant design is assessed.

40
It is recommended that system-level PSC be developed, where at all possible, in a rational, derivative manner from the basic safety concern of health effect.

The main problems with setting criteria at the system level are that success criteria for the system can vary with the nature of the initiating event (e.g., large LOCA, small LOCA) and that great care has to be taken in defining the boundaries of a system.

The most important area for future work is to investigate methods on how to show compliance in the light of uncertainties.

3.5 Safety Component Probabilistic Criteria

(i) Objectives

Components of safety systems have strict requirements for performance. These requirements are usually given in a deterministic way based on experience and engineering judgment and can be complemented by probabilistic criteria. Failure rates of components on demand or mean time to failure during mission are important parameters to determine the reliability of safety systems/functions.

The reliability of components is related to the design and also to the physical operating conditions such as pressure, temperature, neutron flux density and other operating conditions such as testing and maintenance.

Components may be active, e.g., pumps, motor operated valves, or passive, e.g., vessels, pipes, check valves.

Failure rates of components are based on statistical analysis of experience where available or an extrapolation of experience with similar or different equipment.

Such data form the basis of and are reported in the various PSA studies and include generic and plant specific data.

Thus derivation of probabilistic safety criteria for component is not that straightforward as it might look like, due to common mode failures and human errors, etc.

(ii) Comments

Because of the high quality requirements for components, criteria for the performance of safety functions/systems are usually achieved by systems design requirements, such as diversity and redundancy, rather than trying to further increase the reliability of components.
Probability

To analyze the likelihood of the events involved in PSA, it is necessary to express their probabilities of occurrence quantitatively. The term "probability" is usually defined in terms of the frequency of occurrence. In dealing with nuclear facilities, however, the conventional system for assigning probabilities rapidly breaks down as the frequency of possible events decreases, since little information exists to predict the actual probability. Low probability events will, therefore, often be assigned a value through "best estimates" or "engineering judgments". Such an approach, commonly referred to as "subjective probability", is an appropriate method to determine probabilities for use in nuclear safety analyses.

In subjective probability a number is assigned to the likelihood of an event occurring in a defined period of time, as a measure of the degree of belief that the event will actually occur during that time. It is important to distinguish between the degree of belief and the idea of confidence limits applicable to an estimate of probability, which itself has some associated uncertainty. The assignment can be made on the sole basis of subjective judgment, no statistical experience being needed. The result is conceptually identical to a traditional probability and can be used in the same way. The validity of this approach is dependent upon maintaining coherence when assigning probability values to events. Coherence simply means that all of the probabilities are assigned in compliance with the rules of the calculus of probability. These are that the assignment of probabilities is coherent only if the complement of an event with probability "p" is assigned a probability of (1-p), that events which occur with a greater frequency be given larger probabilities, and that if event A is more probable than B, and B is more probable than C, then A is more probable than C. Information is available in the literature of probability and statistics concerning the calculus of probability and the concept of coherence.

The use of subjective probability is acceptable as long as the quantitative value assigned through "best estimates" or "engineering judgments" is consistent with the quantitative value of the relative frequency in situations where more information is available. Thus, the probabilities assigned for various events will be consistent and continuous, and low probability events can be integrated with high probability events into a complete analysis of the options under consideration.

A distinction should be made between the probability of occurrence of an event at a nuclear facility, the probability that the event will have, as a consequence an unexpected release of radioactive materials into the environment, and the probability that an exposure will be received by an individual as a result of the release. The outcomes of these three probabilities are conceptually distinct, and care should be exercised in combining them.
Uncertainties

Any PSA is subject to uncertainty. Within the overall uncertainty of the assessment, several different classes of uncertainty will usually be present. These include not only the conventional uncertainties associated with an imperfect knowledge of the parameters used in the assessment and the appropriateness of the models, but also intrinsic uncertainties resulting from the statistical treatment of the variables, however certain they may be. Uncertainties due to an imperfect knowledge of events affecting the nuclear facility and release pathways are examples of conventional uncertainties, while the uncertainty in the expected outcome from low probability events is intrinsic. Whether the predicted impacts arise as a result of normal release mechanisms or from probable events, there will always be uncertainty in the estimated radiation impact, because present knowledge of conditions cannot be complete.

Other types of uncertainty will be associated with a lack of precision or knowledge about the many technical parameters involved in modelling radionuclide transport in the environment and in transfers through food chains, and air or water pathways, to man. To some extent, these uncertainties can be quantified within certain boundaries and propagated through the dose assessment to give an estimate of the uncertainty of the dose estimates. However, some aspects of the modelling may be dealt with only by making cautious, but reasonable, assumptions, particularly for the purpose of demonstrating compliance with individual-related requirements. The estimates of uncertainty, or of the distributions of parameters, will often be "subjective" in the same way as the probabilities.

Some events will have a large uncertainty associated with estimates of their probability. Events of low probability have an intrinsic uncertainty associated with the magnitude of their outcome. As a result, there will be a large uncertainty in the likely radiation impact. Therefore, estimates of the order of magnitude of probabilities and radiation impacts will often be the best that can be achieved.

Risk

The term "risk" is used with different connotations in various disciplines. Moreover, much has been written on the perception of risks, and some fairly complex mathematical definitions of risk, incorporating factors intended to reflect those perceptions, have been proposed. None of these complex definitions seems entirely appropriate, however, and all are difficult to describe and to use for quantitative risk comparison purposes. It is preferable that risk should be defined in a simple, objective and quantitative manner. This does not preclude subjective consideration of the separate components making up a risk, but such factors would only enter into decisions through further consideration of the overall acceptability of safety options or the optimization of safety rather than through limiting individual risks.

The term "risk" has been used in radiation protection to denote the probability of a serious detrimental health effect from a dose. To extend this definition to include probabilistic events, that risk should be defined as the probability that a serious detrimental health effect will occur in a potentially-exposed individual or his descendants. The risk, \( R \), to an individual or critical group from an event giving rise to a dose in the range from \( D \) to \( D+\Delta D \) is given by:

\[
R = P(D)P(\text{eff}/D)
\]
where \( P(D) \) is the probability of an initiating event, and other environmental changes, giving rise to a dose between \( D \) and \( D + dD \) to the individual representative of the critical group; and \( p(\text{eff}/D) \) is the probability of a serious detrimental health effect in that individual or his descendants from the resultant dose, \( D \).

For doses in the stochastic region, in which effective dose equivalent, \( H_E \), can be used, this expression simplifies to

\[
R = P(H_E) r H_E
\]

where \( r \) is the probability of a serious detrimental health effect per unit effective dose equivalent.

This is valid for small values of \( r H_E \); for large values it would have to be replaced by

\[
R = P(H_E) (1 - e^{-r H_E})
\]

For higher doses, the values of \( R \) will be larger than those calculated from the above expression, since there will be non-stochastic effects to be taken into account.

To find the total risk, the values of \( R \) must be summed over all possible events.

**Risk Limit**

The underlying basis for a risk limitation system is a judgment of the lower boundary of an implied range of risks to individuals deemed to be unacceptable; this judgment is based upon other types of risk that an individual can modify only to a small degree and that can be regulated by national authorities. Since significant doses might result from events that disrupt the normal behaviour of a nuclear facility and which have an assumed probability of occurrence, in a given time, less than one, the objective of protecting individuals can be achieved by an individual risk limitation requirement. By dealing consistently in terms of risk, both the probability of an exposure and the magnitude of the exposure can be included. To take account of this, a risk limit and risk upper bound can be established in direct analogy to the dose limits and upper bounds for normal releases. Such a risk limit should be consistent with the risk implied by the dose limits, such that the overall risk to an individual remains below the level considered unacceptable.

It would be possible to add the risk from routine to probabilistic situations and apply a risk limit to the sum. Alternatively, the two risks could be treated and limited separately. The former approach is simpler in concept, but is not necessarily more appropriate. The design and operational features that are intended to limit the two kinds of risk may be very different. Moreover, it is not self-evident that society would want to accept a small reduction in routine risks to compensate for an increase in the likelihood of an improbable, but serious event. After due consideration, the ICRP has recommended that its current dose limits should continue to apply to routine situations and that risks from probabilistic events should be limited on a similar basis. The Commission was aware of the existence of probabilistic events when it set the numerical value of the dose limit for routine situations, so that specification of a separate risk limit does not imply a need for a corresponding reduction in the dose limit.
exposure of members of the public very rarely approaches the dose limit and the lack of precision in predicting future situations does not warrant the refinement of modifying the dose limit to accommodate the risk limit.

The restriction of doses over a lifetime to 1mSv per year on average implies a constraint of the average annual risk to a level less than about \(10^{-5}\). In a similar manner, it seems reasonable to restrict the risk in a year to the critical group from probabilistic events so that it is also less than about \(10^{-5}\).

**Dose Upper Bound**

The total dose to the critical group will be composed of doses from the source being assessed, doses from other local sources, and doses from other regional and global sources. Also, overlapping doses from different sources to the same critical group are not restricted to any given instant in time. Releases of material during one year may cause doses in future years. The dose rate resulting from the combined effect of all such annual releases may, therefore, increase to some steady state or, if the releases stop at some time in the future, a maximum. The maximum value of the annual does could, therefore, occur far in the future and be maintained over considerable periods of time. To allow for dose contributions from present practices and to provide a margin for unforeseen future activities, the IAEA recommends that national authorities select a fraction of the dose limits as a source dose upper bound for each source of exposure, to ensure that the exposure of individuals will remain below the relevant dose limit.

**Risk Upper Bound**

In a manner similar to the establishment of the source dose upper bound, national authorities may select some fraction of the risk limit as a risk upper bound for the source being evaluated. A requirement of the assessment would then be that the sum of all risks from probabilistic events associated with a single source, which could expose the same critical group at any time, be less than the risk upper bound selected.

**Risk Limitation Technique: Limit lines**

To use a system of limitation on annual individual risk requires that the probability of exposure at or above various levels of annual dose should be assessed. It is important in doing this that a distinction be made between the probability of exposure and the probability of events which may give rise to exposures. The link between these parameters involves the distribution over time of the radiation impact associated with the events.

The basic requirement for compliance with the risk limit or a risk upper bound is that \(P(\text{event}|l)\) is less than the appropriate limit. This overall condition is simple but the derivation and comparison can be more complex as some of the conditional doses are in the non stochastic region.

One procedure for applying individual-related requirements to probabilistic events is to express these limits in a criterion curve. The so called limit line or criterion curve is an indifference line that separate unacceptables from possibly acceptable from possibly acceptable regions in the frequency-consequence space. It is a line of constant expected impact. Such a criterion curve, of the maximum probability that can be permitted for an estimated annual dose from all initiating events, based upon the annual risk constraint of \(10^{-5}\) to the critical group, is shown in figure A1.
The relevant features of the criterion curve are as follows: a probability limit of one for annual doses up to 1 mSv; an inverse proportionality region; a non-proportional region for the dose range in which non-stochastic effects may also occur; and a constant probability for doses that are lethal.

In the lethal dose range, the probability is constant irrespective of dose, because the consequence to the individual is the same regardless of the dose received. For the range of doses in which only stochastic effects occur, the relationship between probability and dose is inversely linear, with values representing the product of the probability of the dose, the annual dose and the probability of a health effect per unit dose. Finally, in the dose range where non-stochastic effects may occur, i.e., individual doses exceeding a few sievert, the shape of the criterion curve is non-linear, in order to take into account the increasing probability of death. This portion of the curve should approximate a sigmoid relationship and would depend to some extent on the time over which the dose is delivered. This could be taken into account, if relevant, for a particular scenario.

The risk upper bound can be incorporated directly into the criterion curve. The apportionment between different sources, necessary to develop the upper bound, requires that some fraction of the limit be selected for the source under consideration. Such a fraction could be incorporated as shown in figure A2. The magnitude of the change in the criterion curve will be dependent upon the fraction selected for the upper bound. The shape of the curve will be altered, since the onset of non-stochastic events occurs in a rather narrow range of doses.

Fig. A1. Criterion curve corresponding to an annual risk constraint of \(10^{-5}\) from all events.

Fig. A2. Criterion curve illustrating the type of change necessary to correspond to a risk upper bound.
Decision-making Techniques

The safety decision-making process consists in principle of an evaluation of all alternative options of safety taking account of each of the components influencing safety efforts and achieved gains. This evaluation is related to stated or implicit preference criteria. Several methods can be used for decision making. Some methods are limited to comparisons between options. For example, "multicriteria methods" compare by pairs the various options taking into account all the criteria, to determine whether one option is better than the other, iterating the process to the final decision. In these methods, one option is considered better than another if the number of criteria for which it is better is sufficient, and if for the remaining criteria the differences are not excessive. These two conditions involve the use of some relative assignment of weight to the criteria. Multicriteria methods usually allow the preselection of the better options, but do not generally lead to a complete ranking. The value of these methods is that they take account of many criteria and provide a simple procedure for dealing with qualitative aspects.

Other methods called "aggregative methods", instead of comparing the different options in pairs, attempt to combine the values of the criteria in each option into a single value, ranking the results for the different options in order to select the best. An inherent requirement of these methods is an adequate quantification of the various criteria. The most widely used aggregative methods are based on utility functions to quantify the different criteria. A utility function is a scale expressing the possible values of one criterion by numbers (called utilities) lying between 0 and 1, assigned in such a way that, if one outcome is preferable to another, the utility of the first is greater than that of the second.

Utility functions are not necessarily linear, and have no other foundation than the preferences of the decision maker regarding a given criterion. The decision is based on the total utility of each option, obtained by combination of the several utilities involved. Account is taken of the relative importance of the various criteria by assigning a weight to each. The best option is the one that maximizes total utility.

An important, but by no means exclusive, method based on utility functions is the special case of "cost-benefit analysis". This procedure assumes that all the criteria involved can be expressed in monetary terms and that utilities are linearly related to such monetarized criteria. In cost-benefit analysis, the weighting of the different criteria is the monetary value of the unit characterizing the criterion.

A word of caution is necessary regarding these quantitative methods of decision making. The optimality of the selected level of safety and of the systems used to achieve it, depends heavily upon the quality of the judgments and data which went into the analysis. It is therefore necessary to evaluate the sensitivity of the solution to variations in some or all of the judgmental inputs and data. Such sensitivity assessment allows the identification of the crucial factors in the decision and helps in making the approach more meaningful, particularly when the problem is complex.

The procedure for obtaining the solution of safety optimization problems has led to the use of the term "differential cost-benefit analysis" to refer to optimization procedures. The level of safety is such that a marginal increase in safety efforts is exactly balanced by a marginal reduction in risk and detriment gains.
On the other hand, decision making procedures based on "cost-effectiveness analyses" are simpler and should not be mistaken for optimization methods based on cost-benefit analysis. They prevent the variables from floating independently and could only be used to determine the most effective safety obtainable from fixed resources or, alternatively, the cheapest safety for a given level of risk.

REFERENCES


[4] "Interface questions in Nuclear Health and Safety, NHA/0(F)5, 1985"


[23] Siddall, E., Nucleonics, 17 (1959), 64.


[27] Higson, D.J., "Some questions on the development of probabilistic safety criteria", these Proceedings.


[37] Virolainen, R., "Use of reliability and risk standards as bases for acceptance in licensing and regulation of nuclear power plants", these Proceedings.
PAPERS PRESENTED AT THE MEETING
AN INTEGRATED SAFETY GOAL CONCEPT

J.H. Sniezek
United States Nuclear Regulatory Commission,
Washington, D.C.,
United States of America

Abstract

In early 1983, the U.S. Nuclear Regulatory Commission published a safety goal policy to set forth its views on what constitutes an acceptable level of safety for the operation of commercial nuclear power reactors in the United States (NUREG-0880). The safety goal was to be evaluated over a 2-year period. The evaluation period ended in April 1985. An important conclusion was that adoption of a safety goal policy would be useful in providing a yardstick for the NRC to use in conducting its regulatory safety decision process. It is expected that such a policy would add more objectivity and predictability to the safety decision process. The NRC staff conducting the evaluation concluded that the basic structure of the provisional safety goals was sound and not in need of radical revisions. As expected, several controversial issues were identified during the evaluation. These primarily involved the extent to which NRC should require safety improvements that (1) would primarily reduce the overall frequency of severe core-damage/core-melt accidents (independent of the severity of offsite health risks) and (2) would serve to benefit the plant owners by averting the onsite economic costs of such accidents. To help resolve these issues, the NRC staff is considering an approach that would integrate the three principal safety goal decision elements (i.e., the core-melt frequency, public mortality risks and the benefit-cost algorithm). Use of this integrated approach in implementing the final policy on safety goals is now under active discussion. Conceptually, this integrated approach would be viewed by itself as the safety goal. This approach would place a monetary ceiling on the overall costs for reactor safety improvements required of a licensee provided an undue risk to public health and safety does not exist. Once this cost for safety improvements has been expended, the safety goal is achieved. This approach would also allow considerable latitude for a plant owner to choose the more cost-effective safety improvements that may also be desirable from the standpoint of overall plant availability. On the other hand, there is a penalty imposed if the plant safety level decreases. A commensurately higher monetary ceiling would be applied to those plants that exhibit because of either design or operation, a higher than normally expected level for the core-melt frequency. A monetary incentive would thus exist for plant owners to promote safety in plant design and operations. The principal conclusions reached during the safety goal policy evaluation, the integrated safety goal concept and the prospective implementation of a safety goal policy in the U.S. are described in detail in the paper. It is anticipated that the Commission will decide on these matters and the final safety goal policy statement during 1986.
Introduction and Background

On March 14, 1983, the U. S. Nuclear Regulatory Commission published a Safety Goal Policy Statement (48 FR 10772) and in May 1983 it was issued as NUREG-0880, Revision 1. The safety goals were qualitative in nature and addressed both individual risk and societal risk (Figure 1). The Commission also established three quantitative objectives and a benefit-cost guideline as a basis for determining whether the qualitative goals were being met (Figure 2).

QUALITATIVE SAFETY GOALS

- **INDIVIDUAL RISK GOAL** - Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

- **SOCIETAL RISK GOAL** - Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

Although the Commission believed that the current regulatory process provided for adequate protection of public health and safety, it concluded that a safety goal could lead to more effective and consistent regulation of nuclear power plants, a more predictable regulatory process, a better public understanding of the NRC regulatory criteria and increased public confidence in the safety of operating plants. The statement of NRC safety goal policy was to express the Commission's views on the acceptable level of risks to public health and safety and on the safety-cost tradeoffs in regulatory decisionmaking.

The objective of the Commission's policy statement was to establish goals which limit to an acceptable level the radiological risk which might be imposed on the public as a result of nuclear power plant operation. While the policy statement included the risks of normal operation, as well as accidents, the Commission believes that risks from routine emissions are small and therefore they do not need to be routinely analyzed on a case-by-case basis in order to demonstrate conformance with the safety goals.

The Commission undertook a 2-year evaluation to assess the effectiveness of the safety goals and design objectives, and to develop information and understanding as to how to further refine and use the design objectives and the cost-benefit guidelines. It was expected that the qualitative safety goals and quantitative design objectives might be changed as a result of the experience.
INDIVIDUAL MORTALITY RISK - 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 ONE-TENTH OF ONE PERCENT (0.1%) OF THE SUM OF PROMPT FATALITY RISKS RESULTING FROM OTHER ACCIDENTS TO WHICH MEMBERS OF THE U.S. POPULATION ARE GENERALLY EXPOSED.

SOCIETAL MORTALITY RISK - 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 ONE-TENTH OF ONE PERCENT (0.1%) OF THE SUM OF CANCER FATALITY RISKS RESULTING FROM ALL OTHER CAUSES.

PLANT PERFORMANCE DESIGN OBJECTIVE - THE LIKELIHOOD OF A NUCLEAR REACTOR ACCIDENT THAT RESULTS IN A LARGE-SCALE CORE MELT SHOULD NORMALLY BE LESS THAN ONE IN 10,000 PER YEAR OF REACTOR OPERATION ($10^{-4}$/REACTOR-YEAR).

BENEFIT-COST GUIDELINE - THE BENEFITS OF AN INCREMENTAL REDUCTION OF SOCIETAL MORTALITY RISKS SHOULD BE COMPARED WITH THE ASSOCIATED COSTS ON THE BASIS OF $1,000 PER PERSON-REM AVERTED.

FIG. 2. Quantitative objectives.

gained during the evaluation period. The NRC staff framed three major questions to be addressed during the safety goal evaluation period:

- To What Extent Is It Practical to Use Safety Goals in the Regulatory Process?

- Should the Quantitative Design Objectives Be Modified or Supplemented? If So, How?

- How Should the Safety Goals Be Implemented at the End of the Evaluation Period?

In order to test the viability of safety goals, the staff examined analyses of the results of probabilistic risk analyses (PRA) conducted on sixteen (16) nuclear power plants. It retrospectively examined several regulatory safety issues which had been resolved without the benefit of safety goals as a guide to aid in the decision process. It was also necessary to perform a number of sensitivities studies and evaluate the level of PRA development to determine how PRA should be used in the regulatory process at its current stage of development. The staff concluded its evaluation of the safety goals in April 1985. The report of its findings (known internally as the Safety Goal Steering
Group Report) has since been under active review by NRC senior management and the Advisory Committee on Reactor Safeguards (ACRS). I will now provide an overview on the major findings and conclusions resulting from the 2-year safety goal evaluation, the remaining open issues and the NRC staff's new concept of an integrated safety goal decision matrix.

The 2-Year Safety Goal Evaluation Program and Steering Group Report

The Commission recognized that a basic impediment to adopting and implementing safety goals and quantitative design objectives was that the PRA techniques for developing quantitative risk and core-melt estimates are complex and have substantial associated uncertainties. This raised the question whether the achievement of a quantitative core-melt frequency or risk goal could be verified with a sufficient degree of confidence for use in the regulatory process. Thus, one of the major tasks during the evaluation was to prepare a description of the state-of-the-art of PRA, its strengths and weaknesses, and insights regarding the risk of nuclear power plants as identified in existing PRAs. The product of this task is the PRA Reference Document (NUREG-1050). It received extensive peer review by PRA experts from all segments of U.S. industry and academia. NUREG-1050 sets forth the NRC staff's consensus on the state of the art of PRA today and on the feasibility of PRA as a regulatory tool.

Other major tasks included:

- assessment of the quantitative design objectives to determine their sensitivity to the uncertainties inherent in their parameters,
- trial use of the quantitative design objectives to evaluate recently established Commission requirements to determine whether the regulatory decision might have been altered by consideration of the safety goal,
- assessment of alternatives to the quantitative design objectives, and
- a scheme for use of the safety goal in the various aspects of the regulatory process, including resolution of generic safety issues, establishing research priorities and establishing licensing and inspection criteria.

Discussion of Steering Group Conclusions

The Steering Group arrived at the following general conclusions at the end of the evaluation period.

1. The use of safety goals can strengthen decisionmaking by adding more objectivity and predictability to the regulatory process. The safety goals will be valuable as a regulatory yardstick against which a wide range of regulatory issues can be measured.

2. The basic structure of the safety goals is sound, and they are not in need of radical revision.

3. The core-melt guideline should be given nearly as much weight as the individual and societal mortality risk design objectives in order to enhance the defense-in-depth safety philosophy and to be more useful as a screening criterion in determining whether to conduct analyses to establish whether or not the individual and societal mortality risk objectives are met.

4. PRA and safety goals should not be used within a framework of strict acceptance or nonacceptance criteria for regulatory decisions. Consistent with this conclusion, the Commission should consider adopting a policy statement rather than a regulation.
5. The staff expects to make substantial use of safety goal comparisons to augment, but not replace, traditional safety review methods for making regulatory decisions.

The most significant change proposed by the Steering Group was that, in addition to person-rem considerations, the averted onsite radiological costs, including economic costs, should be considered as a benefit in the benefit-cost guideline. The ACRS raised this issue and the Commission solicited public comment on it in NUREG-0880. Industry comments were generally opposed to inclusion of averted plant damage costs. They argued that it is not a health and safety factor, and thus is outside the purview of the statutory health and safety responsibilities of the Commission. The Steering Group considered these arguments but did not agree. Based on consideration of TMI-2 accident financial costs and the inability of the $1,000 per person-rem guideline to encompass the spectrum of costs to the public from severe core-damage/core-melt accidents, a change was judged to be necessary. The basis for including averted plant damage costs as a benefit is probably the most controversial safety goal issue currently being debated within the Commission. No other major changes were recommended by the Steering Group to either the qualitative safety goals or the quantitative design objectives published by the Commission in early 1983 (NUREG-0880, Rev. 1). However, for purposes of applying the design objectives for offsite mortality risks, the Steering Group recommended several calculational changes intended to stabilize the use of the safety goals and provide a more representative estimate of the average mortality risks to individuals in the vicinity of the plant.

For purposes of calculating the individual risk of prompt fatality, the Steering Group proposed that if no individuals resided within 1 mile of the plant boundary, then one should be assumed to reside at 1 mile. This was to preclude the need for additional calculations if the population characteristics near the plant were to change in the future. The Steering Group also proposed to decrease from 50 miles to 10 miles the distance used for calculating the risk of delayed cancer fatalities. This would more suitably represent the population potentially at higher risk from severe accident releases. Lesser calculational distances were also considered for purposes of comparing against the national cancer fatality statistics applicable to average individuals in the plant vicinity. The 10-mile distance was finally judged to reasonably comport with the bulk of the potentially significant accident exposures and provide a good perspective on societal risk.

An Overview of Evaluation Results

A large number of sensitivity studies were performed during the 2-year safety goal evaluation period to test the impact of changes in assumptions on the public health effects calculations. Figures 3 and 4 illustrate the results these efforts. Figure 5 indicates the parameters for the base case and figure 6 indicates the significant parameter variations evaluated in the sensitivity study. Additionally, the distribution of potential mortality outcomes for the existing U.S. sites was examined assuming very large and severe accident release magnitudes. Figures 7 and 8 illustrate these results. This data helped the Steering Group conclude that aggregate numerical goals to constrain the potential number of mortalities were not needed to assure adequate societal protection as some had suggested during evolution of the safety goals.

Although results are not yet conclusive, it is also useful to note that preliminary indications from the U.S. source term research work seem to indicate that the magnitude of potential early fatalities relative to Figure 7 (SSTI) could drop considerably. The Steering Group also found that the prompt offsite fatality risk design objective generally is more limiting than the design objective for delayed cancer fatality by nearly an order of magnitude for distances less than about 2 miles from the plant site boundary.
FIG 3 Safety goal design objective sensitivity calculations

1 Based on averaging within 1 mile of the boundary or on 1 mile radius from nearest person per NUREG-0880 (Rev 11). Refer to Table of Reference Case Assumptions.

EARLY FATALITY RISK (Per Reactor Year)
PARAMETER VARIATIONS

Source Term
1/2 Particulates and Iodine
1/10 Particulates and Iodine
1/100 Particulates and Iodine
Noble Gases Release Only

Power Level
1/2 Actual Power Level
1/20 Actual Power Level

Containment Failure
All SST1 Releases
No SST1 Releases

Heat of Release
Medium Heat in Releases
High Heat in Releases

Emergency Response
Evacuation, 1 hr., 10 mph
Evacuation, 3 hr., 10 mph
Evacuation, 5 hr., 1 mph
Summary Evacuation
Sheltering
No Response

Site Population
Palo Verde Site
Palo Verde Site

Health Response Models
Parasmatic Models
Optimistic Models

Meteorological Data
Palo Verde Meteorology
Miami Meteorology

Interdiction Criterion
Interdiction Criterion 500/30 years
Interdiction Criterion 5A/30 years

LATENT CANCER FATALITY RISK$^1$ (Per Reactor Year)

$^1$ Total person-rem to population within 50 miles of plant
$^2$ Refer to Table of Reference Case Assumptions

FIG. 4 Safety goal design objective sensitivity calculations: cancer fatality risk
1. Source Term: SST-1, -2, and -3 (NUREG-0773)
2. Power Level: 1120 MWe
3. Containment Failure Probability: Release probabilities for SST-1, -2, and -3 = 1, 2, and $7 \times 10^{-5}$ per reactor year, respectively
4. Heat of Release: None
5. Emergency Response: Summary evacuation within 10 miles of site
6. Site Population: Indian Point
7. Health Response Models
   a. Prompt: Bone marrow dose response for mortality with supportive medical treatment (e.g., LD 50/60 = 520 rads)
   b. Latent: Central estimate (Reactor Safety Study) for number of latent cancer fatalities induced by radiation, approximating the linear-quadratic-model
8. Meteorological Data: New York City
9. Interdiction Criteria: 25 R/30 years

All SST-1 Releases = SST-1 = $1 \times 10^{-4}$ per reactor year
No SST-1 Releases = SST-2 = $3 \times 10^{-3}$ per reactor year
SST-3 = $7 \times 10^{-5}$ per reactor year

Medium Heat in Releases = $170 \times 10^6$ BTU/h
High Heat in Releases = $430 \times 10^6$ BTU/h

Pessimistic Health Model
   a. Prompt: Bone marrow dose response curve for mortality in 60 days with minimal medical treatment (LD 50/60 = 340 rads)
   b. Latent: Linear, no threshold model

Optimistic Health Model
   a. Prompt: Bone marrow dose response curve for mortality in 60 days with heroic medical treatment (LD 50/60 = 1,050 rads)
   b. Latent: Curvilinear model

FIG. 5. Sensitivity study reference case assumptions.
FIG. 6. Sensitivity study parameter variations.
Fig. 7. Histogram of mean early fatalities for 91 sites.

Fig. 8. Histogram of mean number of latent cancer fatalities for existing sites.
This finding is of course predicated on source term releases more severe than are currently indicated from the new source term work and thus could change. The relative importance of the risk of delayed cancer fatalities could increase. In any event, projections of the delayed cancer fatality risk fall far below the safety goal design objectives for all U.S. reactor sites (Figure 9). Figure 10 shows the relationship of the mortality risks versus distance and the severe accident (SST-1) probabilities that would need to be reached in order to exceed the safety goal objectives for both prompt fatalities and latent cancer fatalities.

![Graph of Latent Cancer Fatality Risk](image)

**FIG. 9.** Latent cancer fatality risk versus distance.

![Graph of Risk and Probability of SST-1](image)

**FIG. 10.** Risk and probability of SST-1 versus distance to nearest person (uniform population distribution).

**Implementation**

1. **General Strategy and Areas of Use**

   It was concluded during the evaluation period that there should be a phased implementation of the safety goals into the regulatory process and the staff could promptly begin use in certain areas, such as in the evaluation of new generic safety requirements. In other areas, such as setting priorities for use of staff resources for sifting through and assessing risk significance of existing regulations, a more gradual implementation was foreseen. Ten regulatory areas were cited as examples where safety goals will be used. Although not detailed here, these...
generally applied to generic issues, plant-specific issues and to the
setting of regulatory priorities for the NRC research and reactor
inspection programs.

2. General Ground Rules for Implementation

For implementing the safety goals, there are some general ground rules
which the NRC staff would expect to use. These will be subject to
revision as additional experience is gained.

a. For those areas of regulation where the staff uses safety goals, the
safety goals will be used in conjunction with traditional safety
review methods for making regulatory decisions. Nuclear power plant
licensees will still be expected to meet NRC's regulations; however,
they may be able to use the safety goals as a basis for requesting an
exemption from certain requirements.

b. In using the results of PRAs, the staff will ensure that each PRA
receives a peer review and will address and allow for estimated
uncertainties by using judgment in applying the results to regulatory
decisionmaking. The staff expects to use mean values for imple-
menting the safety goals. To the extent uncertainties and the mean,
median and confidence range values can be addressed in the use of
results of PRAs, they will displayed. The staff will also remain
mindful that PRA results found to be initially acceptable from the
standpoint of the state-of-the-art and from peer review may either
improve or deteriorate depending on the overall quality and per-
formance of plant personnel and operations (e.g., testing, mainten-
ance, management practices).

c. The use of PRA results and safety goals will not diminish the
continued importance of the defense-in-depth safety philosophy or the
traditional safety review methods used by the staff in making
regulatory decisions, nor will they diminish NRC diligence in
assuring licensee management attention to safe construction and
operation of nuclear power plants.

d. The staff will not require a plant-specific PRA for the sole purpose
of safety goal evaluations. For plants where a PRA exists or
reasonable judgments can be drawn from surrogate PRAs, the safety
goals will be used as one factor in considering plant-specific issues
such as licensee exemption requests, backfits, and schedules for
implementation of backfits. The use of safety goals and PRA is
unlikely to replace the normal methods for reviewing licensing
exemption requests or backfits, but the safety goals will be used by
the staff as authoritative guidance in arriving at a regulatory
decision.

e. Safety goals will not be used for staff evaluations of security and
sabotage issues because there is presently no method for
quantitatively estimating the risk of the threat. Safety goals will
apply to accidents resulting from internally initiated events and
externally initiated events. The staff will be particularly
cognizant of the large uncertainties that are involved in describ-
ing the plant core-melt risk from external events and will ensure that
the uncertainties do not mask the risk of other important potential
core-melt initiators.

f. In conducting benefit-cost analyses, the staff will include the cost
of occupational exposures incurred as a result of implementing the
proposed requirement, as well as the benefit due to occupational
exposures averted as a result of accident risk reduction. Both will

65
be evaluated on the basis of $1,000 per person-rem. In addition, the staff will include averted on-site cost commensurate with the core melt and mortality risks.

g. In using safety goals with matters such as generic issues involving particular accident sequences (where apportionment and fractional allocations of the safety goals may be at question) the staff will strive toward a balanced contribution from such sequences.

h. With respect to the probability of a large scale core-melt accident, the staff will strive for and encourage an improved level of safety for the future plants and standardized plant designs. The lessons acquired by operational experience and PRA results will be carefully considered in striving toward achieving these safety improvements in a cost-effective way.

Integrated Safety Goal Concept

Subsequent to completion of the Steering Group Report, a number of open issues were identified during the NRC management and ACRS reviews. The more difficult and controversial issues centered around the core-melt frequencies and cost-benefit guideline. The thrust of comments generated on these issues are discussed below:

1. The Steering Group posture of accepting a median frequency of $10^{-4}$ per reactor year over a large population of existing and future plants generated considerable comment centering around the issue of whether or not NRC should establish goals that call for overall improvements in the core-melt frequency. Alternative approaches to guide design of future plants and new standardized designs toward increased safety were expressed as being necessary.

2. The recommended use of median as opposed to mean values was viewed as unacceptable by a number of reviewers and the ACRS. The staff has concluded that mean values should be used in computing core-melt probabilities and mortality risks.

3. The continued display of all important averted onsite costs was viewed by some as an acceptable practice consistent with the existing backfit rule and the existing staff guidelines for conduct of benefit-cost analyses. The degree of decision weight, if any, to be given to the averted onsite costs in making regulatory safety decisions remains a central issue. As the trial evaluations conducted by the Steering Group revealed, most of the generic safety decisions made by the staff are unlikely to have been significantly altered by taking either side of this issue.

To aid in the final resolution of these comments and open issues, an integrated core-melt probability, health effects, and benefit-cost concept has been proposed (Figure 11). This matrix reflects a quantitative and integrated interpretation of the Commission qualitative safety goals as these are currently described in NUREG 0880, Revision 1. The matrix is a template for the staff to use in implementing the Commission's final policy on qualitative safety goals.

Some of the essential features of this integrated approach are as follows:

- Consistent with the Commission's traditional defense-in-depth and accident prevention philosophy and safety practice, a heightened focus is being given to the frequency of large scale core-melt accidents and an emphasis on safety improvements is clear when high-frequency core-melt accidents are projected. For example, if the core-melt probability is $> 10^{-5}$/RY and a health effect goal is not met, the cause must be fixed regardless of cost.
A sliding scale on benefits and incentives is set forth to emphasize that improvements will be sought where indicated as necessary for existing plants. The top of the matrix is intended to set forth goals sought for future plants and standardized designs (core melt < 10^-3/RY and both health effects goals met). It is expected that they will have to meet this goal. In essence, the top of the matrix reflects a deminimus risk level for severe accidents, below which no further regulatory safety improvements in plant design and operation would be necessary.

An ALARA approach is embodied in this matrix. It is intended to emphasize by application of 100 percent of the averted onsite cost, that the quantitative mortality risk objectives should be achieved by the plant design and operation; yet it yields a degree of flexibility to the staff to reach decisions on whether risk reduction can be best achieved through improvements in the overall core-melt frequency, by reducing the probability of one or more of the dominant core-melt sequences or by further safety improvements in the prevention or mitigation systems. This approach is consistent with the traditional NRC approach adopted for the risks associated with routine plant operations.

The matrix defines a cost ceiling to be associated with a projected state of risk from a reactor plant. Depending on this state of risk, cost-effective safety improvements would continue to be made. Once the safety improvement costs exceed the defined ceiling, the safety goals are considered to be met. It is expected that in the absence of a plant-specific PRA to define the state of risk, surrogate PRAs of similar designs will be used by the staff, including, where considered helpful, accident precursor projections from actual operating experience.

In summary, the matrix can impose large costs (e.g., many tens and even hundreds of millions of dollars) for safety improvements where the projected risk state involves a high core-melt frequency and failure to achieve a mortality risk objective. In these situations it is considered to be in the public interest to restore the plant to a risk state where an adequate level of protection to the public health and safety is reasonably assured. The lower part of the matrix reflects that the dollar costs of safety improvements are not an important factor where the public health and safety cannot be reasonably assured by the NRC.
It should be noted that the matrix creates a need for an improved integral treatment of the generic and plant-specific safety improvements being required of applicants and licensees. Therefore, a method for cumulative accounting of risk reduction improvements and associated cumulative costs is being developed for use by the NRC staff.

It is anticipated that the Commission will be deciding on its final Safety Goal Policy in mid-1986. It is expected that the final policy will reflect the same qualitative safety goals as expressed in NUREG-0880 (Rev. 1) but that the Commission will solicit public comment on the use of the integrated matrix concept proposed for implementation of the Safety Goal Policy.
EXTERNAL SAFETY POLICY IN THE NETHERLANDS: AN APPROACH TO RISK MANAGEMENT

M.F. VERSTEEG
Directorate for Administrative Affairs,
Directorate-General for the Environment,
Ministry of Housing, Physical Planning
and Environment,
Leidschendam, Netherlands

Abstract

A description is given of the use of risk-management by the Dutch government in their external-safety policy. This risk-management scheme comprises the aspects: risk-identification, risk-quantification, risk-assessment, risk-reduction and risk-control. For the process of risk-assessment quantitative criteria for both individual risk and group risk have been developed. Legislation emerging from this policy is completed or in preparation. As an example are the administrative orders emerging from the so called "LPG-nota". The latter is a policy statement of the Dutch government based on a probabilistic risk-assessment of the whole chain of LPG-handling activities, from import to retail trade.

Introduction

Catastrophic events like the explosions at the Flixborough Works of Nypro UK, the DSM works at Beek or the large toxic release of dioxin at Seveso together with a growing public concern about potential hazards, led the Dutch government to initiate a policy of External Safety. The immediate goals of this policy can be summarized as:
- to protect individuals against undue risk levels, and
- to prevent catastrophic accidents.

The recent catastrophies in Mexico-City, Bhopal and Chernobyl dramatize the urgent need for a systematic awareness of, and approach to
environmental hazards due to these types of activities. It was therefore decided to embark on an extensive research program to obtain operational knowledge of the assessment and management of risks in order to integrate these in decision-making processes. Although the research program is still underway an external safety policy including quantitative risk criteria has been developed. This external safety policy is imbedded in the environmental policy-plan of the Dutch government, as described in a document called: "Environmental Program of the Netherlands, 1986-1990" [1]. In this environmental program a chapter has been devoted to risk-management as a tool for external safety policy. One of the backbones of this external safety policy will be the so called Post-Seveso directive, a European directive soon to be implemented in the environmental legislation. This directive of the European Community makes it mandatory upon each member-state to verify that the most appropriate measures for preventing serious accidents in connection with industrial activities are taken.

Risk-management

In dealing with safety, one is confronted with a number of problems that can be summarized under the heading of Risk-management. That is, a decision-making process in which, on the basis of perceived risk and available means of risk-reduction, a decision has to be made about the acceptability of risk exposure levels and the control of allowed risk levels. An integrated part of the decision should also be an agreement on the emergency measures in case of accidents, e.g. warning procedures, evacuation of population, etc. and the testing of these emergency measures.
A risk-management scheme for fullfilling the abovementioned tasks consists of the following steps (see figure 1):

![Diagram of risk-management scheme]

These steps will be applied not only sequentially but also cyclicly. In other words this is a continuing process, and stops only after a license has been refused.

**Risk Identification**
The need for risk identification is obvious and requires no further explanation.

**Risk Quantification**
At the time of the policy's inception there existed little in the field of risk quantification models, apart from the PRA's in the nuclear industries.

Non-nuclear applications were limited to a few studies like the Canvey-island risk-study[2] and the COVO-study[3], which calculated the risk of 6 major industries in the Rhine-delta. There was also the Public Vulnerability Model (PVM) of the U.S. Coast Guard[4] which dealt with the risk associated with the handling and transport of dangerous substances in sea harbours. It was therefore decided to design a risk quantification scheme along the lines set out in the PVM and adapt it to
the special circumstances in the chemical industry in a densely populated country. A computer model is now operational. This code comprises generic failure data, dispersion models, meteorologic data, population data and dose-consequence models for the effects of toxic, flammable and explosive materials.

**Risk Assessment**

For the process of risk-assessment quantitative criteria have been developed. In setting up such criteria, the attitudes of the parties concerned had to be investigated.

The results of the attitude research have strengthened the argument for attempting to make the basis for policy decisions as objective as possible. One way of achieving this is to quantify risk as accurately and as scientifically as possible and compare the results with quantitative standards. The results of this comparison are clear, but will nevertheless lead to a debate in which all sorts of nonquantifiable arguments will be introduced. The objective arguments can than be weighed in whatever political system of decision-making happens to be in effect. The problem of standards remains, and for the time being the line of thinking of W.D. Rowe has been adopted. He distinguishes three areas of risk: the normal risk level, where permissible activities lie, the excessive risk level, where the risks are unacceptable, and an intermediate range of risk, where the reduction of risk is desirable. This concept is applied to the two goals of the external safety policy, namely protecting the individual against undue risks and the preventing of disasters which affect large segments of the population.
The starting point for determining the limit of unacceptability for individual risk is the frequency of deaths from natural causes. Mortality per year is presently used as the evaluation criterion. It is the lowest for children between 10 and 15 years old, namely $10^{-4}$/year. An industrial activity may not increase this background risk by more than 1%. The upper bound of acceptable individual risk is thus $10^{-6}$/year. An individual risk of $10^{-8}$/year or lower is considered as negligible (see figure 2). In the area between these values (two decades wide) the ALARA (As Low As Reasonable Achievable) principle will be applied. This separation of two decades between the two levels is also very useful in dealing with uncertainties.

**Figure 2: Criterion for individual risk**

Apart from the risk-criterion to protect the individual citizen, a criterion is developed to prevent, as much as possible, man-made hazards with a large societal impact. For these risk criteria two CCDF's (Complementary Cumulative Frequency Distribution) are chosen in the form of two straight lines on a log-log scale of the f-N plot (see figure 3). In order to deal with risk aversion a slope of -2 for these CCDF's is chosen. For example hazardous incidents in which 10 or more people are killed with a calculated frequency of $10^{-5}$/year, are considered as
unacceptable. Again below the lower CCDF the risk is considered as negligible (de minimis level).

Figure 3: Criterion for group-risk in the form of a CCDF

In assessing the calculated risk the 50th percentile CCDF will be of major importance, although the size of the uncertainty intervals, will be of interest as well. If no uncertainty analysis has been made the best estimate CCDF will fulfil the role of the 50th percentile CCDF. The decision-maker should be aware of the uncertainties involved and accomodate these uncertainties in his final decisions. To quote the former Minister Dr. P. Winsemius: "There is no substitute for thinking". The above mentioned assessment process is not a simple "yes or no"- decision but more a guideline for the decision-making process.
Risk Reduction

Risk can be reduced in two ways: first in-situ, by means of the lay-out of plant activities, the application of additional safety-devices and the use of less hazardous technology and the like; second, by means of zoning, i.e. keeping the public apart from the hazardous activity. Often a combination of both types of reduction is necessary. One of the major advantages of risk-quantification is that it can provide information about the cost-effectiveness of different sets of risk-reducing measures. On the basis of this information the licensing authority will be in a better position to judge what can be done at which costs. This of course is very important for his negotiations with the industries involved. This information is also very important for the licensing authorities in their presentation to the public; they are now able to demonstrate the measures which have been considered and the basis on which decisions regarding safety are made.

Risk Control

When it has been decided what an acceptable level of risk is, decisions have to made and implemented to safeguard this situation. The specific measures to be taken, will depend on the type and scale of activity involved.

Generally speaking the following actions will or may be required.

a) For stationary sources the license under the Nuisance Act may specify the safety measures to be taken and the procedures to be followed to test these measures.

b) The municipal authority is responsible for the implementation of the required zoning-measures.

Where required distances between the installation and the public cannot be maintained, the removal of either the vulnerable dwellings
or the hazardous installations may be enforced. The Dutch environmental and physical planning regulations provide for compensation-funds for such rehabilitation measures.

c) In case of risks associated with the transport of hazardous materials action may again be required to enhance the safety, either by improving the means of transport, or by routing and zoning, or both.

Applications

Implementation of the Post Seveso Directive

This guideline, based on the EEC-Directive concerning major-accident hazards of certain industrial activities[5], will soon be implemented in the environmental legislation. Two administrative orders, embodied in the Nuisance Act and the Labour Conditions Act, will require the industries concerned to provide the competent authorities with a notification comprising a quantitative risk analysis. One administrative order is for existing industries, while the other deals with new activities.

LPG policy

The before-mentioned risk-management policy was also applied to the whole chain of activities concerning the import, transport, storage, distribution and retail trade of LPG (Liquefied Petroleum Gas). Based on the expectation of a spectacular growth of the LPG-market, from 1 million tons a year to 10 million tons a year, the Dutch government commissioned a study of the possible risks which would accompany this growth[6].

The results of this study formed the basis for a policy statement of the Dutch government[7]. Legislation emerging from this policy statement is completed or in preparation.
The individual risk levels were translated into safety-distances to make the results more applicable for legislation. For example LPG-selling petrol stations within city limits will be closed if dwellings are located within 15 m distance. Compensation funds are used for this purpose. For larger distances safety-measures will be required.

**Nuclear Energy**

Although the abovementioned risk-management scheme was not primarily developed for nuclear power plants, public hearings and questions raised in the parliament on nuclear safety in relation to the risk-criteria triggered the demand for a PRA for the proposed nuclear power plants\(^3\) within the framework of the existing licensing procedure and the associated environmental impact assessment procedure.

**Future trends**

Developments are started to formulate criteria for late health effects. The feasibility to extend these criteria to the domain of societal risk, is investigated. Also the integration of these criteria with the existing risk criteria is a point of interest.

The role of human factors in the concept of risk-management is another area of development in the current safety policy. The main effort is to incorporate these influences in the domain of risk-quantification and risk-reduction.

Developments are to expected for an enlarged role of risk-perception in the decision-making process. How this can be done is very vague at this very moment. A lot of thinking is still needed on this subject.

\(^{a)}\) Due to the Chernobyl disaster the decision to continue or to stop with the siting-procedure has been postponed until 1988.
REFERENCES

Monographs, Multi-author volumes, Proceedings.

1. Environmental Program of the Netherlands 1986-1990, production and distribution by the Ministry of Housing, Physical Planning and Environment, Department of Information and International Relations, VROM 85902/12-85, 4078/92.


PROBABILISTIC SAFETY ASSESSMENT GOALS IN CANADA

V.G. SNELL
Risk Assessment and Safety Design Branch,
CANDU Operations,
Atomic Energy of Canada Limited,
Mississauga, Ontario, Canada

Abstract

CANDU safety philosophy, both in design and in licensing, has always had a strong bias towards quantitative probabilistically-based goals derived from comparative safety. Formal probabilistic safety assessment began in Canada as a design tool. The influence of this carried over later on into the definition of the deterministic safety guidelines used in CANDU licensing. Design goals were further developed which extended the consequence/frequency spectrum of 'acceptable' events, from the two points defined by the deterministic single/dual failure analysis, to a line passing through lower and higher frequencies. Since these were design tools, a complete risk summation was not necessary, allowing a cutoff at low event frequencies while preserving the identification of the most significant safety-related events.

These goals gave a logical framework for making decisions on implementing design changes proposed as a result of the Probabilistic Safety Analysis. Performing this analysis became a regulatory requirement, and the design goals remained the framework under which this was submitted.

Recently, there have been initiatives to incorporate more detailed probabilistic safety goals into the regulatory process in Canada. These range from far-reaching safety optimization across society, to initiatives aimed at the nuclear industry only. The effectiveness of the latter is minor at very low and very high event frequencies; at medium frequencies, a justification against expenditures per life saved in other industries should be part of the goal setting.

1. INTRODUCTION AND HISTORY

It is paradoxical that in many ways, the very early safety approaches adopted by CANDU designers were more closely tied to social safety goals than those we use today. A large contributor to the formulation of safety goals in terms of probabilistic principles was the experience with research reactors at Chalk River Nuclear Laboratories (CRNL) in the 1950's. The accident to the NRX pressure tube reactor, in 1952 [Ref. A,B] was extremely damaging to the core because it came from a failure of both a normal process
disaster could occur if we had a simultaneous failure of ALL of: a normal process system (such as the reactor power control system), a protective system (emergency core cooling or shutdown) and containment. From this he derived the following design targets:

<table>
<thead>
<tr>
<th>Process failures</th>
<th>One in 10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protective System</td>
<td>One in 100 demands</td>
</tr>
<tr>
<td>Unavailability</td>
<td>One in 100 demands</td>
</tr>
<tr>
<td>Containment System</td>
<td>One in 100 demands</td>
</tr>
</tbody>
</table>

These numbers were chosen large enough to be demonstrable individually by experience or testing in a few years of reactor operation.

These ideas were applied in the design of Canada's first demonstration power reactor - the Nuclear Power Demonstration (NPD) Reactor. Its 1961 Hazards Report used higher unavailability for shutdown, and did not credit containment. It also assessed the dose to the public from less severe accidents than disasters, using as a figure-of-merit a "once-in-a-lifetime" emergency dose. For Iodine-131, for example, this was 25 rad.

The Safety Report for the 200 MW Douglas Point nuclear reactor, in 1962, was perhaps the fullest flowering of the overall risk-based approach. The safety goal, proposed by the designers, was that the risk of death to any member of the public be less than $10^{-6}$ per year, a factor of 10 less than that for NPD. The target risk for injury was taken to be 10 times larger, in the same ratio as experienced in other industries. The breakdown by frequency was similar to that for NPD, with some allowance for the lower frequency of large pipe breaks. Included in this risk evaluation was a quantification of the effects of a major accident on the operating staff. The Safety Report consisted of a systematic listing of all identifiable events, an evaluation of their frequency, and a calculation of their consequences in terms of dose. Again, separation was assumed to be achieved by careful design practice. Note in addition the increasing requirement for nuclear not just to be safer than coal, but to be orders of magnitude safer. This was partly due to the fact that it was a new technology and the "increased safety" seemed achievable, and partly to cover uncertainties. However this did result in an erosion of the rationale for optimizing safety across industries.

2. THE SINGLE/DUAL FAILURE APPROACH

In 1967, F. C. Boyd of the AECB laid the groundrules for the deterministic licensing guidelines, under which all large operating CANDU plants have been licensed. They showed evidence of their risk-based origins, but collapsed the
spectrum of possible accidents into two broad categories: single failures, or the failure of any one process system in the plant; and dual failures, a much less likely event defined as a single failure coupled with the unavailability of either the shutdown system, containment, or the emergency core cooling system. (This single failure, by the way, is an assumed system failure, and is not related to the same term used elsewhere to describe a random component failure additional to the initiating event). For each class, a frequency and consequence target was chosen that designers had to demonstrate were met. In addition, to deal with the siting of a reactor (Pickering A) next to a major population centre (Toronto), population dose limits were defined for each class of accident. For whole body doses, these were:

<table>
<thead>
<tr>
<th></th>
<th>INDIVIDUAL</th>
<th>POPULATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Failure</td>
<td>0.5 rem</td>
<td>10^-4 man-rem</td>
</tr>
<tr>
<td>Dual Failure</td>
<td>25 rem</td>
<td>10^-6 man-rem</td>
</tr>
</tbody>
</table>

with additional limits for thyroid dose. These were chosen as follows, based on the knowledge at the time:

1. The 25 rem individual dose was the threshold of observable cell damage at the microscopic level.

2. The 10^-4 man-rem would cause a negligible (<1%) increase in the number of cancer deaths relative to those from other causes.

3. The 10^-6 man-rem would cause a number of leukaemia cases comparable to the normal incidence for one year.

The single failure individual dose was consistent with international annual limits for normal operation.

The current guidelines were finalized in 1972 by D. G. Hurst and F. C. Boyd of the AECB [Ref. F, and subsequent applications]. They were similar to Boyd's 1967 guidelines, with two key clarifications:

1. The status of the containment system was changed. Failures of containment subsystems (such as failure to isolate ventilation dampers) would now be included as part of the full accident matrix, as opposed to containment being treated monolithically as available or unavailable.

2. If the designer provided two capable independent shutdown systems, he would not be required to postulate a total loss of shutdown capability.
The guidelines were as follows:

<table>
<thead>
<tr>
<th>ACCIDENT</th>
<th>MAXIMUM FREQUENCY</th>
<th>INDIVIDUAL DOSE LIMIT</th>
<th>POPULATION DOSE LIMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Failure</td>
<td>1 per 3 years</td>
<td>0.5 rem wb 10^-4 man-rem</td>
<td>3 rem thy. 10^-4 thy-rem</td>
</tr>
<tr>
<td>Dual Failure</td>
<td>1 per 3000 years</td>
<td>25 rem wb 10^-6 man-rem</td>
<td>250 rem thy. 10^-6 thy-rem</td>
</tr>
</tbody>
</table>

The dual failure frequency was too small to be observed directly. The inference that the dual failure was less than the rates above came from the observed single failure frequency after a few years of operation, and the safety system availability demonstrated through continual on-power testing of the safety systems.

The concept of overall safety goals was narrowed, and approached through subtargets of demonstrating the frequency of more common accidents, and establishing the reliability of mitigating systems. Note the risk aversion implied above, with the frequency*consequence of dual failures being about an order of magnitude less than that for single failures.

3. PROBABILISTIC SAFETY ASSESSMENT

As a safety design tool, the single/dual failure approach gave a basis for design of the four special safety systems, but had several deficiencies:

1. It did not provide a way of treating multiple process failures, even if these could be more probable than single or dual failures. This is particularly true of failures of safety support systems, such as electric power, instrument air, etc. As well, there was no way of putting into perspective any events which were beyond the original design basis of the plant, but for which the regulatory body wanted to know the consequences.

2. In terms of assessing design changes, it did not factor in realistic frequencies, so that a small power excursion, a large loss-of-coolant, and multiple low-frequency failures were all treated on an equivalent footing.
3. By the same token, because events were analyzed with conservative assumptions on plant performance, safety analysis could give a misleading picture to the operator of the expected plant response to an accident.

4. Safety system failures, while explicitly identified and analyzed, were treated simplistically, particularly for safety systems, such as containment and emergency core cooling, with redundant components and subsystems which were highly reliable.

5. There was no framework for looking at long term equipment reliability, once the initial phase of the accident was over.

For these reasons, AECL began a probabilistically-based design review of the Bruce-A plant, later extended to Bruce-B, Pickering-B and the 600 MW CANDU plants [Ref. G]. This consisted of construction of fault trees and event sequences for classes of failures. The event sequences were terminated when either stable plant conditions were achieved or the event sequence frequency reached about $10^{-7}$ events/year. This cutoff frequency, besides being appropriate for a design review, was believed to be consistent with the single/dual failure guidelines, which do NOT require specific design provisions for events involving failure of more than one independent safety system; i.e., at frequencies of the order of $10^{-7}$ events/year.

Some design criteria had to be used to decide if a design change was warranted. To arrive at this, the single and dual failure points were plotted on a frequency/dose graph and a line was drawn between them, and extrapolated to lower and higher frequencies (Fig. 1). This is by no means a safety goal - simply a way of screening proposed design changes. There was no summation of risk: each event was plotted on this graph and evaluated on its own merits. Initiating events were grouped into fifteen classes, called Safety Design Matrices (SDM's), with initiating frequencies determined for the class. This also avoided artificially reducing an event frequency by continuous subdivision of the event. Event sequences were analyzed into the long term, of particular benefit in determining what operator actions are required, and how likely the operator was to perform those actions. The exercise more than fulfilled its purpose, identifying the following design changes, and providing a sound basis for writing abnormal operating procedures.
TABLE 2 - STATION DESIGN CHANGE REQUESTS FROM SDM STUDIES

<table>
<thead>
<tr>
<th>STATION</th>
<th>NUMBER OF CHANGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gentilly-2</td>
<td>92</td>
</tr>
<tr>
<td>Point Lepreau</td>
<td>66</td>
</tr>
<tr>
<td>Wolsung</td>
<td>37</td>
</tr>
<tr>
<td>Pickering B</td>
<td>22</td>
</tr>
<tr>
<td>Bruce B</td>
<td>17</td>
</tr>
</tbody>
</table>

Note how design changes identified in the earlier stations were quickly implemented in the ongoing design of the later ones, as reflected in the smaller number of change requests for the latter.
It is in my opinion arguable if the screening line chosen ever made any difference - a sobering thought when we move from establishing realistic safety goals to their implementation. (Of course, if the goals are chosen unduly pessimistically, the shape of the goal will eventually make a difference.) First, for high frequencies (around $10^{-3}$ per year), a prudent utility will not tolerate the economic loss that a significant release (fuel damage) implies. The only item a screening line might independently catch at high frequencies would be heavy water spills, where the dose from any released tritium could be more limiting than the economics. Second, the probabilistic study confirmed that the safety systems and the process systems were independent enough, in fact, so that for example the large loss of coolant accident required no further design provision down to frequencies of about $10^{-7}$/yr. That is, the nature of the CANDU with its pressure tubes and independent cool moderator, together with the requirement to analyse the dual failure 'loss of coolant plus loss of emergency core cooling' meant that core melt accidents were NOT identified down to such frequencies for the usual accidents. In short, consequences (dose) were limited by the dual failure dose guideline down to $10^{-7}$/yr or so. Indeed, most accidents were limited by the single failure guideline dose.

In other words, the design changes identified in the study, and implemented, generally arose because of overlooked crosslinks or from multiple process system failures, most of which would have been corrected, once found, independent of the existence of a screening line. Some of these lead to indeterminate end-points, i.e., no identified heat sink at frequencies greater than $10^{-7}$/yr. In principle, these could either be handled by performing a degraded core analysis, and showing the doses were met, or by design changes to ensure an identified heat sink such as the moderator or the steam generators. In practice, the effort involved in performing a core melt analysis for a CANDU was not considered cost-effective, so the design changes, most of which were fairly simple, were implemented instead. For frequencies only slightly higher than $10^{-7}$/yr, the scenarios were debated internally as to the cost/benefit of making any change, particularly in view of the conservatisms which still existed to some degree in the analysis.

The message is that for an existing design, realistic safety goals will only affect the high-frequency end of the accident spectrum, and may be well within the capability of intrinsic features of the reactor design. For a new design, if deterministic analysis rules are abandoned, the design could be considerably rationalized by the application of safety goals to the mid-frequency part of the spectrum (Fig.2).
4. INTERORGANIZATIONAL WORKING GROUP

Because of arguments as to the interpretation of the single/dual failure approach, the AECB formed, in 1977, an Interorganizational Working Group (IOWG), headed by Dr. W. Faskievici of Ecole Polytechnique. It consisted of representatives of the designers, regulatory, utilities, and universities, and had as its mandate to identify, document, and clarify Canadian safety principles. The group retained the defence-in-depth approach by requiring specific, independent special safety systems. It expanded the probabilistic basis of the previous guidelines by defining a set of six levels of dose, with defined frequency bands, and with risk aversion built in at the lower frequencies. The proposal required summation of the frequencies of events contributing to a given dose interval, and could therefore be used for risk estimates. Events with frequencies less than $10^{-7}$ per year were, explicitly, not to be considered for design mitigation [Ref. H], although the frequencies of events causing doses >100 rem were to be summed, and shown to be $<10^{-6}/yr.$
TABLE 3 - IOWG PROPOSED DOSE/FREQUENCY GUIDELINES

<table>
<thead>
<tr>
<th>REFERENCE DOSE INTERVAL, REM</th>
<th>THYROID</th>
<th>SUM OF FREQUENCIES OF ALL EVENTS IN DOSE INTERVAL MUST BE LESS THAN (/YR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - .05</td>
<td>.5</td>
<td>$10^{(-1)}$</td>
</tr>
<tr>
<td>.05 - .5</td>
<td>.5 - 5</td>
<td>$10^{(-2)}$</td>
</tr>
<tr>
<td>.5 - 5</td>
<td>5 - 50</td>
<td>$10^{(-3)}$</td>
</tr>
<tr>
<td>5 - 10</td>
<td>50 - 100</td>
<td>$10^{(-4)}$</td>
</tr>
<tr>
<td>10 - 30</td>
<td>100 - 300</td>
<td>$10^{(-5)}$</td>
</tr>
<tr>
<td>30 - 100</td>
<td>300 - 1000</td>
<td>$10^{(-6)}$</td>
</tr>
</tbody>
</table>

These guidelines allowed a factor of ten increase in predicted doses if encountered at a late stage in the design. This was attacked by antinuclear critics as both an increase in what the AECB had previously "allowed" for the maximum dose, even though it referred to a different event, and as an acknowledgement of the possibility of prompt deaths.

For this reason, and some caution about the new probabilistic techniques, the AECB did not adopt it and instead proposed a Consultative Document C-6.

5. CONSULTATIVE DOCUMENT C-6

The AECB issued C-6 in June 1980 [Ref. I]. This retained the concept of several classes of events, five in this case, but with important differences:

1. Although the classes represented decreasing event frequency, assignment of events to the classes was done a priori by AECB staff, based on their belief as to the likelihood of the event. This was done with a conservative bias, so that an analysis done in the framework of C-6 could give a distorted picture of safety. Also by assigning events to a class, the document removed from the designer some of his incentive either to show that an event was indeed less frequent, or to make changes to decrease the frequency. Indeed, the list of events is highly design-specific, and might not be sensibly applied to future plants - a significant limitation as new generations of CANDU are being developed.
2. Because of the sensitivity to appearing to increase the maximum "permissible" dose, the AECB set the maximum dose for the most infrequent class at 25 rem whole body: in other words, events LESS frequent than the traditional dual failure were not recognized in terms of increased allowable doses.

3. Since each event was required to meet a given dose, there was no need to sum to get a risk estimate.

The limits were as follows:

TABLE 4 - DOSE/FREQUENCY LIMITS FROM AECB DOCUMENT C-6

<table>
<thead>
<tr>
<th>EVENT CLASS</th>
<th>WHOLE BODY</th>
<th>THYROID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.05</td>
<td>.5</td>
</tr>
<tr>
<td>2</td>
<td>.5</td>
<td>5.</td>
</tr>
<tr>
<td>3</td>
<td>3.</td>
<td>30.</td>
</tr>
<tr>
<td>4</td>
<td>10.</td>
<td>100.</td>
</tr>
<tr>
<td>5</td>
<td>25.</td>
<td>250.</td>
</tr>
</tbody>
</table>

In short, C-6 can best be viewed as a deterministic approach, despite its growth from two to five classes. It is not helpful in terms of safety goals, due to its distortion of event frequencies and unrealistic capping on maximum dose. It does formalize the requirement for a systematic plant review, as pioneered by the Safety Design Matrices.

In application, it is being used on a trial basis in the licensing of Darlington-A Nuclear Generating Station. Ontario Hydro is also doing a full probabilistic risk assessment for this plant [Ref. J, K], but has separated this study, beyond the requirement for a systematic plant review, from the C-6 context. The predictions of public health and economic risks will be compared to utility-generated targets, but the study is primarily a design review vehicle.

For a proposed second nuclear generating station at Point Lepreau, negotiations have been underway with the AECB to obtain detailed agreement on the licensing requirements and their implementation before the plant is constructed [Ref. L]. It seems likely that the deterministic approach
will be used to design the safety systems, and the intent of C-6 for a systematic review of the plant will be achieved through the use of risk-based criteria for evaluating the results of the probabilistic safety assessment. The probabilistic safety assessment itself will generate realistic event frequencies, and will avoid distortion in the results. As of this writing, no risk summation is planned. Again, the emphasis is on a design review.

6. ADVISORY COMMITTEE ON NUCLEAR SAFETY DOCUMENT ACNS-4

The Advisory Committee on Nuclear Safety is a senior group which advises the Atomic Energy Control Board on nuclear safety. In 1983, it issued a report on a new set of proposed safety requirements, which was a middle ground between C-6 and the IOWG. It basically adopted the IOWG methodology, but compromised by removing the allowance of a factor of 10 on maximum dose in certain cases - i.e., no predicted dose could exceed 100 rem equivalent. Like IOWG, it required the risks to be summed in each category, and allowed a cutoff frequency of \(10^{-7}\) events/year. It permitted the use of realistic frequencies and accident consequence models. The authors pointed out that their "proposed criteria from accident sequences result in a risk to the most highly exposed individual in the general public which is of the same order as that resulting from natural background radiation". Indeed, because of the built-in risk aversion, the high frequency limits dominated the risk.

Their limits, expressed in terms of effective dose equivalent, were as follows:

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>DOSE INTERVAL, REM</th>
<th>SUM OF FREQUENCY OF OCCURRENCE/YR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 - 10(^{-0.5})</td>
<td>3.33 (*) 10(^{-1})</td>
</tr>
<tr>
<td>2</td>
<td>10(^{-0.5}) - 1</td>
<td>10(^{-1})</td>
</tr>
<tr>
<td>3</td>
<td>1 - 10(^{0.5})</td>
<td>10(^{-2})</td>
</tr>
<tr>
<td>4</td>
<td>10(^{0.5}) - 10</td>
<td>10(^{-3})</td>
</tr>
<tr>
<td>5</td>
<td>10 - 10(^{1.5})</td>
<td>10(^{-4})</td>
</tr>
<tr>
<td>6</td>
<td>10(^{1.5}) - 100</td>
<td>10(^{-5})</td>
</tr>
</tbody>
</table>

ACNS-4 has not been used so far on any plant, nor has it been adopted by the AECB in licensing.
All of these attempts to set meaningful safety goals have been seriously challenged by E. Siddall [Ref. M, N]. By comparing the money spent on preventing an extra premature death in various activities, he concludes that about three orders of magnitude more money is spent on saving a life in the nuclear industry than in activities such as medical screening. In this sense, overly restrictive safety goals for nuclear power kill people by diverting financial resources from where they could save more lives per dollar to where they save least. None of the documents discussed above really addresses this point; there is no comparison to society-wide safety goals, and the only numeric comparison made is with normal risks of operation of a nuclear plant.

There is a more subtle effect of applying safety goals to the low-frequency end of the spectrum, and that is the uncertainty associated with frequency and consequence predictions. This argument has been used in the past as a justification of conservative assumptions in setting the goals. Designers too have preferred to use conservative or bounding assumptions in the calculation of accident consequences because it was cheaper, because of the impracticality of designing to fit a continuous safety goal spectrum and because there was no incentive to showing margins to safety targets. The history of both hypothetical and real accidents has, however, gone the other way, with the massive disasters due to core melt/steam explosion as in WASH-1400 now considered all but incredible, and most core melts shown to have minor offsite public health consequences. Iodine had much attention focussed on it in the past, yet because of recent basic chemistry studies and the Three Mile Island Accident, is no longer recognized as a such a significant safety concern for water-cooled reactors. Suppose in response to safety goals in the past, money had been spent on design provisions to reduce iodine release. With current knowledge, this would now be perceived to have been wasted. Indeed, CANDU reactors licensed under single/dual failure guidelines all appeared to be limited by iodine release, a conclusion now being turned on its head. One therefore has to be very careful, not only in specifying safety goals which are themselves conservative as ACNS-4 does by virtue of low absolute risk values and severe risk aversion, but also in the practical application of these goals in determining plant licensing requirements. Such applications should not have additional conservative assumptions layered on, since this conservatism steals money from better use outside the nuclear industry. Removing such conservatisms can also be expensive in terms of R & D and analysis.
CONCLUSIONS

1. For more frequent accidents (one per 1000 reactor years or more), economics is limiting. The regulatory could simply ensure that potential core damaging accidents are identified through a systematic Probabilistic Safety Assessment. The numeric value of the safety goals is less important than their existence, which implies an assessment is indeed done.

2. For very infrequent accidents (<10^-6 events/yr or so), the uncertainties on the consequences are more likely favourable than unfavourable. Although the plants have substantial resistance to such accidents, any assessment is for information only and should not be used for safety goal setting. Safety goals should therefore have an explicit cutoff on event frequency, say around 10^-6 to 10^-7 events/year, and not require summation of very low frequency events since it won't influence the design.

3. For events whose frequency falls between these cases, safety goals are useful in guiding the design. However they should be explicitly justified in terms of the amount of money spent to save a life, to avoid misuse of resources.

REFERENCES


STATUS OF PROBABILISTIC SAFETY CRITERIA IN FRANCE

P. CANDES
Institut de protection et de sûreté nucléaire,
Commissariat à l'énergie atomique,
Fontenay-aux-Roses, France

Abstract

The paper reviews the use of probabilistic approach to NPP safety in France. It introduces the limits of $10^{-6}$/yr as the global probability for unacceptable consequences and $10^{-7}$/yr for each particular family of adverse events. Complementary measures to impose the safety level for some specific situations are described. An example of safety improvements introduced for the loss of electric supply is given.

I - CONCEPTION BASES OF FRENCH NUCLEAR POWER PLANTS

The French nuclear program for generation of electricity relies mainly on the concept of the standardization of significant series of NPP.

Let us note the series of 900 MWe (CP1 and CP2) 1300 MWe (P4 and P4') and 1400 MWe (N4).

Annexe I gives the geographic location of sites and the completion of the program.

For each of these series the justification of the safety features provided to avoid any unacceptable risk is brought by deterministic studies. These studies include calculations of selected scenarios of accidents and their radiological consequences. Such studies involve pessimistic assumption in order to guarantee sufficient safety margins. These scenarios can be initiated either by internal causes or failures, or by external natural or man made events (earthquakes, extreme meteorological conditions, floods on rivers or from the sea, aircraft crashes, industrial extreme events...).

For each plant on a site radioactivity releases are limited by official regulations. These regulations are expressed in terms of quantities (curies) and specific categories of nuclides at levels sufficiently low to give a guarantee of their compliance with radioprotection regulations (dose limitation and alara principle).

The safety approach of the different events characterised by their radioactives releases and taken into account for the design (or as design bases) leads to the following classification table (proposed by EDF and
accepted by the safety authority):

<table>
<thead>
<tr>
<th>Frequency of occurrence category</th>
<th>Estimated frequency (events/year)</th>
<th>Maximum radiological consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Limitation by radioactive releases regulation</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-2}$ to 1</td>
<td>0.5 rem [W.B]</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-4}$ to $10^2$</td>
<td>1.5 rem [thyroid]</td>
</tr>
<tr>
<td>4</td>
<td>$10^{-6}$ to $10^{-4}$</td>
<td>15 rems [W.B.]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>45 rems [thyroid]</td>
</tr>
</tbody>
</table>

This is the actual practice. Annex II gives the list of adverse situations or accidents postulated for 1400 MWe [type N4] by the designers and accepted by french safety autarkies.

II - PROBABILISTIC APPROACH

Historically, probabilistic approach has been introduced in french safety to specify design bases related to external extreme events so has to establish a good balance between bases related to these events and bases related to internal events.

As soon as 1977, after several years of practice in such a way, the safety authority has set a general probabilistic objective. This objective is stated as follows:

The design bases for a pressurized water reactor should be such as the global probability for unacceptable radiological consequences is not higher than to $10^{-6}$/year. For the general approach it is supposed that different families of events (internal events, external events of natural or man made origine) are contributing to the global risk. If the probability of a family of adverse events capable to bring unacceptable radiological consequences, is higher than $10^{-7}$ event per year, such family is taken into account for the design.

The applicant shall also examine if simultaneous failures of redundant systems important for safety, are to be taken into account in the design.
Several comments can be done on this philosophy:

1] The term "unacceptable consequences" is not defined in regulatory terms. This concept has be weighed in terms of level of radiations versus site parameters such as density and distribution of population and mainly the appreciation of the feasibility of an emergency plan.

2] The probability of $10^{-6}$ per year shall be understood as an objective and is not required as a demonstration. Due to the present state of the art significant advances in that field are in progress, but still require an important amount of work, as it is recognized at an international level.

3] As a consequence, calculations and determinations of most of the features of the design, rely always in deterministic approach (application of defence in depth philosophy, quality assurance procedures, experience of operation...).

4] The figure of $10^{-7}$ event per year related to particular families of events, is rather easy to apply for some of these families for example aircraft crashes, but in other cases (e.g. earthquakes), a deterministic approach is necessary to "appreciate" the level of probability. Also it is acceptable to admit that such a value is not a cut off for one single family. Compensation with other families is accepted.

5] It is worthy to note that for deterministic approach assessment calculations are made on the basis of pessimistic assumptions so as to guarantee a safety margin (reasonably large). For the probabilistic approach realistic values are accepted for assessment and calculation of probability figures (the safety objective of $10^{-6}$-$10^{-7}$ quoted above is in itself considered as sufficiently pessimistic in itself).

III - PRACTICE OF PROBABILISTIC APPROACH

1] As quoted above probabilistic approach has been directly applied in France for external events.

2] In other instances probabilistic approach made it possible to show the necessity of implementation of complementary measures to impose the safety level for some specified situations.

This has been the case for:

a] failure of the safe shutdown system in case of transients which necessitate a shutdown.

b] failure of one of the systems for the safe release of heat produced in the reactor to the cold source or from the cold source.

c] simultaneous failure of the whole of electric supply sources.

Such complementary measures can be intended (depending of the type of reactor [900 or 1300 MWs]) as definition of procedures for a specified use of existing means or functions in the reactor, or as conception (e.g. design) improvements. This can imply, consequently differences of treatment of the problem in the two cases. This is due to the fact that the
900 MWe series were designed and built [for most of the reactors of that program] whereas for 1300 MWe type, modifications of the design were still possible.

For the new recent type 1400 MWe (N4) a number of specified operational and accidental situations could be assessed for being included in the design. A probabilistic approach has been used for these assessments.

Let us quote:

- failure of steam generators emergency water supply,
- failure of the safe shutdown system for situations of first and second category,
- failure of the whole of electric supply sources,
- failure of cold source or heat transfer systems to the cold source,
- failure of low pressure emergency core cooling system,
- failure of heat transfer system associated to confinement building spray system.

Other events, such as:

- simultaneous rupture of a main steam pipe and several steam generator tubes,
- total failure of intermediate pressure safety injection system,

are been studied in view to reduce their probability of occurrence or the radiological consequences involved in corresponding scenarios. In addition, always for N4 type, core melting due to the loss of a redundant system has been deemed as unacceptable (e.g. the assessed probability of such an event shall be less than $10^{-7}$ per year).

3) The French probabilistic approach takes into account specially for high water power reactors the experience of operation. For example, for the reactors of the type N4, the rupture of a steam generator tube is classified in the third category instead of fourth category.

4) The 900 MWe PRA

A probabilistic analysis has been undertaken for the 900 MWe series.

The specific objectives of this analysis is twofold:

- provide a basic assessment of the risk related as a standard plant
- realize a model capable to take into account the influence of complementary measures or modifications implemented after the construction of the plant.

The measures quoted under the second dash hereabove are different procedure to face accidental situation (e.g. H procedures). For example H3 procedure is applied in case of loss of electric supply.
5] An example of application improvement of safety in case of loss of electric supply

Electric supply of nuclear power plant in France is implemented from four sources: two independent external electric sources from the general grid and two internal electric emergency supplies diesel actuated. It is also possible to realize the autonomous feeding of the NPP by the main electric generator in case of loss of the grid.

These sources are feeding two independent lines (A and B) for the supply of auxiliary system or safety related systems (safety functions) through two emergency switch boards (6.6 kV LHA and LHB). One diesel generator is directed to line A, the other to line B. The direct consequence of loss of the system is the failure of water supply to water seals of primary pumps. The evaluation probability of such an event in that context leads to the figure of $2 \times 10^{-5}$ per year.

This situation needed improvements: Among them: provide one gas turbine electric generator for each site (most of the French sites have four reactors), provide emergency supply from other reactors in the site, provide complementary water supply to the water seals, and in fine improve the emergency water supply steam generators. These improvements have been directly incorporated in the design for 1300 and N4 series.

CONCLUSIONS

As indicated above probabilistic analysis in French safety has been introduced progressively and in particular since 1977, when quantitative objectives were decided by the safety authority.

Some particular aspects can be mentioned:

1) In the event-trees of accidental sequences the notion or success of failure of accidental procedures (H or U procedures) is introduced.

2) All possible states of the reactor and in particular cold shutdown are taken into consideration.

3) Long term evolution of an accident is taken into account for its contribution to resulting risk.

4) Possibility of recovery of failing systems by complementary means or procedures are included in the evaluation.

5) As far as possible experience of operation leading to a better knowledge of reliability of equipments or initiation of particular types of events, is taken into account.

6) Other aspects such as incident or accidents computerized collection and analysis and development of codes related to behaviour of source terms or release of fission products are strongly developed.

Perhaps as a last comment, probabilistic analysis is encouraged as a tool for the assessment of safety in operations.
Thought is given to different aspects in this field such as:

- situations in which unavailability of certain equipments has been specified [and accepted]
- situations taking into account unexpected unavailabilities.
- degraded situations.

The work presently done for 900 MWe PRA is considered as being a PRA approach one could denominate as phase 1.

The phase 2 for which developments are been done, will express the risk in terms of sources of fission products related to different families of accidents. Work has been published and contributions to NEA/CSNI working groups have been provided. For the present work in this field is mainly done for characterization of the sources of fission products related to severe accidents the first aim is to prepare measures for the mitigation of the radiological consequences of such accidents. Most of the U procedures (U2 et U5) are in this line. Some of these procedures US for example need a certain amount of research and development.

ACKNOWLEDGMENTS

The author thanks warmly the authors of the paper quoted in reference for their help and fruitful discussion.

REFERENCE

- QUENIART Daniel, BRISBOIS Jacques, LANORE Jean-Marie

Utilisation de méthodes probabilistes pour l'évacuation de la sûreté des réacteurs à eau pressurisée construits en France

Colloque international sur l'application des codes et guides de sûreté [documents NUSS]

AIEA - VIENNE - 29 Octobre-2 Novembre 1984 -
Présentation AIEA SM 275-5
**ANNEX I**

**SITUATION AU 1er JANVIER 1984**

**TYPE**

- UNGG
- Gaz-Eau lourde
- Surgénérateur
- REP. refroidissement circuit ouvert
- REP. refroidissement circuit fermé, tours

**PALIER STANDARDISÉ**

- Tranches 900 MWe - REP (PWR)
- Tranches 1 300 MWe - REP (PWR)
- Tranches 1 400 MWe - REP (PWR)

REP = Réacteur à eau ordinaire sous pression

---

**LES DÉCISIONS PRISÉES EN 1983**

- Engagements autorisés en 1983 (Penly-1, Golfech-1), 2 unités, 2 565 MWe
- Engagements autorisés en 1984 (Chooz B-1, Cattenom-4), 2 unités, 2 645 MWe
- Engagements en 1985
  - 1 autorisé
  - 1 optionnel 2 unités

Optionnel : fonction de l'évolution des perspectives de consommation
The following list has been proposed by the applicant (EDF) to the safety authority. Such situations are classified in accordance with the categories characterized by their decreasing frequency versus increasing risk. These situations are taken into account for the design with deterministic criteria and pessimistic assumptions for the basis of the calculations.

- **First category** (estimated frequency 1 per year)
  - events related to normal operation.

- **Second category** (estimated frequency: $10^{-2}$ to 1 per year)
  - incidents with very limited radiological consequences.

Let us quote:

- uncontrolled withdrawal of control rods the reactor being subcritical
- same situation with reactor in operation
- erroneous position and fall of a cluster
- uncontrolled dilution of boric acid
- partial loss of primary coolant.
- starting of an inactive loop
- loss of power - turbine trip
- loss of normal feedwater
- poor functioning of normal feedwater system
- loss of external electric supply
- excessive increase of power
- short pressure cast down of the primary circuit due to opening of pressurizer relief valve
- untimely opening of a secondary valve
- untimely starting of borication system
- **Third category**

Low frequency accidents \((10^{-4} \text{ to } 10^{-2} \text{ per year})\) whose radiological consequences are limited:

- loss of primary coolant (small breaches)
- long duration depressurization of the primary circuit by opening of the pressurizer relief valve
- small breach of the secondary circuit
- total loss of flow of the primary circuit
- erroneous positioning of a fuel assembly in the core
- withdrawal of a control rod at full power
- rupture of the volume control tank
- rupture of gaseous radioactive waste tank
- complete rupture of a steam generator tube

- **Fourth category**

Hyptothetical severe accidents whose consequences are postulated as acceptable \((frequency \ 10^{-6} - 10^{-4} \text{ per year})\):

- fuel handling accident
- large breach in the secondary pump rotor
- ejection of compensation cluster
- large loss of primary coolant
- complete rupture of two tubes of steam generator
STATUS OF PROBABILISTIC SAFETY CRITERIA IN ITALY

A. FERRELI
Italian Directorate for Nuclear Safety and Health Protection (ENEA-DISP), Rome, Italy

Abstract

In Italy the probabilistic approach to safety problems has been progressively introduced starting from the 70's, when quantitative reliability objectives were established for specific systems of the Caorso NPP.

An extensive use of probabilistic techniques has been requested for the PUN, the Italian PWR standard plant. The Italian Regulatory Body issued in 1983 a set of General Design Criteria (GDC) where quantitative targets in terms of effective dose equivalent for the members of the public have been established for the different plant conditions grouped in probability ranges.

With regard to events beyond design basis accidents a design objective has been fixed in terms of maximum overall probability for the complex of sequences that could lead to degraded conditions. In order to verify compliance with the above established targets a Probabilistic Safety Study (PSS) has been performed.

The methodology used is similar to that described as level 1 PRA in NUREG/CR-2300 "PRA Procedure Guide"; the analysis considers only internal and area events, whereas external hazards, both natural and man made, were excluded. A uncertainty analysis is not foreseen at the first stage of the project, because of many design features not yet well defined and the consequential conservative assumptions used.

The weakest points in the design were discovered through sensitivity and partial importance analysis, and plant design modifications have been proposed in order to achieve the probabilistic goal.

The PUN-PSS shall be considered as an interactive tool to be developed and updated together with the design and on the base of the outcomings of
the licensing process. In this way the PUN-PSS appears as a "living schedule" continuously updated and therefore valid to evaluate the safety level of the plant and to support at any moment every decision. Possible set of criteria for the reassessment of severe accidents and the definition of new source terms for regulatory purposes to be used for could be established in the next future. A specific study to evaluate the containment response and reliability up on core melt has been carried out by the Italian regulatory body for plants representative of the most common containment schemes. The results indicate that iodine release fractions are always lower than $10^{-3}$ times the core inventory for those sequence whose conditional probability upon core melt has been evaluated higher than $5 \times 10^{-2}$.

---

Status

In Italy, the probabilistic approach to safety problems has been progressively introduced, also as an item of licensing, starting from the 70's, when quantitative reliability objectives were established for specific systems and components for the Caorso NPP. Subsequently, for ALto Lazio NPP, a BWR plant now under construction, two sets of probabilistic requirements have been specified. The first one fixes upper limits for the doses to the members of the public, bounded to the expected frequencies of prefixed groups of initiating events. The second requirement is aimed at assessing the generic adequacy of the reliability levels of the plant protective functions, without specified numerical targets: as a reference element to judge of the adequacy of the results, the balance of the protective function reliability in relation to the frequencies of the initiating events has been assumed. For the implementation of this requirement a probabilistic assessment has been performed, and licensing acceptance criteria have been chosen. Consideration was given to the common mode failures; dependencies of auxiliary systems were treated by means of fault tree linking
techniques, while for other kinds of common mode failures the latest available techniques (binomial model) have been used. Human factors were extensively treated by means of human reliability techniques (Swain and Bell procedures) for those sequences with relevant impact on either the core melt or containment failure.

An even more extensive use of probabilistic techniques has been required for the PUN, the Italian PWR standard plant to be developed in the framework of the present National Energy Plan.

The Italian Regulatory Body issued in 1983 a set of General Design Criteria (GDC) afforded by the experience matured at that time. Going on with the experience already gained with Alto Lazio NPP, quantitative targets in terms of effective dose equivalent for the members of the public have been established for the different plant conditions grouped in probability ranges. In particular for the operating conditions, which include also the abnormal operating transients up to a calculated frequency of $3 \times 10^{-2}$ per event, a limit of 0.1 mSv per year, averaged over the plant life, has been assumed.

Targets in term of effective dose equivalent per single event have been established for accidents having an occurrence probability lower than $3 \times 10^{-2}$: in particular a limit of 5 mSv has been established for accident whose annual probability is higher than $10^{-3}$, and a limit of 0.1 Sv for accident whose annual probability is lower than $10^{-3}$.

The above mentioned targets are presented in a graphical form in the attached figure. The dotted line represents the theoretical dose limit for events of a defined probability.

Moreover, to comply with the above mentioned criteria for operating conductions, the following inequality shall be verified:

$$\sum p_i \times d_i \leq 0.1 \text{ mSv/year}$$

where:

- $p_i$: annual event probability
- $d_i$: effective dose equivalent for the event
The continuous line represents the design targets for single accidents having a probability higher than $3 \times 10^{-2}$.

It has to be noted that, taking into account the margin related to design and licensing calculation models, the effective dose equivalent line versus event probability would be largely lower, as shown in the figure.

With regard to events beyond design basis accidents a design objective has been established in terms of maximum overall probability for the complex of sequences that could lead to core degraded conditions.
In selecting such a probability target, consideration was given to the available international positions and to the results of existing studies. In this regard, where evaluations for new plants or recent designs have been performed, they showed the actual possibility to obtain results better than $10^{-5}$, while the trend of some vendors was towards $10^{-6}$ per year.

On these bases an annual probability target of $10^{-5}$ has been fixed, with the additional aim of $10^{-6}$ to be addressed through the consideration of possible design alternatives, including the most updated, even without altering the general proven characteristics of the plant.

In order to verify compliance with the above established targets a Probabilistic Safety Study (PSS) is required.

PSS execution shall be interactive with the design development, since the verification is not considered as a final check of the design, but shall go on together with any important design choice. Moreover, the PSS shall allow the evaluation of the balancing among the different sequences leading to core degradation (each one of them should also not exceed 10 per cent of the overall probability). The PSS shall also allow the identification of possible areas where it might be considered appropriate or necessary to introduce an improvement in systems and components.

It is common knowledge that the results of probabilistic studies are strongly dependent on the way the studies are performed. In order to reduce this dependency, some guidelines have been given in the frame of the best available methodologies.

The methodology used for PUN/SPS is similar to that described as level 1 PRA in NUREG/CR-2300 "PRA Procedure Guide". The analysis considered only internal and area events, whereas external hazards, both natural and man made, were excluded. Success criteria were developed from transient and ECCS analyses using, as much as possible, realistic models and plant performance parameters: this last feature has to be noted as a significant difference between the PUN-SPS and Alto Lazio probabilistic assessment. Operator errors in procedure implementation, system
dependencies and common cause failures were also taken in due account.
Specific attention, through the use of suitable calculation methods, was
required for the contribution of common mode failures to system
unreliability. Moreover, also in order to stimulate the adoption of
diverse redundant systems, a minimum failure probability of $10^{-5}$ has
been established for any single safety function performed by individual
non-diversified systems.
A uncertainty analysis is not foreseen at the first stage of the project,
because of many design features not yet well defined and the
consequential conservative assumptions used (e.g., no repair of failed
components; no credit for manual actuation of systems when automatic
initiation failed). However, the PUN-PSS does contain a sensitivity study
aimed to assess the influence of specific plant parameters and
engineering assumptions used in modelling plant response and systems
behaviour.

An uncertainty analysis, which should be an integral part of any
probabilistic analysis, will be performed at a later stage of the
development of the project, when the design will be better defined. This
analysis can then serve as a base for further development of the project.

Results and experience gained

A first result of the PUN-PSS showed a core melt probability greater than
the upper limit of the reference range given in the GDC.
The weakest points in the design were discovered through sensitivity and
partial importance analysis, and plant design modifications have been
proposed in order to achieve the probabilistic goal.
Some of the main proposed modifications follow:
1) The SIS design was modified providing two redundant sump MOV's per
train, and interlocks with MOV's in miniflow lines of high-head pumps
were removed; moreover a new configuration of the system allows
quarterly testing during plant operation of the check valves common to
both low-head and high-head injection lines.
2) The RHR design was modified providing each suction line with a third MOV, normally open, which allows MOV quarterly testing during normal operation.

3) Modifications of NSWS, ESWS and CCWS are under consideration to improve availability of the fluid auxiliary systems.

4) Design alternatives of vital AC/DC Electrical SYstem are under consideration so to improve system availability.

5) A Back-up Protection System has been added to the original design. The system includes an alternate reactor trip function and actuates also the ESIS in the RCP seal injection mode and the EFWS.

6) Design changes associated with SG PORV control system have been introduced to avoid SG safety valve lifting during steam pressure transients with condenser unavailable, and to reduce the probability of a consequential stuck-open relief valve. The modification includes a direct reactor trip on condenser unavailable signal.

The combined benefit of the proposed changes have been evaluated by the designer and the results show that the probabilistic safety targets may be reached by their implementation. Area events contribution to the core Damage Frequency (CDF) has to be still evaluated, but could be balanced by the removal in the study of some hypotesis to conservative.

Final conclusion is, of course, subject to the validity of input assumptions when detailed design of the proposed changes will be carried out.

A review of the PUN-PSS has been also performed and as part of this review effort, an importance analysis has been carried out to identify the dominant contributors to the overall CDF. This analysis confirms that the proposed plant design modifications represent the optimum means of reducing the total CDF.

As already mentioned, the PUN-PSS shall be considered as an interactive tool to be developed and updated together with the design and on the base of the outcomings of the licensing process.
In this way the PUN-PSS appears as a "living schedule" continuously updated and therefore valid to evaluate the safety level of the plant and to support at any moment every decision.

On the basis of the result already gained, it was possible to single out a first set of methodological actions aimed to validate the assumptions made at the first stage of the study and to address eventual revisions. Some of the control points suggested by the PUN-PSS are described below:

1- Execution of the uncertainty analysis, when design, hardware and procedure are enough defined.

2- Review of the new SG design to define the effectiveness of certain provisions against SG tube failure (absence of adverse conditions which can favour certain failure mechanisms; effectiveness of the Quality Assurance Program during maintenance to avoid the introduction of loose parts in the primary and secondary circuits; the loose part detection system) and the validity of certain hypothesis assumed to define the SG tube rupture probability (confirmation of the hypothesis of linear degradation of the mechanical properties).

3- Reevaluation of the IPS reliability, particularly with regard to:
   - reliability of the software,
   - common cause failures,
   - effects of the electric supply quality,
   - effects of environmental conditions and their dependency from the auxiliary conditioning system,
   - effectiveness of the automatic tests and evaluation of influence of undetectable failures (such as sensor drifts or calibration errors) on the system unreliability on demand.

Future Prospects

Efforts in research on severe accidents and source term have recently been sped-up, with the cooperation of most countries involved in nuclear programs.
The existing recent studies have shown that a consistent improvement has been gained in the knowledge of severe accident phenomena and related consequence, and the possibility for the plants to cope with accidents much more severe than those ones considered in the design.

There is therefore the need for an understanding of how best to use these new findings and to what extent they are applicable to the regulatory process.

In response to this need the Italian regulatory body, with the support of external national organizations, initiated a specific study, whose expected outcome is a possible set of criteria for the reassessment of severe accidents and the definition of new source terms to be used for regulatory purposes.

To identify reference accident sequences for source term definition a probability target must be defined. Once dominant sequences leading to core melt have been identified, a conditional probability threshold upon core melt may be used. For instance, for a selected conditional threshold of 0.1, only those sequences will be selected whose overall probability (from the initiating event to external releases) is higher than 0.1 times the core melt probability.

In Italy the possible use of a 0.05 probabilistic threshold is now under consideration. This value may be motivated by consistency with the 5% reference value which is normally used for expressing "practical impossibility" in subjective probabilistic evaluations. It also includes consideration of a generally agreed upon field of phenomenological knowledge and of the very low probability of single events which could damage both reactor core and containment (such as very large earthquakes, big aircraft crashes, pressure vessel explosions), whose consideration for S.T. definition is not warranted.

For the quantitative assessment of the new source term the probability distribution of the various phenomena which take place inside the containment should be know (e.g., pre-existing openings, recovery actions such as components repair or use of alternative means, as well as fission...
products release and behavior). Where data are poor or incomplete, qualitative good-judgement may support the analysis.

A test exercise was recently performed in Italy on this matter. The selected plants are representative of the most common containment schemes. They are:

- Zion Large Dry CContainment PWR
- Peach Bottom MARK I BWR
- Limerick MARK II BWR
- Grand Gulf MARK III BWR.

Qualitative and quantitative evaluations led to neglect the most unlikely (also if less known thereotical phenomena), such as early containment failure due to steam explosion and hydrogen detonation, while consideration of pre-existing openings on the containment and recovery actions from the operator have been included.

For those sequence whose conditional probability upon core melt has been evaluated higher than $5 \times 10^{-2}$, the results indicate that iodine release fractions are always lower than $10^{-3}$ times the core inventory; also if other radionuclides were not included in the study, it is believed that similar results could be obtained for all radionuclides except noble gases which must be considered as almost completely released.

The above conclusion shall not be taken as an unconditional suggestion of generalized source terms for regulatory purposes. It only provides an example of a possible approach for a source term revaluation.

The exercise therefore needs to be further developed and should include both the consideration of more sequences and the specific use of advanced mechanistic models.

To conclude, it should be emphasized that probabilistic methodologies do not replace but integrate the traditional ones; on the contrary it should be mentioned their importance in the development or validation of deterministic criteria, and in this regard its application may also be considered to the redefinition of the design basis events to be assumed in the safety analysis.
REFERENCES

(1) A. Valeri - Revisione dello SPS del PUN - Parte 1 - DISP/SER
   Giugno 1985

(2) H. Filacchione et al. - Review of the PUN PSS - NUS Report - Sept. 1985

(3) M. Cozzone, A. Valeri - "Analisi per l'individuazione dei punti deboli del progetto basate sull'analisi di importanza - DISP/SER
   Sett. 1984
THE SWEDISH VIEW OF PROBABILISTIC SAFETY CRITERIA — PRESENT STATUS

L. CARLSSON*
Swedish Nuclear Power Inspectorate, Stockholm, Sweden

Abstract

Today we do not have a formal Probabilistic Safety Criterion. However, extensive use of PSA on all plants is promoted. The safety work in Sweden is divided into two areas: first, core damage preventing activities, and second, severe accident phenomena. In this paper the Swedish authorities' recommendation to the Swedish Government and an overview of the Swedish reliability evaluation program (ASAR — As-operated Safety Analysis Report) is included. The last part of the paper gives some results from Swedish PSA work.

I. ACTIVITIES FOR CORE DAMAGE PREVENTION

The Swedish reliability evaluation program

There are major efforts under way in Sweden, carried out in cooperation between the Nuclear Power Inspectorate (SKI) and the nuclear utilities and focussing on the use of reliability engineering as one of the more important tools to maintain and improve reactor safety. In this context, it is of course realized that preventing disturbances, incidents and accidents is essentially the same as promoting safe and reliable normal operation of the nuclear power plant.

Thus, a thorough plant-specific systems reliability analysis (PSA) will constitute a major part of the present Swedish recurrent safety analysis program. Within the framework of this program the Swedish utilities are required to prepare an "As-operated Safety Analysis Report" (ASAR) for each plant. According to directives given by SKI the ASAR should include a plant-specific PSA, which however, stops at core damage, not developing into a full-scope PSA.

Thus, plant specific system reliability analyses of all Swedish plants will be performed during the time period 1982-87 as a part of the ASAR program. The utilities are responsible for carrying out the analyses, and the

* Present address: Division of Nuclear Safety, International Atomic Energy Agency, Vienna.
Inspectorate will review the completed analyses. The results of each plant-specific safety review (utility ASAR and SKI review) will be reported to the Swedish Government.

This first phase of the Swedish national reliability evaluation program will have as an objective to increase the awareness of the capabilities, limitations and use of the reliability methods rather than develop principles for safety goal discussions. Some key elements is this reliability evaluation program are:

- very detailed, plant-specific fault and event trees developed and reviewed in close cooperation with senior plant operation and maintenance personnel, providing a detailed map of system functions and interdependencies and identifying sequences that are main contributors to the probability of core damage.

- extensive use of computer graphic techniques to facilitate detailed documentation, modification and analysis

- use to the greatest possible extent of actual component data from the Swedish reliability data bank for nuclear plants, which is continuously updated.

Thus, the principal objective of the Swedish program is to introduce reliability engineering for continuous use in the operation and maintenance of the plants e.g.

- establishing the basis for a systematic evaluation of operating experience when analyzing disturbances and incidents, keeping track of component and system reliability and their effect on plant safety

- planning and reviewing plant modifications

- training plant personnel in system functions and interdependencies facilitating their awareness of the safety significance of various operational and maintenance tasks.

Present Status of the ASAR program

The Swedish Nuclear Power Plants have all been taken into operation over a period of 13 years from 1972 to 1985. The ASAR program started in 1981 resulting in the first report to the Government in 1983 for the oldest plant Oskarshamn 1. The second in order was the Ringhals 2 plant a PWR. This year the ASAR for Barsebäck 1 and 2 and Ringhals 1 will be submitted to the Government.

At present Ringhals 1 is reviewed by SKI. The status of the different parts of the probabilistic safety analyses carried out is given in table below.
The external event analysis will follow given that the plant event trees and fault trees have been developed.

SKI has developed a database for storing and assessing fault trees for all Swedish Nuclear Power Plants.

The database will be used for safety evaluation and research activities. This will be described in other papers presented later this year.

**PSA and Safety Goals**

In Sweden, a very cautious approach is taken with regard to using PSA techniques trying to establish quantitative estimates of risk to public health and safety and associated safety goals. The reason behind this approach is that there are many difficult pitfalls to avoid in such full-scope PSA studies inter alia with regard to

- political acceptance, e.g. of the way various social consequences of large accidents are modeled
- acceptance by the statistical sciences community e.g. of assigning probabilities to phenomena about which little is known empirically, e.g. containment response in some types of core melt accidents
- possibility of "tunnel vision phenomena" by putting to much emphasis on good results from theoretical analysis and forgetting to check with actual plant conditions, e.g. with respect to quality of operation and maintenance (c.f. Salem incident).

The present philosophy in Sweden regarding quantitative safety or reliability goals is that calculations of absolute severe core damage frequencies cannot be used as a single criterion for safety evaluations.

On the other hand results from in-depth, plant-specific PSA:s could and should be used as a guidance. No formal reliability goals have been set up, but tentatively the following approach is discussed

- estimates of very low core damage frequencies (sa $10^{-6}$/year or less) only indicate that the system is well designed. The focus should then be on keeping a close watch on operation and maintenance, ensuring that actual components and systems reliability performance meet the levels used in the PSA

- estimates of core damage frequencies of the order of $10^{-4}$ and above should lead to considerations of system modifications as the risk on severe damage to the plant probably is to high both from the inspectorate's and the owner's point of view (loss of investment and of production capacity)

- severe damage to certain other parts of the plant than the core (e.g. pressure vessel or containment) should also be considered in future PSA:s.

Thus any safety and reliability goal considerations must be dynamic and must be given time to develop at the same time as a vigorous application of reliability engineering is promoted. The definition of formal, quantitative safety goals seems less important than the actual knowledge and safety awareness established within a highquality systematic reliability evaluation program at each plant. Only when a number of plant specific PSA:s have been performed with given and known levels of detail, relative comparisons seems appropriate between event sequences and later between plants.

Finally, it should once more be underlined that a close monitoring of operational experience is the best assurance of keeping operational safety high - and the only way of verifying PSA results and creating public confidence in them is shown in figure below.
II. ACTIVITIES FOR PREVENTING SEVERE ACCIDENT RELEASES

In letters to the Swedish Government, the Swedish Nuclear Power Inspectorate (SKI) and The National Radiation Protection Institute (SSI) propose improved protection against releases in the case of a severe accident for the nuclear power plants in Forsmark, Oskarshamn and Ringhals. The proposed requirements are based on reviews of plant-specific severe accident studies submitted by the plant owners in April, 1985. Some main points in the proposed requirements are:

- Improved protection against early and direct damage to the containment in the case of a core melt. Measures proposed by the owners include improved protection of particularly exposed penetrations and support structures, as well as installation of additional equipment enabling rapid flooding of the lower dry-well in the Forsmark 1-3 and Oskarshamn 3 BWR's.

- All containments should be provided with devices for pressure relief, protecting the containment against the major number of such beyond-design-basis events that may lead to loss of containment integrity due to overpressure. The relief devices should be so designed that they can function independently of operator action and of other safety systems.
if the containment design pressure is substantially exceeded. In addition, operators should be able to use the relief devices actively as a part of accident management actions. The relief devices should be so designed that they, together with other safety systems (e.g. containment sprays), ensure with high reliability that releases to the environment are kept below 0.1 percent of radionuclide inventory in a 1800 MW(th) core, noble gases excluded, and with some regard to how various radionuclides contribute to radiation risks, especially ground contamination. Appropriate measuring equipment should be provided to enable prediction and monitoring of releases through the relief devices.

- The improved protective measures against releases in the case of a severe accident should be implemented by Sept. 1, 1989 at the latest.

The release protection level required for the Forsmark, Oskarshamn and Ringhals plants is equal to that required for the Barsebeck plant with its Filtra filtered vent system, which became operational in November, 1985. However, alternative technical solutions to the large Barsebeck filter may be envisaged, according to the SKI-SSI review report. Such alternative technical solutions are presently being discussed with the utilities concerned and include:

- Large area, unfiltered and reclosing relief systems to cope with dry-well to wetwell isolation failure in combination with a LOCA in BWR pressure suppression containments, thus preventing containment damage which, in turn will probably cause failure of core cooling in such sequences.

- Improved containment spray systems.

- Small area venting systems with retention devices such as scrubbers or filters to provide long term pressure control in the containment.

The proposed requirements are based on the general severe accident policy guidelines issued in 1981 by the Swedish Government and Parliament. These guidelines put a high priority on prevention of extensive ground contamination in order to limit social consequences in the case of a severe reactor accident. This priority is the main basis for the 0.1 percent release limit, which also provides good margins against acute radiation illness and fatalities.

In addition to these general policy guidelines, SKI and SSI inter alia states the following in their review report as a basis for the proposed requirements:

- The primary safety objective is still to prevent core damage. This preventive safety level has improved in Swedish reactors in the past five years due to safety-enhancing measures implemented on the basis of operational experience and plant-specific PRA's. Also, the safety level is better known. Nevertheless, it must be taken into account that severe accidents can occur.

- There is substantially improved knowledge on severe accident phenomena, indicating that containments have good capabilities to withstand severe accidents, provided that "weak spots" identified in design-spe-
pecific studies, are strengthened. Furthermore, design-specific accident management strategies should be prepared, aimed at protecting the containment function, and, in the long term, at reaching a stable plant state with the damaged core cooled in a containment at normal pressure and possibly filled with water above the level of the damaged core.

- Even if theoretical calculations indicate a fairly low probability for large releases, it does not appear reasonable to let a containment with a damaged core remain at elevated pressures - perhaps exceeding the design pressure - for extended times. Firstly, diffuse leakage of radioactivity to auxiliary buildings, etc. may create serious problems for accident management actions bringing the plant to a stable state. Secondly, there are, and will probably remain, uncertainties about containment failure pressures and failure modes (e.g. leak before break) as well as about the behaviour of various radioactive substances during a wide range of possible severe accident conditions. Thirdly, it must be recognized that a containment with a damaged core and in a state characterized by elevated or increasing pressure will create difficult decision making and public information problems for the emergency management authorities.

A Swedish Government decision on the proposed requirements is expected early in 1986.

Some general results from performed PSA studies

Major improvements in plant safety have taken results from the ongoing program. That benefit has fallen out from identification of peaks in accident sequence frequencies and a general improved understanding of reactor safety from a probabilistic point of view.

Results from analysis of older plants show higher relative peaks on the LOCA scenarios than the ones from analysis of newer plants with internal main circulation pumps.
Older plants are also less electric separated and have not been designed for some of the external events.

The estimates on the operator teams' probability of performing a correct action when needed are overall very rough. In the newer plants with four redundant trains the fourth train has not received any credit due to CCF judgment. The distributions and point estimates of medium and large LOCAs as initiating events are arbitrary internal values. This all together makes it difficult to compare results from one analysis to another without redoing some parts in each study. These considerations underline that the first step is to reduce peaks in accident sequence estimates. Comparison of one plant to another will take place but at a later stage. The methodology used today shows big differences from one plant PSA to another. So, in the meantime, ranking of safety improvements is made with pairwise developed merit numbers based on core melt probabilities and consequences as well as time for improvement and the cost of improvement.
DEVELOPMENT OF THE NON-DIMENSIONAL
METHOD OF RANKING RISKS

J.C. CHICKEN
J.C. Consultancy Limited,
Godalming, Surrey, United Kingdom
and
John C. Chicken Consultancy GmbH,
Langenargen, Federal Republic of Germany

M.R. HAYNS
Safety and Reliability Directorate,
United Kingdom Atomic Energy Authority,
Culcheth, Warrington, Cheshire,
United Kingdom

Abstract

This paper presents a critical review of the progress that has been made in the development of the risk ranking technique. The aim of the development of the technique has been to produce a method of making a comprehensive assessment that takes into account the technical, economic and socio-political factors involved in determining the acceptability of a risk.

The paper shows how the ranking of the risks associated with two major projects can be determined. The process of building up the ranking includes a critical examination of the data available and the methods used for deriving the ranking from such data.

The paper is divided into three parts. Part one examines in general terms the data that is likely to be available for ranking acceptability. Part two demonstrates by ranking the Moss Morran liquefied energy gas facility and the liquefied natural gas facility proposed for Eemshaven how the technique can be used in practice. Part three assesses the efficacy of the technique in its present state of development and reflects on the possible future role of the technique. The future uses suggested for the technique include both as an aid to regulatory policy making and as a management tool.

1. INTRODUCTION

This paper examines the practical problems associated with applying the method of ranking the acceptability of risks which was described in a paper presented at the 1984 Annual Meeting.\(^1\) The incentive for the development of the technique is to produce a unified, non-emotive, non-dimensional and easily understood way of describing the acceptability of risks. In this paper the ranking of two projects is built up by assessing their overall acceptability in terms of the associated technical, economic and socio-political factors. These factors provide an overall assessment of the acceptability of the risks inherent in a proposal.
The range of factors that have to be considered depends largely on the purpose for which the ranking is to be used. Only when the ranking is used for overall policy decisions do all the factors have to be taken into account. The ranking is determined by integrating the scores associated with the relevant factors, the scores allocated being an assessment of the acceptability and uncertainty of each factor. The scoring is built up in whole numbers as this reflects with sufficient sensitivity the precision with which each factor can be determined. Table 1 shows how the scores are related to the ranking and the type of control action likely to be associated with each level of ranking.

### Table 1: Definition of Rank Acceptability and Control Action

<table>
<thead>
<tr>
<th>Risk Rank</th>
<th>Acceptability of Proposal</th>
<th>Total Score Allowable for Each Rank</th>
<th>Maximum Allowable Score for Each Ranking Factor (Technical, Economic, and Socio-Political)</th>
<th>Control Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unlikely to be acceptable</td>
<td>&gt;6 - 12</td>
<td>4</td>
<td>Unlikely any possible</td>
</tr>
<tr>
<td>2</td>
<td>Only acceptable if risk can be reduced</td>
<td>&gt;4 - 6</td>
<td>3</td>
<td>Administrative and engineering</td>
</tr>
<tr>
<td>3</td>
<td>Yes subject to certain action</td>
<td>&gt;2 - 4</td>
<td>2</td>
<td>Engineering</td>
</tr>
<tr>
<td>4</td>
<td>Yes without restriction</td>
<td>0 - 2</td>
<td>1</td>
<td>None</td>
</tr>
</tbody>
</table>

The practical problems involved in applying the ranking method are examined in three steps which are: the data required, ranking the acceptability of the British Moss Morran and the Dutch Rijnmond decisions, and, finally, to assess the efficacy of the technique, its more general uses and possible future developments.

2. **Data for Ranking**

The technical, economic and socio-political groups of data which have to be assessed are each quite different in nature.

Understanding the technical group of data is essential to evaluating the nature and acceptability of a risk. Ranking the technical aspects of risks can also have many other uses. It can for example be particularly useful for identifying priorities for allocation of resources to various activities such as design, modification and maintenance. In the nuclear industry quantified assessments of the technical aspects of risks have been widely used. In one definitive study of probabilistic risk assessment (MUREG 1050) a clear indication of the uncertainty associated with such studies is given by statements that estimates of the frequency
of nuclear reactor core-melt may differ by two orders of magnitude and that estimates of the likelihood of operator error may deviate by an order of magnitude. The magnitude of these uncertainties led to some interesting conclusions about the usefulness of quantitative risk assessment, the conclusions are:

"Probabilistic Risk Assessment results are useful, provided that more weight is given to the qualitative and relative insights regarding design and operations, rather than the precise absolute magnitude of the numbers generated.

It must be remembered that most of the uncertainties associated with an issue are inherent to the issue itself rather than artifacts of the Probabilistic Risk Assessment Analysis. The Probabilistic Risk Assessment does tend to identify and highlight these uncertainties, however.

Probabilistic Risk Assessment results have useful application in the prioritization of regulatory activities, development of generic regulatory positions on potential safety issues and the assessment of plant-specific issues. The degree of usefulness depends on the regulatory application as well as the nature of the specific issue."

"The basic attributes of a Probabilistic Risk Assessment are not highly compatible with a safety-goal structure that would require strict numerical compliance on the basis of the quantitative best estimates of Probabilistic Risk Assessment. However, there could be useful application if the structure were less strict or the goals were set so conservatively that there would be little regulatory concern if the actual value substantially exceeded those goals.

The results of a Probabilistic Risk Assessment should only be one consideration in regulatory decisions, i.e., they should not replace other conventional considerations."

These conclusions draw attention to two very important findings. First, they accept that the significance of a risk will not be known accurately and the allowance for uncertainty is not generally adequate so there is a need to develop a comprehensive way of allowing for uncertainty. Secondly, they confirm that decisions about risk acceptability are in practice made partly in qualitative and relative terms.

Further indication of the range of uncertainty that can be associated with estimates of risk is given by the results of a study of decision making and risk analysis in relation to the siting of liquefied energy gas facilities. The study argued that for most risk estimates the range of uncertainty is at least $10^2$. To emphasise that $10^2$ may be the minimum range of uncertainty attention is drawn to two figures from the study. They are both estimates for the probability of an internal system failure, one is $3.2 \times 10^{-3}$ and the other is $1.0 \times 10^{-11}$. Such a wide difference shows dramatically how great the uncertainty in risk estimates can be.

The conclusion about the technical data that seems to be justified is that the data likely to be available is bound to contain an element of uncertainty. An understanding of the magnitude and significance of the uncertainty is essential for the assessment of the acceptability of a proposal. It is in dealing with uncertainty in risk assessment that the ranking technique can be particularly helpful.
In our everyday lives we are all conscious of the financial significance of variations in our expenditure. With major projects the variation in cost can be many millions of pounds. In NUREG 1050 it is shown that the total financial risk for a pressurized water reactor with certain safety modifications is between $5 \times 10^5$ and $8 \times 10^7$ dollars per plant lifetime.\(^{(2)}\)

The US Nuclear Regulatory Commission had a study made of the socio-economic consequences of nuclear reactor accidents. Many of the findings of the study are applicable to any major industrial risk assessment. The study stressed the uncertainties in predicting the economic impact of an accident and suggested that economic losses will mainly be in the form of loss of property, loss of life, loss of business and production and increased taxes.\(^{(4)}\) One important implication of the variability in the economic argument is given by the statement: "We can reduce the risk in any sector provided we are prepared to pay the cost."\(^{(5)}\) This exposes the concept of opportunity cost which underlies many economic decisions. Ranking may help such decision making.

There are clear indications from the study of the siting, mentioned earlier, that the authorities responsible for deciding about the acceptability of sites attempt to take into account the need for economic development in the area surrounding the proposed site.\(^{(3)}\) But there are no universally agreed ways in which such factors are taken into account and this fuzziness in the economic argument shows the need to evaluate the uncertainty in the figures when determining the ranking.

In an earlier study of the correlation between expenditure on life saving and the public's perception of risk the following conclusions were drawn:\(^{(6)}\)

1) There is some indication that the level of expenditure on risk reduction is more related to people's perception of risk than to estimates of the probability of the risk.
2) There are indications that policy makers are willing to contemplate higher levels of expenditure to reduce involuntary accepted risks than for voluntarily accepted risks.
3) The value of life for compensation purposes often seems to be put at about £200,000, but there is a considerable range in the valuations.
4) The range of cost of saving an extra statistical life (often referred to as the CSX value) used is from £0 to $2 \times 10^6$. For many decision situations the values used are in the range £10^4 to £10^5.
5) The cost of action to save a life is sometimes higher than the compensation paid for loss of life.

In a more recent study of the way human life is valued for various purposes attention is drawn to the view that life insurance does not really value life but just amounts to saving to provide for dependants or the future.\(^{(7)}\) The values of human life reported in ref 7 range from £1 x 10^3 for a child-proof drug container to £20 x 10^6 for a change in British building regulations.

The conclusion that seems to be justified about the economic data is very similar to the conclusion about the technical data, namely that there is a wide range in the data used and this uncertainty must be taken into account in determining the ranking score.

At the heart of assessing socio-political factors is determination of public opinion. Before any attempt can be made to assess public
acceptability of a major project the technical nature of the risks involved must be identified and described in a way that is understandable by the public concerned.

Public opinion can be assessed by polls but the results of such polls are not permanent, public opinion is fickle and opinions do change. Dr Keyes, a Director of the Westinghouse Electric Corporation, has summarized the roll of polls in the following incisive way: (8) "Certainly, the techniques are not perfect. Sometimes the pollster errs; sometimes, his client. Nevertheless, polling is one of the most important tools available in measuring public attitude on certain issues in order to ascertain the public will which, in the long run, will find expression in the actions of government in a democratic society."

Provided public opinion is carefully assessed it is possible to obtain some indication of the nature of possible opposition. If the opposition is based on a lack of information or on a misunderstanding of information given, it is possible by judicious publicity and education processes to reduce opposition, but such processes can take a considerable time. (9)

The conclusion about socio-political data that seems to be warranted is that although a great diversity of views are involved there are survey techniques available that enable opinions to be ranked in a way that correlates directly with the ranking technique proposed.

3. DEMONSTRATION OF THE APPLICATION OF THE RANKING TECHNIQUE

To demonstrate how the ranking technique may be applied in practice two well known cases, Moss Morran and Rijnmond, that have caused a certain amount of controversy and on which the decision process is now complete were assessed.

3.1 THE MOSS MORRAN FACILITIES AND PIPELINE

The Moss Morran liquefied energy gas terminal facilities and pipeline were planned as part of the facilities required to exploit the Brent oil and gas field in the North Sea. The proposal was that the oil and gas should be brought ashore by pipeline at St Fergus and then after some processing transmitted down to the Firth of Forth area for processing after which they would be transported mainly by sea to their destination.

There were three main steps in the process leading to outline permission being granted.(3) Step 1 was Shell and Esso formally lodging planning applications to develop a processing facility at Moss Morran and a storage and shipping terminal at Braefoot Bay. Step 2 included the Secretary of State for Scotland calling for the decision to be made at central rather than local government level, a public inquiry into the acceptability of the proposal being held, local government authorities publicising the fact that the planning applications had been lodged and describing the general nature of the proposals, the local authorities asking a firm of consultants to advise them on the hazards involved and the environmental impact of the proposals and the directors of planning of the local authorities concerned preparing a report on the socio-economic impact of the proposal. The conclusion of Step 2 was marked by the Secretary of State receiving the report of the public inquiry. The final step, Step 3, started when it was found that the public inquiry had exposed differences in views and concern about the possibility of a vapour cloud being ignited by radio frequency transmissions. The
Secretary of State invited written comments on the subject. It was finally concluded from tests that radio frequency transmissions were unlikely to produce sufficient power to reach the minimum required for ignition. In August 1979 the Secretary of State announced he would grant outline planning permission.

The risks associated with the pipeline from St Fergus to Moss Morran were assessed by the Health and Safety Executive in 1978 and again in 1980 when it was proposed to increase the pipeline size from 16-inch to 24-inch diameter. The assessment showed that the chance of leakage from the pipeline people in the area of the pipeline at risk fell in the range 1 to 4 \times 10^{-6} per year. The report advised: "...the level of risk would not be such as to lead to a recommendation that a Construction Authorisation should be withheld on health and safety grounds".

Although the consultants made consequence analysis calculations they expressed the results in qualitative terms like low, very low or extremely low and gave no estimate of the possible number of fatalities. The Action Group estimated that the probability of an individual fatality was 7 \times 10^{-4} per year. The one hazard figure that seems to be very high is the shipping hazard figure. The same figure of 10^{-3} per year appears to have been used in the assessment of the acceptability of Eemshaven, Braefoot Bay and Wilhelmshaven despite the three ports having very different traffic patterns. This apparent statistical anomaly has been adversely commented on in reference 3.

TABLE 2 RANKING FACTOR SCORE FOR MOSS MORRAN

<table>
<thead>
<tr>
<th>FACTOR</th>
<th>SCORE</th>
<th>JUSTIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHNICAL</td>
<td>2</td>
<td>All the advice, which was a mixture of qualitative and quantitative assessments suggested the proposals were acceptable subject to detailed justification. The installations are similar to those accepted in other parts of the world.</td>
</tr>
<tr>
<td>ECONOMIC</td>
<td>1</td>
<td>National Energy Policy required the Brent Oil and gas field to be exploited. The financial risks of the operation were undertaken by private companies and were consistent with the scale of risk they undertook in other parts of their work.</td>
</tr>
<tr>
<td>SOCIO-POLITICAL</td>
<td>1</td>
<td>The proposals were accepted at Government level but the Secretary of State made it a condition that he was satisfied with the safety audit. The opposition to the proposals was essentially of a limited local nature.</td>
</tr>
<tr>
<td>TOTAL SCORE</td>
<td>4</td>
<td>So a risk rank 3 was justified.</td>
</tr>
</tbody>
</table>
Official concern about the safety and risk justification of the Moss Morran site is indicated by the conditions that were attached to the outline planning permissions granted to Shell and Esso. Nearly 50 conditions were attached to each permission, the most important condition from the safety point of view being the requirement that a full hazard and operability audit should be conducted before the facilities would be allowed to be commissioned. The importance attached to the audit is indicated by the fact that the Secretary of State decided the audit must be to his satisfaction and not just to the satisfaction of the Health and Safety Executive.

From the information above it is considered that the risk ranking that can be justified for Moss Morran is 3. The construction of the ranking is shown below in Table 2. With the benefit of hindsight the ranking of the Moss Morran proposals shows that they are acceptable subject to certain conditions being satisfied.

3.2 THE RIJNMOND DECISION

The history of the Rijnmond Decision is complicated and has its origins in the early 1970's when plans were made to import large quantities of liquefied natural gas (LNG) from Algeria. Eight possible sites for the LNG terminal were considered. The two main contenders were Rotterdam and Eemshaven.

The discussion that took place about which was the most acceptable site has been divided into three rounds. Round A was the period up to the final signing of the contract for the supply of LNG and included the preliminary search for a terminal site. Round B involved the cabinet and several government departments and at this stage it was recognized that siting involved several issues such as energy policy, the environment, safety, land use and regional planning. At the beginning of this round Rotterdam was the preferred site and discussions were held with the local authorities in the region. These discussions showed that these local authorities, particularly the Rijnmond Public Authority were likely to apply stringent safety requirements to any LNG terminal. The involvement of Rijnmond Public Authority is the reason the decision became known as the 'Rijnmond Decision'. Round C was the final round which ended with the cabinet deciding in favour of Eemshaven. During this period there were formal council debates and public meetings. The views of the local authorities were presented to the cabinet in June 1978. In addition to the local authorities, trade unions were in favour of Eemshaven. The environmentalist groups, Shipowners Association and Electricity Corporation were against Eemshaven. In August 1978 the cabinet announced its preference for Eemshaven primarily on socio-economic and regional industrial grounds. The decision was debated at considerable length in Parliament and finally approved in October 1978.

The view has been expressed that in part the reason that the decision went in favour of Eemshaven was that the Governor of Groningen was a skillful politician and a longstanding member of one of the parties in power. On this basis the final decision appears to have been guided by past political constraints than by consistent government policies.

For a major accident it was predicted that the number of deaths and casualties would be ten times lower for Eemshaven than for Maasvlakte, but such differences are not really very important.

131
On the basis of this evidence it was possible to rank the acceptability of the risks associated with the sites. The Maasvlakte site was given a rank 3 and the Eemshaven site was given the more acceptable rank 4. The construction of the Eemshaven ranking is given in Table 3.

**TABLE 3 RANKING FACTOR SCORE FOR THE EEMSHAVEN SITE**

<table>
<thead>
<tr>
<th>FACTOR</th>
<th>SCORE</th>
<th>JUSTIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHNICAL</td>
<td>1</td>
<td>Probability of a major accident put at $5 \times 10^{-8}$ and the increase of risk of individual death $&lt;3 \times 10^{-7}$, this is why a lower score than Maasvlakte is justified.</td>
</tr>
<tr>
<td>ECONOMIC</td>
<td>1</td>
<td>Benefit to the development of the area. Risk the same as the other site.</td>
</tr>
<tr>
<td>SOCIOPOLITICAL</td>
<td></td>
<td>The site was accepted. Political support for the site. Trade union support for the site.</td>
</tr>
<tr>
<td>TOTAL SCORE</td>
<td>2</td>
<td>So a rank 4 is justified.</td>
</tr>
</tbody>
</table>

3.3 ASSESSMENT OF THE RANKING

The information available was adequate to show that the ranking technique gives a clear and comprehensive evaluation of the acceptability of a proposal. The process of constructing and justifying the ranking scores exposes very clearly the strengths and weaknesses of the evidence on which the assessment of acceptability has to be based.

The technical factor evidence showed considerable differences between the two cases considered. One very important difference was between the qualitative evidence about risks presented by the consultant used for Moss Morran and the quantitative evidence used to compare the Maasvlakte and Eemshaven sites. If there had only been qualitative evidence about the risks associated with Moss Morran any ranking of acceptability would have been questionable. There was, however, some quantitative data, which included estimates of pipeline failures, the risk of a shipping accident and estimates of fatalities. Also, it was possible to estimate the order of the risk by comparison with the estimates of the risks made for other similar installations and this gives some confidence in the acceptability of the risk.

Nevertheless from the study Kunreuther et al made of four similar plants in four different countries some criticism of the differences in the analyses used in such cases appears justified. In five of the eight risk assessment reports involved there was no mention of the uncertainties associated with the final findings, so it was not clear whether the results were mean, maximum or minimum values.

Another way the ranking of the technical factors can be justified is by comparison with the steps in the Ashby criteria, as shown in Table 4.
TABLE 4  TECHNICAL RANKING AND THE ASHBY CRITERIA

<table>
<thead>
<tr>
<th>RISK RANK</th>
<th>ACCEPTABILITY</th>
<th>TECHNICAL SCORE MAXIMUM</th>
<th>ASHBY CRITERIA (RISK OF DEATH PER YEAR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UNLIKELY TO BE ACCEPTABLE</td>
<td>4</td>
<td>Unacceptable (one in 1000)</td>
</tr>
<tr>
<td>2</td>
<td>ONLY ACCEPTABLE IF RISK CAN BE REDUCED</td>
<td>3</td>
<td>Willing to spend money to reduce risk (one in 10,000)</td>
</tr>
<tr>
<td>3</td>
<td>YES SUBJECT TO CERTAIN ENGINEERING ACTION</td>
<td>2</td>
<td>Warnings given (one in 100,000)</td>
</tr>
<tr>
<td>4</td>
<td>YES WITHOUT RESTRICTION</td>
<td>1</td>
<td>Acceptable (one in a million)</td>
</tr>
</tbody>
</table>

The assessment of the acceptability of the economic factors associated with the two cases considered is perhaps the weakest part of this ranking exercise as there was not a great deal of direct evidence available. The assessment of acceptability was based, mainly, on the fact that the installations in some way or other formed part of the national fuel policy of the countries they were built in and that the risks were of a type normally accepted by the companies involved. If the companies had been unused to dealing with such risks, doubts about the acceptability of the economic factors would have existed.

Scoring of the acceptability of the socio-political factors was in this study somewhat simplified as the ultimate decision was known. However, sampling techniques exist for determining the attitudes of the relevant populations. Studies have also been made which have identified the basic underlying value structures in different cultural groups. Knowledge of such basic value structures can be particularly helpful in determining likely public reaction to controversial issues.

The conclusions that seem to be justified about the ranking technique are that it gives an overall assessment of all the factors that have to be considered in determining the acceptability of a potentially hazardous installation, no other method gives such a comprehensive assessment of all the factors involved, and the technique identifies those issues that are likely to generate the most concern about a proposal.

4. THE CURRENT STATUS OF THE DEVELOPMENT OF THE RANKING TECHNIQUE

Now to examine some of the other uses that have been made of the technique, the problems with the technique and possible future developments.

4.1 CURRENT USES OF THE TECHNIQUE

Two specific uses of the technique that have been made are to assess the acceptability of the transport of potentially hazardous materials and to make a preliminary assessment of the current acceptability of buildings for the storage of irradiated nuclear fuel.
In assessing irradiated nuclear fuel transport the technical consequences of possible accidents led directly to assessment of the economic factors. The economic assessment had to take into account the possible potential loss of revenue and the possible claims for compensation. Assessing the potential loss of business both in the short and long term led to the assessment of the socio-political factors. An accident to a nuclear fuel cargo could have an adverse effect on the nuclear industry and the significance of such an event had to be assessed. The experience gained in this assessment showed clearly how building up the ranking of an activity exposes weakpoints in the argument and data used and indicates where improvements can most effectively be made.

A preliminary ranking of the acceptability of an irradiated nuclear fuel store about twenty years old was made. This necessitated consideration being given to the possibility of age defects in the buildings causing risks in addition to the other risks.

Taken together these two applications of ranking indicate something of the range of possible uses for the technique. There is also interest in the development of the technique from government and intergovernment organisations. The attraction they see in the technique is that it presents a genuine comprehensive assessment of the acceptability of a proposal in a way that may help to eliminate unnecessary public debate about its acceptability.

Quite apart from these developments the Dutch Directorate-General of Labour has made use of a simplified form of ranking in their guidance on the classification of hazardous areas in relation to the installation and selection of electrical apparatus where there is a gas explosion hazard. They identified four types of zone, which are: Zone 0 which is a hazardous area in which an explosive atmosphere is continuously present or present for long periods. Zone 1 which is a hazardous area where an explosive atmosphere is likely to occur in normal operation. Zone 2 which is a hazardous area where an explosive atmosphere is not likely to occur and if it does occur will only exist for a short time. The fourth type of zone is a non-hazardous area.

4.2 PROBLEMS WITH THE RANKING TECHNIQUE

The problems with the technique are mainly associated with the adequacy, relevance and accuracy of the data that has to be used. Ideally for the ranking of proposals to be comparable the quality and comprehensiveness of the data used to rank each proposal should be the same. In practical terms perfect data is rarely available and some compromise has to be made.

When a proposal is being ranked or assessed doubts about the accuracy of the data used must exist and the only way to overcome this problem is to revise the ranking as better data becomes available. For major projects the ranking would, in general, be reviewed several times as they progress from conception to completion. This iterative development and review of ranking enables allowance to be made for: changes in the accuracy of the data, changes that take place in the relative significance of the hazards considered, changes in design, and operational changes.

4.3 FUTURE DEVELOPMENTS

It is intended to apply the technique to ranking the acceptability of a wider range of projects including the assessment of the acceptability of
a major new project. The testing of the technique will be aimed at
determining its efficacy both as a management and as a regulatory tool.

In future applications of the technique it is hoped to develop a more
consistent approach to the assessment of the various factors,
particularly in the way uncertainty in the data used is allowed for. It
may be that two forms of the technique are required, one for management
purposes and the other for regulatory purposes. The management form
would consider mainly the technical factors and those aspects of economic
and socio-political factors that impinge on corporate objectives.

The regulatory form would be a comprehensive assessment and would
certainly include the acceptability of the proposal to the workforce, an
assessment of the way the project satisfies national safety standards,
and an assessment of the financial and technical capability of the
organization concerned to undertake all the obligations associated with
the project. The two forms of ranking could be linked with management
ranking being regarded simply as the first stage ranking and the
regulatory ranking as the final ranking.

5. CONCLUSIONS

We believe that the study shows that the risk ranking acceptability
technique that has been developed is a useful tool in two important ways.
First it can be tailored to a variety of management and regulatory
evaluation needs ranging from a purely technical assessment to a
combination of technical, economic and socio-political assessments. Used
in these ways the technique can show the action required and how
resources may be most effectively allocated. The second way the
 technique can be used is for presenting to the public an easily
understandable assessment of complex risk issues. Used in the latter way
the technique has the potential for reducing the amount of discussion
often involved in arriving at decisions about the acceptability of
controversial projects.

REFERENCES

1) Chicken, J. C. and Hayns, M. R., A Multi-Factor Criterion for Risk
Acceptability, a paper presented at the 1984 Annual Meeting in
Knoxville USA of the Society for Risk Analysis.

2) NUREG-1050, Probabilistic Risk Assessment (PRA) Reference Document,

3) Kunreuther, H. C. and Linnerooth et al, Risk Analysis and Decision

4) NUREG/CR-3566 PNL-4911, Socioeconomic Consequences of Nuclear
Reactor Accidents, The Nuclear Regulatory Commission, published

5) Kunreuther, H. C. and Ley, E. V. (Editors), The Risk Analysis
Controversy, An Institutional Perspective, Springer-Verlag, Berlin,


10) Health and Safety Executive Report of the Steering Committee on radio frequency ignition hazards at St Fergus, Scotland, February 1979.


A METHOD TO INCORPORATE UNCERTAINTY AND
DEGREE OF COMPLIANCE IN SAFETY GOALS

M.R. HAYNS, S.D. UNWIN
Safety and Reliability Directorate,
United Kingdom Atomic Energy Authority,
Culcheth, Warrington, Cheshire,
United Kingdom

Abstract

We propose a method for the construction of quantitative regulatory safety goals that are compatible with current risk assessment and uncertainty evaluation techniques. The concept of 'degree of compliance' is introduced in order to reflect the vagueness inevitably attached to any reasonable notion of 'safety' underlying a safety goal. The logical and general procedure for comparing risk assessment with safety goal produces data in a convenient and transparent format designed to facilitate regulatory decision making.

1. Introduction

One essential element required of a safety goal is that it is couched in terms compatible with the capabilities of the methods used to assess compliance with it. Many detailed examples of such compatibility have been discussed. Some of the more obvious are:

1. whether to use biologically average or "worst risk" cases.

2. whether the risk estimates are based on "best estimate" or conservative assumptions.

3. whether the mean or median values of distributed quantities should be specified.

In these, and many other cases, the problem is merely one of choice, followed by the requirement that consistency with this choice be maintained. In other cases, more detailed justification of particular choices may be required. This is especially true if choices of particular computer codes are to be made and their use is to become mandatory in demonstrating compliance.

A further question that must be addressed is that of the connection between design criteria and safety goals. There is clearly a significant difference in both conceptual and practical approaches to the two. Design criteria (at least in the U.K.) are set to give plant designers targets to aim for when confronted with the task of providing necessary safeguards.

* Currently attached to Sandia Laboratories, Albuquerque, New Mexico, United States of America.
equipment and in assessing the capability of the plant to withstand abnormal operating conditions. Safety goals, on the other hand, have been concerned almost entirely with the public health hazards arising from "beyond design basis" accidents; i.e., accidents in which the designed-in capabilities of the equipment are exceeded and severe consequences could ensue. The very term "beyond design basis" highlights the difficulty since no account of such eventualities is considered in the design targets criteria approach. We recognize that a connection must be made between these two approaches both for the sake of consistency of methodology and interpretation in the technical community.

The purpose of this present paper is to discuss the general area of compatibility in the two senses considered above. The vehicle for this is a proposed method for expressing both the safety criterion and the results of a risk analysis in forms which allow comparisons to be made both logically and in line with the nature of the data available. In addition, the method permits a logical connection between the design basis and the beyond design basis aspects of the problem.

2. The Nature of Uncertainties and Compatibility between Criteria and Results

It is fundamental to the evaluation of the response of a complex plant to accident conditions that the results of any computations will have uncertainties associated with them. Whether the calculations are intended to determine the reliability, availability, and capability of plant in a design basis sense or to determine the risk posed by severe accidents in a plant, the same fundamental problems arise, although in these two cases, the scale and implications of the uncertainties may be quite different. For safety goal applications, the methods of Probabilistic Risk Assessment have proven to be appropriate and our present discussions of uncertainties will relate to 'uncertainties in PRA' although the methodology to be developed is accessible to straightforward generalization beyond the PRA domain. The differences in the nature and treatment of uncertainties in the deterministic approach commonly used for design basis assessments is a topic worthy of a separate assessment. A current review of the quality of uncertainty analysis now available within PRA[1] gives us confidence that bounds can be defined sufficiently well for the needs of assessment criteria.

Many related and unrelated quantities go to form the overall uncertainties in the final result. These may be broken down into:

1. Statistical: Projecting the expected performance of plant items into the future from a data base of similar components, is at the heart of any reliability assessment. Such questions as the size and applicability of the data base, and the intended use and maintenance procedures for the components, introduce varying degrees of uncertainty.
2. Common Mode and Common Cause Failures: Possible events or factors which may affect many items of plant simultaneously are notoriously difficult to identify and quantify. Quality control of batch produced components, faulty maintenance applied to more than one component, physical 'closeness' of components and, in the extreme, external events such as aircraft impact all have the potential to render inoperative, redundant items of plant, no matter how many are provided.

3. Human Factors: It is difficult also to quantify the influence of human beings on plant performance, either through mitigating actions or through errors of omission or commission. Since it is inevitable that 'operator actions' have to be included in the assessment of plant performance, this feature alone may introduce significant uncertainties.

4. Physical and Chemical Modeling: Having established the likelihood of exceeding the normal operating envelope of the plant, it is then necessary to determine the plant response. In a PWR, for example, this involves calculating the thermal hydraulic conditions in the primary and/or secondary circuits, establishing whether success/failure criteria have been met (e.g., on peak clad temperature) and, in those rare events where complete loss of heat rejection occurs, of how the core melts and releases its inventory of fission products to the environment. Clearly, such computations cannot be made with precision and, indeed, for the less likely but more severe events, a great deal of judgment is incorporated into the evaluation.

These four illustrative examples (there are more) are used only to show that the calculated risk from a reactor can never be precise. Indeed, there are some instances in which it is not even possible to quantify the degree of uncertainty attached to the result. For example, one cannot assign confidence bounds to uncertainties due to possible 'incompleteness' since the phenomena and possibilities not included in the analysis may be unknown. This problem is usually circumvented by arguing that experience and judgment would lead us to believe that such uncertainties are small. However, in the main, the principal uncertainties in the analysis may be quantified and the results expressed in the fashion provided by probability theory. This last statement covers many detailed difficulties concerned with, for example, the manner in which uncertainties arising from disparate sources should be combined. Such difficulties have been addressed recently[2] and must be detailed in any guidance to analysts supporting any proposed safety goals.

It is generally accepted that PRA exposes uncertainties in the evaluation of risk. In the period post publication of WASH-1400, this was considered to be a detrimental aspect of the method; however, more recent thinking (e.g., reference 1) considers this aspect to be a strength of the method. We share this view. Further, in the proposed scheme, this feature is fundamental to the demonstration of compliance.

139
3. Safety Goals, Compliance and CCDFs

Consider the situation that a regulatory body wishes to establish a safety criterion for a system (the term 'safety' being employed in a very general sense) with reference to the level of some parameter, $x$, associated with the system. The most simple form of criterion to formulate is that the parameter $x$ must not exceed some value $x_0$. For instance, it might be required that the frequency of exceedence of a given consequence level $u$ (e.g., a certain number of early or late fatalities or a degree of fiscal loss), denoted $v(u)$, should not exceed $v_0(u)$. Then the plot of $v_0(u)$ against $u$, assuming that $u$ may vary continuously, constitutes a so-called 'regulatory line', a much discussed concept[3]. Returning to our simple system characterized from a safety point of view solely by the parameter $x$, let us assume that some vagueness or uncertainty is attached not only to the value $x$ associated with the system, but also to the actual level deemed to be adequately safe, $x_0$. Hence, both the system property and the safety criterion might be represented as functions or distributions over the parameter $x$ rather than single numbers. Such functions may be represented by Figure 1 where a curve, $a$, describes the system property and a curve, $r$, describes the safety criterion. We have chosen $r$ to be maximized at $x_0$, that is, the function represents a dispersion about $x_0$ for conceptual ease. Here, we do not specify the nature of the functions $a$ and $r$, i.e., whether they are probabilistic in nature or employ some alternative quantification of uncertainty or vagueness. Indeed, we do not specify whether or not the same form of uncertainty or vagueness is attached to the system property as to the regulatory criterion, i.e., whether the two functions $a$ and $r$ are of the same nature. We state only that the two functions must be compared in some manner to determine compliance or otherwise of the system with the safety goal. Intuitive investigation of Figure 1 would lead one to believe that since the maximum of curve $a$ falls below the maximum of curve $r$, that the system satisfies the safety criterion although one may attach slight doubt to the compliance in the light of the small overlap between the curves. If it were the case that both curves represented probability distributions over the parameter $x$, then one would deduce it to be 'unlikely' that the system does not satisfy the safety criterion. If, however, the peaks of a
and \( r \) coincided and they retained their symmetric forms, then the likelihood of compliance (retaining the probabilistic interpretations of the curves) would be 0.5 (i.e., a 50-50 chance) and a more detailed system analysis would be required.

Consider once again the case where the parameter evaluated for a plant is the frequency of exceedence of the consequence level \( \mu \), denoted \( v(\mu) \). Now, \( v(\mu) \) may be uncertain or vague and we characterize the plant by a function over \( v(\mu) \), denoted \( a_\mu[v(\mu)] \) where the index \( \mu \) is attached to 'a' in order to demonstrate that the function need not be the same as that for the exceedence frequency \( v(\mu') \) of some other consequence value, \( \mu' \). In this second case, the function would be \( a_\mu'[v(\mu')] \). To reiterate, the dispersion over the frequency of exceedence of a consequence level need not have the same form for every consequence level considered. The collection of all these functions for different consequence levels, therefore, may be combined succinctly into a single function with two arguments: \( a(v,\mu) \), where \( a(v,\mu) = a_\mu[v(\mu)] \). Likewise, the safety goal at a particular consequence level, \( \mu \), is now no longer a single number \( v_0(\mu) \), but is a dispersion about some number represented by the functions \( r_\mu[v(\mu)] \), or by \( r(v,\mu) \) where \( r(v,\mu) = r_\mu[v(\mu)] \). Hence, at a set consequence level, \( \mu = \mu_i \), we compare \( a(v,\mu_i) \) and \( r(v,\mu_i) \) in order to address the question of compliance at that level.

Figure 1 may therefore be viewed as a cross-section of Figure 2 where the horizontal axis of Figure 1 lies along the line \( \mu = \mu_i \) of Figure 2 and the vertical axis of Figure 1 is normal to the plane of Figure 2. Of course a plot such as on Figure 2 only has meaning where \( \mu \) may be smoothly varied. Hence separate plots for separate 'types' of consequences (e.g., early deaths and fiscal loss) are necessary.

![Figure 2](image)

This method has the advantage that details of the various consequence level attributes are displayed explicitly. Thus, for example, if \( \mu \) were a measure of the number of early deaths, those accident sequences contributing to regions of concern could be identified and appropriate measures be taken. In order to be useful, a criterion should be able to utilize available information and provide recommendations to a level of detail commensurate with that information produced by the calculational methods being adopted. Current PRA techniques indeed produce
functions of the form \( a(v,y) \) where \( a(v,y) \) is of a purely probabilistic nature. The appropriate construction and interpretation of the regulatory function, \( r(v,y) \) are matters requiring more careful consideration and are addressed in the following section.

4. Nature of the Safety Criterion Function

The most established format for the presentation of risk is that of the CCDF \([4]\) and, hence, this will be employed as a basis for the illustration of our proposed method. Let us assume that a function \( a(v,y) \) is available from a PRA (we shall see later that such results are indeed available for certain plants) and that this function is probabilistic in nature. More specifically,

\[
a(v,y)dv = \text{Probability that the frequency of exceedence of consequence level } y \text{ is in the range } dv \text{ about } v. \tag{1}
\]

4.1 Probabilistic Safety Criterion Function

Let us first consider the case where the safety goal function is also probabilistic in nature, i.e.,

\[
r(v,y)dv = \text{Probability that for exceeding consequence level } y, \text{ the safety goal frequency (i.e., the frequency not to be exceeded) is in the range } dv \text{ about } v. \tag{2}
\]

If the regulatory body is to decide upon a maximum permissible frequency for exceeding a given consequence level, then there is little justification for attaching a probability distribution to this frequency. The regulatory frequency for each consequence level is formulated by the regulators and no probabilistic uncertainty is involved. However, where the regulatory safety goal is not couched in terms of a fixed set of frequencies, but in terms of other risk levels which are themselves uncertain, then \( r(v,y) \) may indeed be probabilistic in nature. Consider, for example, the safety criterion that the frequency of exceedence of consequence level \( y \) due to the plant is to lie beneath the frequency of exceedence of consequence level \( y \) due to an earthquake where \( y = \text{the early death of } x \text{ individuals located less than } y \text{ miles from the plant perimeter} \). Here, uncertainty is attached to the numerical frequency-consequence representation of the safety criterion itself. Such criteria are discussed further in Section 8.

Now, if we knew that the frequency of exceedence of consequence level \( y \) for the plant were \( v \), then the probability that the plant meets the safety goal (at level \( y \)) is equal to the probability that the regulatory frequency at level \( y \), is greater than \( v \), denoted \( R(v,y) \), where

\[
R(v,y) = \int dv' r(v',y). \tag{3}
\]
Hence, given only a probability distribution for the plant level-\(\mu\) exceedence frequency, \(a(v,\mu)\), the probability that the plant lies within the safety goal at level \(\mu\), \(Q(\mu)\), is given by

\[
Q(\mu) = \int_0^\infty dv \int_0^\infty dv' r(v',\mu) \frac{\partial}{\partial v} (v')^o
\]

i.e., using Equation (3),

\[
Q(\mu) = \int_0^\infty dv a(v,\mu) R(v,\mu).
\]

We have established, therefore, a mathematical procedure for the comparison of \(a(v,\mu)\) and \(r(v,\mu)\) to ascertain compliance. Due to the probabilistic natures of \(a\) and \(r\), \(Q\) is a probabilistic quantity or, more specifically, \(Q(\mu)\) is the probability of compliance at consequence level \(\mu\). Note that \(R(v,\mu)\) might equally have been defined and supplied as the safety criterion function rather than \(r(v,\mu)\), and the compliance measure combination rule would then be defined by Equation (5) rather than Equation (4).

4.2 Fuzzy Logical Safety Criterion Function

So far we have dealt with the case in which for exceeding each degree of consequence, \(\mu\), there exists a regulatory frequency which must not be exceeded if the plant is to meet the safety goal. The actual magnitudes of these exceedence frequencies were not known exactly and, hence, probability distributions were attached to them. Nevertheless, each regulatory exceedence frequency was a single number (albeit unknown) and a plot of exceedence frequency against a continuously variable consequence parameter, \(\mu\), would result in a single (in general curved) line across the \(v-\mu\) (frequency-consequence) plane. In effect, the \(v-\mu\) plane is divided into two portions, the dividing line being the safety goal (see Figure 3). A point \((v_1,\mu_1)\) in the plane lying

![Diagram of consequence level vs. frequency of exceedence](https://via.placeholder.com/150)

**FIG. 3.**
above the line is to be regarded as an 'unsafe point' in that if the CCDF for the plant were plotted and it passed through this point, then the plant would be deemed not to reach the safety goal at consequence level \( \mu_1 \). Of course, there would in fact be a distribution, \( a(v,u) \), rather than a single line for the plant CCDF, but we are referring to the 'true' CCDF, the uncertainty in the location of which the distribution represents. If the plant CCDF were to pass through a point \((v_2, \mu_2)\) lying beneath the safety goal line, i.e., a 'safe point', then the plant would be deemed to satisfy the safety goal at consequence level \( \mu_2 \).

Naturally, one is perfectly at liberty to define 'safety' in such a strict binary fashion whereby a point located at an arbitrarily small distance above the safety goal line is unsafe and a point located at an arbitrarily small distance below the line is safe. We propose, however, that such a definition is inconsistent with a 'reasonable' notion of safety and does not reflect the manner in which a rational individual would perceive the distinction between a safe and an unsafe environment. A more satisfactory situation would be one in which we could in some way blur the line that separates safety from unsafety and then this fuzzy line would constitute the safety goal. We stress that by the term 'fuzzy line', we do not imply that there exists a crisp (i.e., ordinary) line, the location of which is uncertain (as in the previously discussed case of the probabilistic regulatory function), but that the line itself is a fuzzy entity. Consider Figure 4 displaying a representation of a fuzzy regulatory line. Once again, a point well below the (fuzzy) line is deemed to be safe, a point well above the line is deemed to be unsafe but in between, that is within the fuzzy line, there exist degrees of safeness. Hence, we are introducing a categorizational vagueness, i.e., a question of the degree of safeness of a point rather than a probabilistic uncertainty as to whether a certain point is safe or not.

This form of vagueness is common to many forms of perception and linguistic descriptions of our environment. A particular individual's notion of 'tallness,' for example, is not accessible to strict, binary logic in that somebody who is six feet in height is 'tall' whereas somebody who is half an inch less than this height is 'not tall'. An individual perceives and defines 'tallness' as a fuzzy concept and views different people as being
tall to different degrees. There exists a mathematical framework in which such vagueness may be represented and this is fuzzy set theory (see reference 5 for an introduction to the subject). Just as crisp (i.e., non-fuzzy) set theory underlies the strict binary logic which is quite inappropriate for application in many domains such as those discussed here, so fuzzy set theory seeks to underlie the fuzzy logic that more accurately reflects human rationale. Considering Figure 3 once more, we may view the v-μ plane as being split into two portions where all points below the line belong to the set of points labeled 'safe'. Hence, a point either does or does not belong to the 'safe' set where a strict binary logic is imposed. However, in the fuzzy logical description of safety, a point (v,μ) may be ascribed a degree of belonging to the fuzzy set of point labeled 'safe', i.e., there are degrees of safeness. Let us call the 'safe' set S, and let us denote the degree of membership of the point (v,μ) to this set as m_S(v,μ). i.e.,

\[ m_S(v,μ) = \text{The degree of membership (on a scale of 0 to 1) of the point (v,μ) to the fuzzy subset S of points in the v-μ plane labeled 'safe', i.e., the degree to which the point (v,μ) reaches the safety goal.} \]

If \( m_S(v_1,μ_1) = 1 \), then the point \((v_1,μ_1)\) belongs completely to the set S and it is safe, i.e., it lies within the safety goal. If \( m_S(v_2,μ_2) = 0 \) then the point \((v_2,μ_2)\) is unsafe, i.e., it lies outside the safety goal. Hence, \( m_S(v,μ) \) may lie anywhere in the range 0 to 1 inclusive, the larger the value, the greater the degree of membership of the point \((v,μ)\) to S, i.e., the safer the point \((v,μ)\). Figure 5 shows a possible plot of \( m_S(v,μ) \) against v, the exceedence frequency, for a fixed consequence level μ.

\[ \frac{m_S(v,μ)}{1} \text{ FIXED CONSEQUENCE LEVEL } μ \]

To summarize, we now have two functions. The first, \( a(v,μ) \) defined in Equation (1), is probabilistic in nature and characterizes the safety level of the plant while the second, \( m_S(v,μ) \), is fuzzy in nature and defines the safety goal. The question now arises of how to combine these two functions in order to assess the compliance of the plant with the safety goal. The combination of two probabilistic functions, as undertaken in the last subsection, is a standard procedure, whereas the manner in which fuzzy and probabilistic functions are combined is not so familiar. The procedure for combining such types of functions is
discussed in detail elsewhere[6], and here, we merely summarize
the most pertinent aspects. Consider the fuzzy proposition $P = 'the plant meets the safety goal at consequence level $\mu'$
equivalent to, by our definition of safety, 'the plant is safe
with respect to consequence level $\mu'$'. The proposition is fuzzy
because the term 'safe' is fuzzy. The probability that the fuzzy
proposition is true, $Q(\mu)$, is given by

$$Q(\mu) = \int dv \ a(v,\mu) \ m_S(v,\mu). \quad (7)$$

Hence, in effect, we begin with the probability that the plant
frequency of exceeding consequence level $\mu$ is in the range $dv$
about $v$, $a(v,\mu)dv$, and we then qualify (multiply) that
probability by the degree to which the point $(v,\mu)$ belongs to the
'safe' fuzzy set. Integration over all possible exceedence
frequency values produces $Q(\mu)$, interpreted as the probability
that proposition $P$ is true, i.e., that at consequence level $\mu$,
the plant complies with the safety goal.

Comparison of Equations (7) and (5) reveals identical combination
rules for $m_S(v,\mu)$ and for $R(v,\mu)$ with $a(v,\mu)$, i.e., the fuzzy
goal function $m_S(v,\mu)$ is treated identically, in a technical
sense, to the probabilistic safety goal $R(v,\mu)$ in ascertaining
compliance.

5. The Compliance Probability

The quantity $Q(\mu)$ is the probability that the plant satisfies the
regulatory requirements at consequence level $\mu$. It is the
quantity $Q(\mu)$ which we shall use as the basis of our
acceptability criterion.

From Figure 2 we see that a full analysis would provide the value
of $Q$ at a series of points $\mu_i$, each representing the probability
of compliance at that consequence level. Graphically, this could
be illustrated as in Figure 6. Curve (i) indicates that the
plant complies with the criterion for small $\mu$, the probability of
compliance decreasing as $\mu$ increases. Curve (ii) illustrates a

![FIG. 6.](image-url)
case where the plant complies at low and high $\mu$ but not at intermediate values. Such a result would focus attention on the factors contributing in this mid-range so that 'risk specific' modifications could be put in train.

Two further uses of Figure 6 should be noted. First, the value of $Q(\mu)$ could be used as a trigger in licensing, e.g.,

\[
\begin{align*}
0.95 \leq Q(\mu) \leq 1 & \quad \text{No action} \\
0.5 \leq Q(\mu) < 0.95 & \quad \text{The inspector would wish to have assurance that, for example, the uncertainties were dependable and could not be narrowed before accepting such levels.} \\
0 \leq Q(\mu) < 0.5 & \quad \text{Non-compliance.}
\end{align*}
\]

These are merely illustrative and if normal UK practice were followed, no guidance would be formalized but it would be left to the inspector's judgment. Secondly, the quantity $\mu$ can be a measure of any of a series of consequence types calculable via PRA: early fatalities, delayed fatalities, area of ground contamination, fiscal loss, etc. There is no reason why the method should not be applied to consequence types that have no sliding scale: core melt, release of 1ERL, etc. In each of these cases, there is a single, unique consequence $\mu$ and we would have simply the probability $Q(\mu)$ that the plant complies with the regulatory requirements pertaining to that particular quantity (e.g., the USNRC specifies core melt frequency as a criterion).

The ease with which $Q(\mu)$ may be evaluated, of course, depends upon the functional forms of $a(\nu, \mu)$ and $r(\nu, \mu)$ or $m_s(\nu, \mu)$. Indeed, the safety goal may be selected to be of a well-behaved form and in Section 7, we discuss the construction of such functions. As an example of the evaluation of $Q(\mu)$, let us consider the case that the plant function, $a(\nu, \mu)$, may be well approximated to a lognormal distribution over the parameter $\nu$ for fixed values of consequence level $\mu$; or, more specifically,

\[
a(\nu, \mu) = \frac{1}{(2\pi)^{1/2} \sigma_a(\mu)^2} \exp\left(-\frac{(\ln \nu - \eta_a(\mu))^2}{\sigma_a(\mu)^2}\right).
\]

To reiterate, for planes of fixed $\mu$ (see Figure 2), the probability distribution over $\nu$ is lognormal, the parameters $\eta_a$ and $\sigma_a$ depending upon the value of $\mu$. Let us first consider a probabilistic safety goal function, $r(\nu, \mu)$, and assume that it also is of a lognormal form:

\[
r(\nu, \mu) = \frac{1}{(2\pi)^{1/2} \sigma_r(\mu)^2} \exp\left(-\frac{(\ln \nu - \eta_r(\mu))^2}{\sigma_r(\mu)^2}\right).
\]

From Equation (3), we may evaluate the exceedence probability form of this safety goal, $R(\nu, \mu)$, to obtain

\[
R(\nu, \mu) = \frac{1}{2} \text{erfc} \left(\frac{\ln \nu - \eta_r(\mu)}{(2)^{1/2} \sigma_r(\mu)}\right).
\]
where erf is the complementary error function. With the use of Equation (5) we may evaluate \( Q(\mu) \), the probability that at consequence level \( \mu \), the plant complies with the safety goal. We obtain:

\[
Q(\mu) = \frac{1}{2} \left[ 1 + \text{erf}\left(\frac{\eta_r(\mu) - \eta_a(\mu)}{\sqrt{2\sigma_r^2(\mu) + 2\sigma_a^2(\mu)}}\right)\right]
\]

(11)

where erf is the error function.

If the goal is fuzzy in nature, i.e., \( m_g(v,\mu) \), then we are at liberty to endow it with an identical functional form to \( R(v,\mu) \) as described by Equation (10) if desired:

\[
m_g(v,\mu) = \frac{1}{2} \text{erfc}\left(\frac{\ln v - \eta_r(\mu)}{(2)^{1/2} \sigma_r(\mu)}\right).
\]

(12)

Of course, \( \eta_r \) and \( \sigma_r \) no longer have their probabilistic interpretations in this context and should be viewed merely as two functional parameters characterizing \( m_g(v,\mu) \). Note that \( m_g \) has an appropriate functional form. For any consequence level \( \mu \), as \( v \rightarrow 0 \) then \( m_g \rightarrow 1 \), i.e., absolute safety corresponds to a zero exceedence frequency of a consequence level. When \( v \) becomes large, then \( m_g \) approaches zero, i.e., large exceedence frequencies are unsafe since they have small degrees of membership to the 'safe' set. The numerical correspondence between Equations (12) and (9) describing the fuzzy and probabilistic goals is straightforward. For a fixed value of consequence level \( \mu \), the value of \( v \) at the 100\(\%\)th percentile of \( r(v,\mu) \), i.e., where \( R(v,\mu) = 1 - \beta \), is that value of \( v \) that has a degree of membership of \( 1 - \beta \) to the 'safe' set, \( S \), i.e., \( m_g(v,\mu) = 1 - \beta \). Hence, for a given \( \mu \), the 5th percentile of \( r(v,\mu) \) is at a value of \( v \) that has a degree of membership of 0.95 to the 'safe' set of points. To reiterate, if a point \( (v,\mu) \) has a degree of membership \( \beta \) to the 'safe' set (i.e., it is safe to the degree \( \beta \)), then if the function defining the fuzzy set memberships were instead interpreted as a probabilistic safety function in the exceedence form (i.e., \( R(v,\mu) \)), we would deduce that the probability of the point \( (v,\mu) \) lying on the safe side of the true crisp safety goal line is \( \beta \).

An interesting aspect of the fuzzy logical goal of Equation (12) is that it only concedes absolute safety (i.e., \( m_g(v,\mu) = 1 \)) at \( v = 0 \) whereas the probabilistic function \( r(v,\mu) \) assigns a finite probability to the crisp safety line passing through frequencies at \( v > 0 \). Despite the more stringent and, indeed, more intuitively appealing fuzzy representation of 'safety' and 'absolute safety' (i.e., nothing is really 'absolutely safe'), the probability of compliance evaluated, \( Q(\mu) \), is identical for the probabilistic and fuzzy cases since \( m_g \) and \( R \) are analytically identical, as are the two combination rules, Equations (5) and (7). Hence, when \( m_g(v,\mu) \) is given by Equation (12) and \( a(v,\mu) \) by Equation (8), then the probability that the fuzzy proposition, 'the plant complies with the safety goal at consequence level \( \mu \)' is true, is given by Equation (11).
6. An Example

Couched in its purely mathematical habit, the proposed method might be considered as obscure; however, the modus operandi of the approach may be clarified by the use of an example.

6.1 Data Availability

a) The Plant: Several PRAs are available which have quantified uncertainties in their estimates of risk. The fact that certain treatments may be open to question does not matter for our present purposes. For illustration, we have chosen the study of the Limerick Plant performed by NUS Corporation[7]. This was chosen because (i) it is very recent and is as near to the state-of-the-art as we have, (ii) it presents (arguably) the best available treatment of uncertainties, and (iii) the results are presented in such a fashion as to be immediately useful.

b) The Safety Goal: An interpretation of the NII safety principles in terms of an exceedance frequency versus consequence plot recently became available[8]. Some uncertainty was attached to the appropriate location of the crisp line in the v-μ plane corresponding to the NII principles and, hence, we are provided with the basis for a goal of the probabilistic type. In fact, Reference 8 provides bounding CCDFs for the NII safety goal although the bounds are not qualified by confidence levels. The procedure for obtaining such bounding CCDFs is an extremely difficult one and the value of the results is questionable; however, we only use the results for illustration and do not enter into the debate over their value here.

Figures 7 and 8 show the raw data needed for our calculations. Figure 7 shows the 5th, 50th, and 95th percentile CCDFs for internally initiated events at the Limerick Station, with latent fatalities as the consequence measure chosen here for comparison. Figure 8 shows the CCDF interpretation of the NII safety principles for internally initiated events for the number of fatal cancers. Two bounding CCDFs were produced to represent the uncertainty in the location of the appropriate CCDF. Purely to allow progress, we arbitrarily identify the upper boundary curve as the 95th percentile CCDF and the lower bounding curve as the 5th percentile CCDF. In the real case, R(v,μ) or m(v,μ) would be specified as part of the criterion. We now fit the lognormal form of a(v,μ) (Equation (8)) to the Limerick CCDFs and the lognormal form of r(v,μ) (Equation (9)) to the NII CCDFs representing the safety goal. Figure 9 displays plots of the functions a, i, o, and r against consequence level obtained as fits to the Limerick and NII data.

With the use of Equation (11), we may evaluate Q(μ) and Figure 10 displays the probabilities that the Limerick Station complies with the CCDF interpretation of the NII safety principles at various levels of late fatalities, μ.
LIMERICK BWR CCDFs for Latent Cancer Fatalities: Internal Initiating Events

Number of Latent Fatalities vs. Frequency of Exceedance (year$^{-1}$)

Fig. 7.

CCDF Interpretation of the NII Safety Principles for Internal Initiating Events

Fig. 8.
6.2 Results

Figure 10 illustrates very well the level of detail available from such a procedure. Compared with the NII safety principles, the Limerick plant complies at low consequences (i.e., the probability that Limerick satisfies the safety principles is close to unity at \( \mu = 1 \) latent fatality). At the high consequence end, the probability approaches 0.5 while there is an interesting 'dip' at about \( 10^3 \) fatalities. The plant approaches a compliance probability of 0.1 interpreted as non-compliance according to our previous choice. A detailed investigation of the accident sequence analysis could, in principle, reveal the cause of the shape of \( Q(\mu) \). A brief examination of the study, particularly Section 9, provides some idea of why minimum compliance likelihood occurs at \( 10^3 \) fatalities. The dominant release category for this plant is called OPREL. It is made up of sequences related to transients or small break LOCAs in which the ability to maintain the coolant inventory is lost and core melt ensues. However, the suppression pool remains sub-cooled.
and any radionuclides have to pass through this pool before release. Thus, the amount of material released is relatively low and, hence, the dip at modest values of fatalities. We would therefore conclude that protection against loss of coolant inventory following transients is of particular concern (at least in this BWR) and that the question of the decontamination factor which may be claimed for radionuclides passing through a suppression pool would be at the heart of any more detailed analyses.

7. The Construction of Fuzzy Safety Goals

While the interpretation of a probabilistic function safety goal is a fairly clear one (i.e., resulting from the translation of risk criteria couched in non-CCDF form into uncertain CCDF form, e.g., the NII principles, comparison with earthquake risk, etc.) the interpretation and, indeed, the construction of fuzzy safety goals are topics requiring further discussion. Here, we wish to
consider fuzzy safety goals in terms of some fundamental aspects of risk criterion development. Of necessity, this section is of a rather mathematical nature; however, the pace adopted is a slow one.

7.1 Inbuilding Risk Bias

Let us return to the simple situation of a crisp regulatory line in the $v$-$\mu$ plane. The most fundamental case one might consider is where the shape of the line is determined by the equation $v\mu = K$ where $\mu$ is the consequence level, $v$ is the maximum permissible exceedence frequency of level $\mu$ and $K$ is a constant. Taking logs (base 10) of both sides of this equation, we have that $\log v = J - \log \mu$ where $J = \log K$. Here, the product of the consequence level and the frequency with which it is exceeded must not exceed $K$, for any consequence level. The first stage of generalization is to build in a so-called 'risk bias' factor, i.e., $v\mu^a = K$ defines the crisp regulatory line or

$$\log v = J - a \log \mu.$$  (13)

Here, the gradient of the $\log v$ vs. $\log \mu$ plot is no longer -1 and is modified to $-a$. If $a > 1$, the criterion represented by Equation (13) is said to be 'risk averse' whereas if $0 < a < 1$, then the criterion is said to be 'risk seeking'. By this is meant that the greater the value of $a$ (for fixed $J$, and defining the units of consequence such that $\mu = 1$ is the smallest consequence level), the greater the portion of the $v$-$\mu$ plane falling on the 'unsafe' side of the safety goal line. Further, as $a$ increases, the rate of passage of points for a particular value of $\mu$ from 'safe' to 'unsafe', as a proportion of the total number of points (for that $\mu$) on the 'safe' side, increases with increasing $\mu$. Hence, by increasing $a$, the aversion to high consequence-low frequency events increase more rapidly than the aversion to low consequence-high frequency events. This is termed 'risk bias'.

How now may risk bias, a fundamental aspect of crisp line safety goal formulation, be manifested in the fuzzy goal formalism proposed here? Let us consider a particular degree of safeness, $L_\sharp$, that is, $L_\sharp$ lies somewhere in the range 0 to 1 inclusive. Now consider a safety goal characterized by the fuzzy subset $S$, 'safe', of the $v$-$\mu$ plane, with membership values $m_S(v,\mu)$.

Let us digress briefly in order to consider some of the general properties required of $m_S(v,\mu)$ for consistency with the general concept of safety. First we require that

$$\text{if } v_1 > v_2 \text{ then } m_S(v_1,\mu) \leq m_S(v_2,\mu)$$  (14a)

and

$$\text{if } \mu_1 > \mu_2 \text{ then } m_S(v,\mu_1) \leq m_S(v,\mu_2).$$  (14b)
i.e., at a given consequence level \( \mu \), the greater the frequency of exceedence, the lesser (or equal) the level of safety and at a given frequency of exceedence, the larger the corresponding consequence level, the lesser (or equal) the level of safety. Let us define an 'ideal' safety goal in the following manner: The function \( m_{S}(v,\mu) \) is smoothly varying and

\[
\text{if } v_1 > v_2 \text{ then } m_{S}(v_1,\mu) < m_{S}(v_2,\mu) \quad (15a)
\]

and

\[
\text{if } \mu_1 > \mu_2 \text{ then } m_{S}(v,\mu_1) < m_{S}(v,\mu_2). \quad (15b)
\]

That is, the symbols of Equation (14) are replaced by \( < \). Of course in practice, for a consequence of \( \mu = 1 \) early death, for example, one may be inclined to assign equal memberships of the points \((v = 10^{-10} \text{yr}^{-1}, \mu_1) \) and \((v = 10^{-11} \text{yr}^{-1}, \mu_2) \) to the 'safe' set (i.e., membership unity) but let us assume that for an ideal safety goal, \( m_{S}(10^{-10} \text{yr}^{-1}, \mu_1) < m_{S}(10^{-11} \text{yr}^{-1}, \mu_2) \). The requirement of Equation (15) can be easily satisfied while retaining consistency with an intuitively reasonable notion of safety by making \( m_{S}(v,\mu) \) approach the value unity arbitrarily rapidly where required as \( v \) or \( \mu \) decreases and by making \( m_{S}(v,\mu) \) approach zero arbitrarily rapidly where required as \( v \) or \( \mu \) increases. The reason we have this requirement of an 'ideal' safety goal is so that the trajectory of points in the \( v-\mu \) plane satisfying

\[
m_{S}(v,\mu) = L_1 \quad (16)
\]

is a single, smooth line. Hence, all points whose degree of safeness is \( L_1 \), i.e., whose degree of membership to the 'safe' fuzzy subset of the \( v-\mu \) plane is \( L_1 \), lie on a single, smooth line. This is demanded purely for the sake of the general technical accuracy of this section, where risk bias is discussed. If the safety goal is not to be constructed or understood purely in terms of risk bias, then the restrictions of Equation (14) are likely to be quite adequate.

Let us now demand that the trajectory in the \( v-\mu \) plane passing through all points of safety level \( L_1 \), coincides with a line displaying a certain risk bias characteristic. Let this line be defined by

\[
\log v = J_1 - a_1 \log \mu \quad (17)
\]

where \( J_1 \) and \( a_1 \) are constants, \( a_1 \) being a measure of risk bias. To reiterate, we are demanding that all points of safety level \( L_1 \) lie along the line defined by Equation (17) and, hence, a risk bias is built into what we deem to be safe to the level \( L_1 \).
The lognormal-related fuzzy safety goal of Equation (12) is 'ideal' in that it satisfies Equation (15a) and, through suitable choices of \( \eta_r(\mu) \) and \( \sigma_r(\mu) \), may be made to smoothly vary and to satisfy Equation (15b). Hence, the safety goal form of Equation (12) will be used for our current example. Now, if we wish the \( v-\mu \) trajectory defined by Equation (16) to coincide with the line given by Equation (17), we must demand that

\[
\zeta(J_i - \alpha_i \log \mu) = \sqrt{2} \sigma_r(\mu) \text{erfc}^{-1} 2L_i + \eta_r(\mu) \tag{18}
\]

where \( \zeta = (\log e)^{-1} \). We see that this expression places a restriction on the possible functional forms of \( \sigma_r(\mu) \) and \( \eta_r(\mu) \), although there is still some freedom in the selection of each of these functions. Let us now make a further demand of our fuzzy safety goal. This is that there exists a risk bias in determining what is deemed to be safe to the degree \( L_* \), where \( L_* \neq L_i \). That is, the trajectory in the \( v-\mu \) plane defined by

\[
m_s(v, \mu) = L_j \tag{19}
\]

is to coincide with the risk-biased line

\[
\log v = J_j - \alpha_j \log \mu. \tag{20}
\]

Again, for consistency between Equations (19) and (20), we require that

\[
\zeta(J_j - \alpha_j \log \mu) = \sqrt{2} \sigma_r(\mu) \text{erfc}^{-1} 2L_j + \eta_r(\mu) \tag{21}
\]

thus placing a second restriction upon the forms of \( \sigma_r(\mu) \) and \( \eta_r(\mu) \). In fact, Equations (18) and (21) together define \( \sigma_r(\mu) \) and \( \eta_r(\mu) \) completely and we have that

\[
\sigma_r(\mu) = A - B \log \mu \tag{22}
\]

and

\[
\eta_r(\mu) = C - D \log \mu \tag{23}
\]
where the constants $A$, $B$, $C$, and $D$ are given by

$$A = \frac{\zeta(J_i - J_j)}{\sqrt{2} \left( \text{erfc}^{-1}2L_i - \text{erfc}^{-1}2L_j \right)} \quad (24a)$$

$$B = \frac{\zeta(a_i - a_j)}{\sqrt{2} \left( \text{erfc}^{-1}2L_i - \text{erfc}^{-1}2L_j \right)} \quad (24b)$$

$$C = \frac{\zeta(J_j \text{erfc}^{-1}2L_i - J_i \text{erfc}^{-1}2L_j)}{\text{erfc}^{-1}2L_i - \text{erfc}^{-1}2L_j} \quad (25a)$$

and

$$D = \frac{\zeta(a_j \text{erfc}^{-1}2L_i - a_i \text{erfc}^{-1}2L_j)}{\text{erfc}^{-1}2L_i - \text{erfc}^{-1}2L_j}. \quad (25b)$$

Hence, for consistency with the lognormal form of $m_S(v, \mu)$ given by Equation (12), we are only at liberty to specify the risk bias at two safety levels. Inspection of Equations (24) and (25) reveals that once the constants $A$, $B$, $C$, and $D$ are determined using the two specified safety levels of chosen risk bias, then all safety levels, $L_k$, correspond to trajectories in the $v$-$\mu$ plane that coincide with risk biased lines of the form

$$\log v = J_k - a_k \log \mu \quad (26)$$

where the constants $J_k$ and $a_k$ are already determined and not open to choice. This, we would not expect to be a severe restriction on the goal construction since it serves to ensure a smooth change in risk bias for a smooth change in degree of safety considered.

Before discussing examples of risk-biased fuzzy safety goals, we draw attention to a special case of Equations (24) and (25), this being the case where the two safety levels selected at which to specify risk bias are complementary, i.e., $L_i + L_j = 1$. In that case, Equations (24) and (25) become
Therefore, if one wishes to specify risk bias at, for example, safety levels 0.95 and 0.05 or 0.8 and 0.2, then Equations (27) and (28) may be employed to construct the fuzzy safety goal $m_g(v, u)$. Due to the relative simplicity of Equations (27) and (28) compared to Equations (24) and (25), one would, in practice, select complementary safety levels at which to specify risk bias.

7.2 Example Fuzzy Safety Goals

Here we construct two possible fuzzy safety goals, each of the lognormal form described by Equation (12).

**Goal 1**: For what we consider to be safe to the degree 0.95, we attach no risk bias, i.e., $\alpha = 1$. More specifically, the points in the $v-u$ plane of 0.95 safety level, i.e., the points along the trajectory defined by $m_g(v, u) = 0.95$ are to lie along the line $\log v = -4 - \log u$. Here, $u$ may be a measure of delayed deaths, fiscal loss, etc. (see Figure 11). Hence, the point corresponding to $u = 1$ being exceeded with a frequency of $10^{-6}$ yr$^{-1}$ (assuming that we have chosen to measure frequencies in yr$^{-1}$) is considered to be safe to the level 0.95. Further, for what is considered to be safe to the degree 0.05, we also chose to have no risk bias attached and the trajectory defined by $m_g(v, u) = 0.05$ is to coincide with the line $\log v = -3 - \log u$. That is, the exceedence of $u=1$ with a frequency of $10^{-3}$ yr$^{-1}$ is considered to be safe to the degree 0.05.

**Goal 2**: Here, let the definition of the 0.95 level of safety be identical to that for the 0.95 level of Goal 1. However, let us in this case attach an 0.05 safety level to low frequencies at higher consequence levels than would be done in a risk-unbiased case. That is, when considering low
frequencies, what we deem to be safe to the degree 0.05 corresponds to higher levels of consequence than we would choose in a risk-unbiased situation. This notion may be clarified by a simple example. Let us assume that we attach an 0.05 degree of safety to the point where the frequency of exceeding $\mu=1$ death is $10^{-3} \text{yr}^{-1}$. In a risk-unbiased situation, therefore, we would attach the same level of safety, 0.05, to the point where the frequency of exceeding $10^6$ deaths is $10^{-9} \text{yr}^{-1}$ (so that the product of the frequency and consequence, i.e., the risk, is conserved). However, $10^{-9} \text{yr}^{-1}$ is such a small frequency (corresponding to a return period of about a tenth of the age of the universe) that we may be willing to attach the low safety level of 0.05 to even more deaths at that frequency, e.g. $10^8$ deaths. We shall employ the figures of this example and, for Goal 2, we select the 0.05 safety level trajectory to coincide with the risk-seeking line $\log v = -3 - 0.75 \log \mu$, i.e., $\alpha < 1$. The risk-biased lines defining the two fuzzy goals are displayed on Figure 11.
Again, the Limerick PRA latent fatality CCDFs (Figure 7) provide convenient data against which to compare the two safety goals developed here. Hence, for such a comparison, we interpret \( \mu \) in our goals as a measure of the number of latent fatalities. To summarize our goal parameters in terms of the notation of the previous subsection, we have,

\[
\text{Goal 1: At } L_1 = 0.95 \text{ we demand that } J_1 = -4, \alpha_1 = 1 \\
\text{At } L_2 = 0.05 \text{ we demand that } J_2 = -3, \alpha_2 = 1
\] (29a)

\[
\text{Goal 2: At } L_1 = 0.95 \text{ we demand that } J_1 = -4, \alpha_1 = 1 \\
\text{At } L_2 = 0.05 \text{ we demand that } J_2 = -3, \alpha_2 = 0.75
\] (29b)

Since for both goals, the safety levels at which the risk bias factors were selected are complementary (i.e., \( L_1 + L_2 = 1 \)), then Equations (27) and (28) may be employed to evaluate the constants \( A, B, C, \) and \( D \). Substitution of these constants into Equations (22) and (23) gives the functions \( c_r(\mu) \) and \( n_r(\mu) \) for each goal. Once more effecting a lognormal fit to the Limerick plant CCDFs (see Equation (8)) we may employ Equation (11), which, in terms of the constants \( A, B, C, \) and \( D \) reads

\[
Q(\mu) = \frac{1}{2} \left[ 1 + \text{erf} \left( \frac{C-D\log \mu - n_a(\mu)}{\sqrt{2[2A-B\log \mu]^2 + 2\sigma_a^2(\mu)}} \right) \right],
\] (30)

to evaluate the compliance probabilities, \( Q(\mu) \). Figure 12 displays a plot of \( Q(\mu) \) against consequence level \( \mu \) for each of the two safety goals. Inspection of Figure 12 reveals the effect of 'widening' the safety goal (as in Goal 2) towards the low frequency-high consequence end of the \( v-\mu \) plane. Both functions \( Q(\mu) \) are of the same general form, each displaying a dip around \( 10^3 \) latent fatalities (as was the case for the NII goal); however, whereas for Goal 1, \( Q(\mu) \) deceases to a value under 0.2, for Goal 2, \( Q(\mu) \) deceases only to approximately 0.4. Of course, in accordance with our previously suggested compliance rules, Limerick fails to comply with both goals at \( \mu = 10^3 \) latent fatalities. The region over which there exists non-compliance, however, differs for the two goals. For Goal 1, this region is that for which \( \log \mu \geq 1.7 \) and for Goal 2, it is that for which \( 2.25 \leq \log \mu \leq 3.75 \). Hence, for Goal 2, there is a greater consequence level region over which the Limerick Station PRA might be inspected in more depth in order to narrow uncertainties and demonstrate compliance with higher probabilities, and a smaller consequence level region over which, for compliance, the plant design and components need to be modified.

8. Probabilistic Safety Goals

In Section 4, we discussed the idea of a safety goal that takes the form of a probability distribution over exceedence frequencies at each consequence level. Such a goal is to be interpreted in the following fashion: there exists a single, crisp line in the \( v-\mu \) plane which constitutes the safety goal but
the location of the line is uncertain and this uncertainty is represented as a probability distribution of the form $r(v, u)$, defined in Equation (2). Such a format would be appropriate where the safety criterion is not stated in terms of a line (crisp or fuzzy) in the $v$-$u$ plane, but in terms of the risk associated with other phenomena and situations, where the magnitude of that risk is uncertain. A safety criterion may be, for example, that the presence of a certain plant is not to increase by more than one percent, the frequency of a consequence level $u$ being exceeded at or near that location, i.e., the increment to the existing background risk (due to earthquakes, floods, aircraft impact, etc.) must be evaluated to demonstrate compliance. Of course, there is uncertainty attached to the background risk itself so such a safety goal would be presented numerically in a probabilistic fashion. We note that despite the fact that the goal is presented as a probabilistic function, the 'true' crisp regulatory line still exists (albeit unknown) and one runs into the previously discussed problem of the consistency of a crisp line safety goal with an intuitively reasonable notion of safety. Such problems are obviated by the use of fuzzy goals.
The incorporation of fuzziness into probabilistic safety goals, however, is beyond our present aim. Returning to the example of a safety goal couched in terms of incremental risk, it is clear that quite detailed, site specific evaluations of certain hazards (without the plant) are required for the demonstration of compliance. At present, such detailed data are generally unavailable and, consequently, a specific example cannot be provided. We should note, however, that when such CCDF confidence bounds become available, they will become wider for events of increasing consequence level (i.e., increasing rarity). This situation contrasts with that of Section 6 where the safety goal pertaining to internally initiated events comprised, essentially, parallel confidence bound lines (on a logarithmic plot). We observe that, in a mathematical sense, the widening of confidence bounds in a probabilistic safety goal towards high consequence events is equivalent to a widening, in the fuzzy sense, i.e., an increased fuzzification (see Goal 2 discussed in the last section) of a fuzzy goal towards the high consequence domain.

The mathematical framework developed here may be adapted quite simply to accommodate safety goals defined in terms of incremental risk, assuming that the frequency distributions for background risk were available. Once again, let $a(v,\mu)$ characterize the risk associated purely with the plant, defined more precisely by Equation (1). Let the background risk be characterized by the function $b(v,\mu)$ where

$$b(v,\mu)dv = \text{Probability that for the background risk, the frequency of exceeding consequence level } \mu \text{ is in the range } dv \text{ about } v.$$ (31)

Further, let the safety goal be defined as such: The presence of the plant will not increase the frequency of exceeding consequence level $\mu$ by more than a factor of $1/k(\mu)$, where the function $k(\mu)$ is specified. Note that for generality, we permit different increments in exceedence frequencies for different consequence levels. For example, we may demand that for compliance, the frequency of exceeding one death is not to increase due to the presence of the plant by more than 0.1%, but that the frequency of exceeding $10^5$ deaths may increase by up to 10%. In this case, we would have that $k(1) = 10^5$ and $k(10^5) = 10$. Note also that the safety goal is not confined to terms of risk increment due to a specific external hazard. Provided that the plant CCDFs are available for both internal and external initiators, and that the background CCDFs are available also, then our method permits an evaluation of the total increment to background risk and suggests criteria for the demonstration of compliance.

For the probability of compliance at consequence level $\mu$, $Q(\mu)$, we have that

$$Q(\mu) = \int dv a(v,\mu) \int dv' b(v',\mu) \frac{1}{k(\mu)v}.$$ (32)

If, once again, we consider the case where $a(v,\mu)$ is lognormal in form (see Equation (8)) and $b(v,\mu)$ is also taken to be lognormal, i.e.,
\begin{equation}
    b(v, \mu) = \frac{1}{(2\pi)^{1/2} \sigma_b(\mu)} \exp\left[ -\frac{1}{2} \left( \frac{\ln v - \eta_b(\mu)}{\sigma_b(\mu)} \right)^2 \right].
\end{equation}

then, it can be shown that

\begin{equation}
    Q(\mu) = \frac{1}{2} \left[ 1 + \text{erf}\left( \frac{\eta_b(\mu) - \eta_a(\mu) - \ln k(\mu)}{\sqrt{2}(\sigma_b^2(\mu) + \sigma_a^2(\mu))^{1/2}} \right) \right].
\end{equation}

9. Summary and Conclusions

We have proposed a method of judging the compliance of plant with a safety goal which incorporates a representation of the uncertainties in the plant risk evaluation. Where the safety goal is not defined in terms of frequency-consequence limit lines, then our method incorporates the uncertainty that arises in translating the goal into the CCDF format compatible and appropriate for comparison with current probabilistic risk assessments. Where the goal is to be formulated in terms of frequency-consequence limitations, then the concept of 'degree of compliance' is incorporated, reflecting in a realistic fashion the vagueness naturally associated with any reasonable notion of a safe environment. The perceived advantages of the general methodology are:

a) It constitutes a logical, disciplined technique to give a consistent interpretation of the PRA results.

b) It uses the information currently available in the PRA methodology to provide a more detailed, yet transparent interpretation of the acceptability of the plant.

c) The level of detail provided by the PRA may be as low or as high as the calculational methods permit.

d) Risks of any form (societal, individual, fiscal ...) may be considered within the same logical framework.

e) Site specific requirements may be included in the safety goal very simply.

f) The regulator can 'tune' the safety goal to reflect the degree of uncertainty permissible in the risk assessment in any particular consequence domain.

g) For safety criteria involving a knowledge of background risk, the method incorporates whatever the level of uncertainty is in that risk.

h) The method can incorporate the reasonable and inevitable vagueness attached to the regulators' notion of adequate safety.
i) It is readily applicable to non-nuclear hazards.

There exist disadvantages also. These may include

a) General unfamiliarity with 'fuzzy logic' could inhibit the use of the method.

b) It requires a level of understanding of PRA methodology which is beyond that normally associated with safety goals.

c) In the case of incremental risk criteria, more site specific data are required pertaining to background risk than are currently available.

d) It requires detailed guidance to the analyst on PRA methods and the treatment of uncertainties.

We are confident that in the longer term, these disadvantages could be overcome. The aim is to make the setting of safety goals compatible with the state-of-the-art in PRA which we anticipate will generally become available in a few years time.

REFERENCES


PROSPECTS FOR PROBABILISTIC SAFETY CRITERIA (PSC)

F. NIEHAUS
Reliability and Risk Assessment Section,
Division of Nuclear Safety,
International Atomic Energy Agency,
Vienna

Abstract

Many countries are developing PSCs. At first glance the various proposals which have been made look very different and include core-melt probabilities, individual risk levels, limit-lines for societal risk and probability density functions for individual exposure to radiation (1,2). Most of these proposals are highly controversial and at present subject to an analysis of their implications for actual safety decisions. Also the "first principles" which are being used for PSC developments vary considerably; ranging from comparisons to societal risk levels in general, comparisons to risks of competing energy technologies, to comparison to radiation risks from normal operation (3). This paper suggests that the various approaches are not as different as one might infer and explores the possibilities to develop an integrated hierarchical framework for PSCs in accordance with various objectives.

1. Introduction

Many countries are developing PSCs. At first glance the various proposals which have been made look very different and include core-melt probabilities, individual risk levels, limit-lines for societal risk and probability density functions for individual exposure to radiation (1,2). Most of these proposals are highly controversial and at present subject to an analysis of their implications for actual safety decisions. Also the "first principles" which are being used for PSC developments vary considerably; ranging from comparisons to societal risk levels in general, comparisons to risks of competing energy technologies, to comparison to radiation risks from normal operation (3). This paper suggests that the various approaches are not as different as one might infer and explores the possibilities to develop an integrated hierarchical framework for PSCs in accordance with various objectives.

2. The need for PSCs

At present nuclear safety is assured by mainly deterministic criteria. Probabilistic considerations have, of course, been used, however, not in a very systematic way. Many working in the nuclear field believe that it is neither feasible nor desirable to propose PSCs. The following points to some important developments which demonstrate that it will be unavoidable and useful to establish PSCs.

As a complement to the deterministic safety analysis, PSA has been developed and is being widely used, to a large extent as a result of TMI accident. Table 1 gives a listing of PSAs completed so far (4).
In addition PSA is being heavily used outside the area of nuclear power plant safety for other facilities of the fuel cycle, including waste disposal, and in other potentially hazardous industries, in particular petrochemical plants. So far the use of PSA has been mainly restricted to a limited number of industrialized countries. However, within the framework of an Interregional Technical Co-operation Project of the IAEA 12 Member States (Table 2) are developing significant PSA activities with the objective to perform a level-1 PSA (5). In addition, there are a number of bilateral agreements for co-operation in PSA.

### TABLE 1. PRA STUDY RESULTS — CORE MELT FREQUENCIES [9]

<table>
<thead>
<tr>
<th>PLANT</th>
<th>PROGRAMME DATE</th>
<th>CORE MELT PROBABILITY (YR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARKANSAS-1</td>
<td>IREP, 1981</td>
<td>5 x 10^{-5}</td>
</tr>
<tr>
<td>BIBLIS B</td>
<td>DRS, 1978</td>
<td>4 x 10^{-5}</td>
</tr>
<tr>
<td>BIG ROCK POINT</td>
<td>UTILITY, 1981</td>
<td>1 x 10^{-3}</td>
</tr>
<tr>
<td>BROWNS FERRY-1</td>
<td>IREP, 1981</td>
<td>2 x 10^{-4}</td>
</tr>
<tr>
<td>CALVERT CLIFFS-1</td>
<td>RSSMAP, 1982</td>
<td>2 x 10^{-3}</td>
</tr>
<tr>
<td>CRYSTAL RIVER-3</td>
<td>IREP, 1980</td>
<td>4 x 10^{-4}</td>
</tr>
<tr>
<td>GRAND GULF-1</td>
<td>RSSMAP, 1981</td>
<td>4 x 10^{-5}</td>
</tr>
<tr>
<td>INDIAN POINT-2</td>
<td>UTILITY, 1982</td>
<td>4 x 10^{-4}</td>
</tr>
<tr>
<td>INDIAN POINT-3</td>
<td>UTILITY, 1982</td>
<td>9 x 10^{-9}</td>
</tr>
<tr>
<td>LIMERICK</td>
<td>UTILITY, 1982</td>
<td>3 x 10^{-8}</td>
</tr>
<tr>
<td>MILLSTONE-1</td>
<td>IREP, 1982</td>
<td>3 x 10^{-4}</td>
</tr>
<tr>
<td>MILLSTONE-3</td>
<td>UTILITY, 1983</td>
<td>1 x 10^{-4}</td>
</tr>
<tr>
<td>OCONEE-3</td>
<td>RSSMAP, 1980</td>
<td>8 x 10^{-5}</td>
</tr>
<tr>
<td>PEACH BOTTOM-2</td>
<td>WASH-1400, 1975</td>
<td>3 x 10^{-9}</td>
</tr>
<tr>
<td>RINGHALS-2</td>
<td>SSPB, 1983</td>
<td>4 x 10^{-4}</td>
</tr>
<tr>
<td>SEABROOK</td>
<td>UTILITY, 1983</td>
<td>2 x 10^{-4}</td>
</tr>
<tr>
<td>SEQUOYAH-1</td>
<td>RSSMAP, 1981</td>
<td>6 x 10^{-8}</td>
</tr>
<tr>
<td>SHOREHAM</td>
<td>UTILITY, 1983</td>
<td>4 x 10^{-8}</td>
</tr>
<tr>
<td>SIZEWELL B</td>
<td>CEGB, 1982</td>
<td>1 x 10^{-4}</td>
</tr>
<tr>
<td>SURRY-1</td>
<td>WASH-1400, 1975</td>
<td>6 x 10^{-8}</td>
</tr>
<tr>
<td>YANKEE ROWE</td>
<td>UTILITY, 1982</td>
<td>2 x 10^{-8}</td>
</tr>
<tr>
<td>ZION</td>
<td>UTILITY, 1981</td>
<td>7 x 10^{-8}</td>
</tr>
</tbody>
</table>

a Includes external event contribution where appropriate.
b Values which are asterisked (*) represent median values; otherwise points estimates are listed.

### TABLE 2. MEMBER STATES PARTICIPATING IN THE PSA INTERREGIONAL PROGRAMME

<table>
<thead>
<tr>
<th>Brazil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgaria</td>
</tr>
<tr>
<td>China</td>
</tr>
<tr>
<td>Czechoslovakia</td>
</tr>
<tr>
<td>Hungary</td>
</tr>
<tr>
<td>India</td>
</tr>
<tr>
<td>Mexico</td>
</tr>
<tr>
<td>Philippines</td>
</tr>
<tr>
<td>Poland</td>
</tr>
<tr>
<td>Spain</td>
</tr>
<tr>
<td>Turkey</td>
</tr>
<tr>
<td>Yugoslavia</td>
</tr>
</tbody>
</table>

166
PSA is also being introduced formally into the licensing process for nuclear power plants and other industrial facilities (3) in some countries. As an example Table 3 gives the schedule for use of PSA in licensing of nuclear plants in Finland.

TABLE 3. MINI-PSA

<table>
<thead>
<tr>
<th>YEAR</th>
<th>CONSTRUCTION</th>
<th>PERMIT APPLICATION</th>
<th>REVIEW OF THE MINI-PSA IN STUK</th>
<th>CORRECTION OF THE MINI-PSA</th>
<th>CONSTRUCTION PERMIT</th>
<th>PSA OF LEVEL 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATING LICENSE APPLICATION</td>
<td>PSA OF LEVEL 2</td>
<td>REVIEW OF THE PSA OF LEVEL 1 IN STUK</td>
<td>CORRECTIONS</td>
<td>CONCLUSIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPERATING LICENSE</td>
<td>CORRECTION OF THE PSA OF LEVEL 2</td>
<td>AFTER THE START-UP TESTING</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Above reference was made to PSA use outside the nuclear area have been cited. In particular the Seveso directives of the CEC (6) call for a mapping of potentially hazardous industrial installations in their Member States. In 1985 a new "Directive" calls for an impact analysis for private and public projects. Recently IAEA, ILO, UNEP, and WHO prepared a Project Document on Assessing, Controlling, and Managing Health and Environmental Risks from Energy and Other Complex Industrial Systems (7). The Project will encompass a number of risk management case studies on a regional basis and the development of a risk management procedures guide as outlined in Figure 1 (8). The work is complemented with data collection activities and training courses.

3. **Objectives**

It is clear from the above that the use of PSA is rapidly spreading throughout the world and across technologies. It is thus both unavoidable and necessary to develop PSCs with the general objective to make optimal use of the numerical results generated by PSAs to ensure safety and to balance investments in safety. More specifically Table 4 (3) lists a number of objectives which, however, cannot all be met by one single and simple PSC.
General Framework for Studies to be conducted within the Joint IAEA/ILO/UNEP/WHO Project on Assessing, Controlling and Managing Health and Environmental Risks from Energy and other Complex Industrial Systems

**FIG. 1.**

**TABLE 4 ASSESSMENT OF PSCs BY OBJECTIVES**

<table>
<thead>
<tr>
<th>OBJECTIVES</th>
<th>DESIGN TOOL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SYSTEM INTEGRATION</td>
</tr>
<tr>
<td></td>
<td>BALANCE IN SYSTEMS</td>
</tr>
<tr>
<td></td>
<td>DESIGN PRIORITISATION</td>
</tr>
<tr>
<td>PUBLIC SAFETY (REGULATORY REQ ) (DEFENSE IN DEPTH)</td>
<td>PREVENT</td>
</tr>
<tr>
<td></td>
<td>INITIATING EVENTS</td>
</tr>
<tr>
<td></td>
<td>ACCIDENT SEQUENCES</td>
</tr>
<tr>
<td></td>
<td>MITIGATE</td>
</tr>
<tr>
<td></td>
<td>CONTAIN</td>
</tr>
<tr>
<td></td>
<td>ESFs</td>
</tr>
<tr>
<td></td>
<td>SITING</td>
</tr>
<tr>
<td></td>
<td>EMERGENCY PLANNING</td>
</tr>
<tr>
<td>RISK MANAGEMENT</td>
<td>RESEARCH PRIORITISATION</td>
</tr>
<tr>
<td></td>
<td>PUBLIC ACCEPTANCE</td>
</tr>
</tbody>
</table>

168
4. PSA results

With this general objective in mind it is necessary before discussing PSCs to briefly review the strengths and weaknesses of the commodity PSA results, which will be measured by any such criterion.

PSA results are a systematic combination of the best available knowledge about safety in a quantitative (probabilistic) way. Attempts are being made to include qualitative information (9). PSA cannot substitute for lack of information. However, it can, because of its systematic procedure, help to identify where (important) information is missing. The mathematical treatment of data allows for an explicit analysis of uncertainties which is an advantage of PSA and not a drawback. Some of the uncertainties are statistical variations of parameters. The largest fraction, however, is contributed from subjective judgement of the experts, i.e. subjective judgement on the degree or lack of knowledge. Of course "unknowns" cannot be included.

Thus, results of PSAs are not a prediction of the future in a statistical sense. Probabilities of rare events can never be "verified" statistically. The analysis is done for exactly the purpose that what is being "predicted" will not happen. In this respect PSA modelling activities are similar to many other modelling activities, e.g. energy and econometric models. It should also be noted that decisions are not probabilistic, but they are either yes or no. Also results are not probabilistic: either core damage occurs or not. Also "right" decisions in a probabilistic (or in a general decision theoretic) sense can turn out to be "wrong" and vice versa. Thus, it can be concluded that the purpose of any analysis is to make informed decisions and not to predict the future.

4.1 Level-1 PSA results

The most important result of a level-1 PSA is the identification of dominant accident sequences. They allow to spot weaknesses in design, operation and maintenance and to evaluate the relative importance of safety systems or functions. This information is much more important than the bottom-line core melt number. However, it can be noted from Table 5 (11) that the relative contribution from certain accident sequences can be very different from plant to plant. Uncertainties are reasonably low.

Level-1 PSAs allow for effective hazard control.

4.2 Level-2 PSA results

Modelling the progression of a potential accident from core damage, eventual melt-through of pressure vessel, possible reactions and behaviour in containment, to eventual containment failure and radioactive releases is highly uncertain. The most important results are analysis of measures to mitigate consequences of an accident and information about the timing and magnitude of eventual releases, see, e.g. Figure 2 (12).

Level-2 PSAs allow to establish procedures for effective accident management.
### Table 5. Dominant Contributors to Core Melt, as Shown by Probabilistic Risk Analyses at Selected Plants (Adapted from NUREG-1050, USNRC Draft Report)

<table>
<thead>
<tr>
<th></th>
<th>PWRs</th>
<th></th>
<th>BWRs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Plant A</td>
<td>Plant B</td>
<td>Plant C</td>
<td>Plant D</td>
</tr>
<tr>
<td>Small LOCAs</td>
<td></td>
<td></td>
<td>18</td>
<td>14</td>
</tr>
<tr>
<td>Injection failure</td>
<td>—</td>
<td>—</td>
<td>14</td>
<td>67</td>
</tr>
<tr>
<td>LTDHR failure</td>
<td>48</td>
<td>27</td>
<td>—</td>
<td>12</td>
</tr>
<tr>
<td>Large LOCAs</td>
<td></td>
<td></td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>LTDHR failure</td>
<td>34</td>
<td>—</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>Interfacing LOCAs</td>
<td></td>
<td>—</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>Transients – PCS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of off-site power</td>
<td>14</td>
<td>14</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>Injection failure</td>
<td>38</td>
<td>—</td>
<td>34</td>
<td>21</td>
</tr>
<tr>
<td>LTDHR failure</td>
<td>34</td>
<td>—</td>
<td>—</td>
<td>34</td>
</tr>
<tr>
<td>Transients – PCS available</td>
<td>5</td>
<td>—</td>
<td>1</td>
<td>—</td>
</tr>
<tr>
<td>Injection failure</td>
<td>3</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>LTDHR failure</td>
<td>3</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ATWS</td>
<td>2</td>
<td>14</td>
<td>—</td>
<td>11</td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
<td>7</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

**ATWS**: Anticipated transient without scram.

**LOCA**: Loss-of-coolant accident; an interfacing LOCA is caused by a failure of the check valves that isolate the low-pressure injection system from the reactor coolant system.

**LTDHR**: Long-term decay heat removal, including recirculation and residual heat removal.

**PCS**: Power conversion system.

### Diagram

**Containmant Pressure Time History, Low Pressure Case**

**FIG. 2.**
4.3 Level-3 PSA results

Risk curves for societal risks as given e.g. in Figure 3 (13) or numbers for individual risk are highly uncertain, like most other estimates of public risk from potentially hazardous installations. They provide information for planning purposes (including siting), generic safety decisions, and, though limited, for emergency planning.

Level-3 PSAs allow to establish procedures for risk management.
5. **General framework for PSCs**

Based upon the foregoing it is suggested to explore the possibility to develop an integrated hierarchical framework for PSCs including three levels:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Public risk level:</td>
<td>Umbrella-type overall criteria</td>
</tr>
<tr>
<td>Objective:</td>
<td>general risk management</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Severe plant damage level with loss of main safety functions</td>
<td>To be defined as a result of PSA. For nuclear power plants severe core damage probability</td>
</tr>
<tr>
<td>Objective:</td>
<td>hazard control</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Safety functions performance criteria</td>
<td>To be defined as a result of generic insights from PSAs. For nuclear power plants this could include containment performance.</td>
</tr>
<tr>
<td>Objective:</td>
<td>licensing</td>
<td></td>
</tr>
</tbody>
</table>

All three levels of PSCs should of course be consistent, however, not necessarily in a strictly mathematical statistical manner.

Each criterion could be defined in 3 ranges, following the example of (14): unacceptable, reduction desired, acceptable.

Since PSA offers the advantage to explicitly treat uncertainties, each criterion could be established for 50% confidence and 90% confidence taking the respective PSA uncertainties into consideration (e.g. factor of 5 for safety functions, factor of 10 for severe plant damage, factor of 50 for public risk).

6. **Individual risk**

Most important for risk management purposes is to define limits for individual risk. Because of the nature of risk it might be necessary to separate between early and latent effects. Consider the artificial situation in Figure 4.

Person A has a $10^{-7}$ chance per year of being killed by overexposure, Person B has a $10^{-3}$ chance per year of being exposed to 1 rem, Person C will receive 1 mrem for sure. If all persons stay for 1 year, using a risk factor of $10^{-4}$ per rem, all three persons have the same risk of $10^{-7}$. Thus, from a risk management viewpoint such expectation number would be sufficient.
However, based on such a number there would be room to develop more sophisticated approaches in accordance with the legal requirements and established procedures in a country. It should be noted that the established radiation protection principles could be more easily extended to latent effects. Since the purpose of such an individual risk PSC is risk management, any such number would naturally be derived on the basis of comparative risk.

Person C:
\[ 4 \text{ year}^{-1} \cdot 10^{-3} \text{ rem} \]
\[ \text{ind. risk}: 10^{-7}/\text{year} \]

Person B:
\[ 10^{-3} \text{ year}^{-1} \cdot 4 \text{ rem} \]
\[ \text{ind. risk}: 10^{-7}/\text{year} \]

Person A:
\[ 10^{-7} \text{ year}^{-1} \cdot \infty \text{ rem} \]
\[ \text{ind. risk}: 10^{-7}/\text{year} \]

Individual risk of $10^{-7}$ per year from various probabilities of radiation exposure

FIG. 4.

7. Societal risk

Societal risk PSCs have the objective to prevent accidents which would affect a large number of people. It has been demonstrated repeatedly that expectation numbers of societal risk are a useless indicator. It thus seems to be necessary to develop limit lines in the probability – consequence dimension as the appropriate societal risk PSC.

Several approaches could be utilized here. A simple probability – consequence limit line is easy to understand but has the disadvantage that it theoretically allows for infinite risk. Even the further restriction by an individual PSC does not solve this problem but leaves too much arbitrariness to the analyst. A simple solution to this problem is to put the additional constraint that all possible accident sequences have to be grouped into e.g. 10 categories.

A somewhat similar solution to this problem is to split the limit line into a histogramme of consequence categories. The requirement is then that the sum of probabilities of all accident sequences leading to consequences within a given category has to be less than the given limit.

Since most PSA results are displayed in CCDF format it would be most useful to use the same format for the societal PSC.
The slope of a limit line has to be less than \(-1\) to achieve the objective. Suggestions range between \(-1.2\) and \(-2\). It should be noted, however, that too steep a slope will significantly influence the allocation of safety resources to the prevention of low-probability events at the expense of more frequent events. Studies performed so far in the nuclear area demonstrate that at present plants are overdesigned for the more frequent events (15).

This implication definitely demands the definition of a lower probability limit for events to be considered. As discussed above not much meaning in a statistical sense is attached to very low probabilities. Such events are thus also rather useless for consideration in risk management (e.g. less than \(10^{-7}\)).

The societal PSC should be consistent with an individual PSC. If based on comparative risk studies this would be naturally assured. Another approach has been presented in (14).

Separate societal PSCs have to be developed for early and latent effects.

Since the objective of this umbrella-type PSC is risk management it would be useful to provide for a property damage PSC including off-site and on-site cost. In order to be consistent the actual position of such a PSC depends on any cost-effectiveness criterion.

8. Cost-effectiveness PSC

It has been proposed that all PSCs bound an area where risk reduction is desired. This, of course is consistent with the objective to use umbrella-type PSCs for risk management purposes. Since all value judgements are contained in the PSCs, risk management based on cost-effectiveness analysis becomes straightforward. No aggregation of different risks is required, no trade-offs have to be performed (except public – occupational). The objective is to minimize the mathematical expectation value of societal risk at a given budget under the condition that the individual and societal PSCs are met. The appropriate numerical parameter is best obtained from comparative cost-effectiveness analysis rather than GNP. This parameter must, of course, take the particular situation of a country into account.

9. Core-melt PSC

Based on such umbrella-type PSCs a core-melt PSC could be derived for hazard control. It should be consistent with, but not strictly connected in a mathematical sense to the umbrella PSCs. The objectives would be to evaluate all generic questions about design, operation, maintenance, backfitting, etc. as outlined in Table 6 (16).
10. **Performance PSC for safety functions**

There seems to be general agreement that because of large differences in plant design it is not very promising to develop PSCs for accident sequences and initiating events. Rather it has to be investigated if it is useful to develop performance criteria for safety functions possibly including containment (3). This is an area which has not yet been systematically explored and more research is necessary to determine if performance PSCs can be developed for use in licensing.

11. **General open questions needing attention**

If performance PSCs for safety functions are feasible it would be possible to use a hierarchical approach to PSCs in licensing to allow for flexibility. If for new and unusual design the performance PSCs cannot be met it would be necessary to comply with core-melt PSC. If this is not possible it would be necessary to comply with individual and societal PSCs.

Such an approach would not call for sophisticated methods to demonstrate compliance.

It would not be necessary to call for a standardization of PSAs, however, it would be useful to establish quality assurance guidelines for PSAs and standard requirements including external events, common mode failures and human error.

As discussed before societal PSCs for risk management purposes require a limit on consideration of low probability events. This problem needs particular and urgent attention. However, if such PSCs are not part of a licensing process it should be easier to find a solution.
A more difficult problem which is still unresolved concerns the scaling of individual and societal PSCs regarding the size of the facilities. Should a 1000 MWe nuclear power plant be treated in the same way as a research reactor or a 5 man company producing heavy explosives? If the basis for any numerical values is negligible risk than no distinction is necessary. If it is based on comparative risk the answer is still open. A study (17) performed already a number of years ago and rather limited in its sample indicated hardly any relationship between acceptable risk and expected benefit.

Conclusion

Considering the present wide-spread use of PSA and risk assessment in general it is necessary to develop PSCs with the objective to make optimal use of the numerical results generated by PSAs to ensure safety, and to balance investments into safety.

In spite of some open questions it seems to be useful to explore the possibility to develop an integrated hierarchical approach to PSCs on the three levels of risk management, hazard control and licensing requirement.
THE USE OF PROBABILISTIC METHODS IN
THE LICENSING OF NUCLEAR POWER PLANTS:
A RECENT EXAMPLE

U. BÄVERSTAM, C. WIKTORSSON
National Institute of Radiation Protection,
Stockholm, Sweden

Abstract

In 1981 the Swedish government decided that the nuclear power plant at Barsebäck in southern Sweden should be provided with filtered ventilation. The main reason was to prevent severe ground contamination in case of an accident. A ventilating device was connected in late 1985.

The Government also decided that no later than 1989 all other Swedish power plants should be provided with some kind of devices assuring as good a protection for the population around these plants as around Barsebäck.

In handling this matter and the licencing questions connected to it our institute has partly relied upon probabilistic methods and considerations. In short, the following actions have been taken: The power plant owners have supplied our institute with results from systematic reliability studies (involving probabilistic arguments) and some preliminary suggestions for solutions. Combining these with results from probabilistic studies performed by ourselves and with a number of criteria for acceptance of risk (some of which probabilistic) we have formulated some conditions that must be fulfilled before licencing of the arrangements required. In the last stage of the process the plant owners are supposed to use as one tool probabilistic arguments to make sure that the conditions are fulfilled. The paper presents the working process in some details, with the emphasis put on the probabilistic approaches.

INTRODUCTION

Probabilistic Safety Criteria are not used in Sweden. However, probabilistic analyses and methods are used in different ways both by the authorities involved and by the plant owners. Recently a probabilistic approach was used in the handling of licensing questions related to mitigating devices to be installed on swedish power plants. Since the probabilistic aspects of this work may be of a more common interest they are here briefly described and discussed.
In 1981 the Swedish Government decided that the nuclear power plant at Barsebäck (BWR, 2 blocks of 1700 MW thermal each) in southern Sweden should be provided with filtered ventilation. The main reason was to prevent severe ground contamination in case of an accident. It was prescribed that more than 99.9% of the radioactive core content - except for the noble gases - should be retained in case of an accident. The decision was not based on technical safety considerations but mirrored society's high demands on safety with respect to severe ground depositions. A ventilating device (FILTRA) in accordance with the directions was connected in October 1985.

The Government also decided that not later than 1989 the remaining Swedish power plants should be provided with some kind of devices assuring as good protection for the population around these plants as around Barsebäck. It was explicitly stated that if other techniques could be found that gave results comparable with filtered ventilation, or if the assessment of the risks involved were substantially changed, then the safety conditions for the remaining Swedish power plants should be adjusted according to these findings. Thus the Government actually in an indirect way prescribed the use of probabilistic methods - firstly in the search for "comparable" techniques, and secondly in the risk assessment.

Since some "comparable" techniques could possibly offer much cheaper solutions than the very expensive FILTRA gravel bed, the power plant owners, not long after the Governments directions, started plant-specific analyses. The two companies involved - the state power board and the private company OKG - used somewhat different techniques, but both relied on systematic reliability analysis. Event tree techniques were used to find the sequencies having the highest probabilities for a core melt down. These sequencies were then analyzed by means of various computer codes to find the thermo-dynamical state in the containment, and the behaviour of the radioactive substances. Thus site specific release source terms were found.

A number of general measures to reduce the accident probabilities and possible releases were formulated. Some calculations of the effects on the surroundings from such releases were also made. The calculations were performed using weather parameters etc according to (slightly varying choices of) "most probable" conditions.

These results, together with some preliminary suggestions for solutions, were presented to the National Institute of Radiation Protection and the Swedish Nuclear Power Inspectorate during the spring of 1985. These authorities work with different aspects of the licencing question - NIRP with the environment, the Nuclear Power Inspectorate with the plant safety - and were expected to give status reports to the Government in late 1985. The authorities chose to write a joint report. In the present paper the work underlying the NIRP part of this will be discussed.
BASIC CRITERIA FOR ACCEPTANCE

At NIRP the work was started by a discussion of possible basic underlying criteria. These should mirror both the general view in the Governments FILTRA direction and the general radiation protection policy in Sweden. The following criteria were found:

1. The risks (for man and environment) should not be above the level that was demanded in 1981 for the Barsebäck power plant. Here "risks" means probabilities of unwanted events.

2. Sequences having very low probabilities (say less than 1.E-8 per reactor year) should be disregarded.

3. The probability for a core melt down must be kept at an "acceptably low" level regardless of its environmental consequences.

4. The total probability of health effects for any one individual should not be significantly increased due to the risk of a nuclear accident.

5. The probability of long lived depositions that prevent the use of land must be kept below a very low value, say 1.E-8 per reactor year.

6. The probability of acute biological effects on man must be kept below a very low value - probably that used in item 4.

7. Although expectation values are not very useful when dealing with low probability / large consequence events, the following was formulated as a necessary but not sufficient condition: The expectation value of the collective dose from an accident should be much less than the expected collective dose from time integrated releases.

From these criteria a number of conclusions could be drawn directly. So, for example, need not, and should not, large containment fractures be taken into account since they have very low probabilities. (Moreover, it can be questioned whether the FILTRA facility will substantially reduce the effects of accidents of this type.) Also, to ensure the same limitation of maximum consequences for an individual regardless of plant site, the largest acceptable releases must be the same for all reactor blocks. This in turn puts larger constraints on the larger reactors than on the smaller ones.

At this point in the work - or perhaps somewhat later - it was found necessary and also desirable to cut the problem in two. It was not found acceptable to combine the probabilities from the reliability analyses of the plants with the probabilities connected to the environmental dispersion due to a given release. The reasons for this (very important) departure from a pure probabilistic handling of the matter will be discussed below.
There were therefore two questions to be answered: i/ Are the probabilities of certain environmental consequences (as stipulated in the criteria above), given the dispersion source term, today assessed as significantly lower than they were when the FILTRA requirements were laid down? ii/ Is there an acceptably high probability that the safety arrangements proposed by the power companies would fulfill the requirements following from the answer of the first question?

CONSEQUENCES OF A GIVEN RELEASE

To assess the probabilities of environmental and health consequences and compare these with the corresponding Barsebäck/FILTRA results one would need some probabilistic calculations. However, neither had any full PRA been performed for the Barsebäck power plant with the FILTRA facility included (and lack of time did not permit us to perform any), nor had the power companies performed any full PRA for their suggested mitigating concepts. We therefore had to rely on approximate calculations. These were, however, in one important respect much simplified as compared to the usual case: As the NIRP staff was interested in limiting the acceptable amounts of nuclide specific releases, the difficult question of "true" source terms could be completely avoided. Thus, it was not necessary to handle parameters such as nuclide specific releases and delay times etc. (Considerations of this kind would rather fall under question ii.) However, some assumptions concerning heat content of the release etc had to be made.

As an aid in these assessments the results of a consequence analysis performed by NIRP back in 1979 (More effective preparedness, NIRP 1979, in Swedish), supplemented with some new calculations for selected nuclides, were used. An updating of the dispersion and dose calculations of the NIRP 1979 report showed that, with an unchanged source term, the results found in 1979 were still valid, i.e. they had not changed more than was judged insignificant.

In short the following conclusion was drawn: The criteria 1 and 3 - 7 can be regarded as fulfilled if the release of nuclides of importance for long time ground contamination is limited to 0.1 % of their amounts in a core of the Barsebäck size. A release of this size will possibly lead to restrictions concerning the use of land over a surface of approximately 10 square kilometers. Cs-134 and Cs-137 are pointed out as the most important nuclides in this category. However, all depositing nuclides having half lives of the order of a week or more are regarded as potentially of interest. Thus, also more long lived iodine isotopes must be regarded when they appear in depositing chemical forms.

Thus, the same release limitations as stated for FILTRA were found valid in this case (except possibly for a slightly more restrictive view of the iodine problem). This result can, however, not be interpreted as if the FILTRA requirements were
the optimal ones, but rather says that they fulfill the stipulations. The results of a thorough probabilistic treatment also including the accident probabilities might have given somewhat different results.

ASSESSMENT OF PROPOSED SAFETY ARRANGEMENTS

This matter concerns Nuclear Power Inspectorate rather more than NIRP. However, both authorities were of the same opinion: If an additional number of technical features were included, it was judged possible to achieve the required results along the lines proposed by the power companies. This implied that solutions, rather cheap as compared to the FILTRA concept, could be used. In this judgement the probabilistic analyses performed by the companies were of great value. However, the authorities relied upon them just to find the most probable accident sequences rather than to put numerical values on their probabilities. Evidently, the numerical values given by the power companies were regarded as ranking values rather than as nominal ones.

DISCUSSION

In dealing with this licensing case one might have expected NIRP to use probabilistic methods throughout. The basic information was there, incomplete but possible to use. Then, why was it not so? There seems to have been three main causes. First, there were two independent authorities handling this case, one mainly concerned with the interior of the plant, the other with the environment. This certainly complicated a common judgement of the probabilistic inputs. Second, and this is of course the crucial point, the NIRP staff was not willing to accept the probabilities calculated within the plant, based on event tree analyses, as "the same kind of probability" as the environmental frequentistic ones. So was it, for example, felt that common cause failures, unexpected external events, small operator mistakes etc could change the outcomes of the calculations significantly. Third, since no full PRA had been performed before the Government's FILTRA decision back in 1981, no good comparisons of probabilities could be performed.

This difficulty in comparing the probabilities was, however, also due to the formulation of the criteria for acceptance. These criteria, which by the way were formulated in a less stringent way in the report to the Government, did not fully specify how to deal with this licensing case. They can be regarded as necessary but not sufficient conditions. In order to have been quantitatively useful, however, especially the first of them should have been formulated in a more stringent way. The present wording did not give enough information on how to compare the "risks" of the proposed new devices with the "risks" of Barsebäck/FILTRA. (One of several interpretations could be that the "new" curves for cumulative probability versus consequence must not raise above the "old" one for any consequence, but several others are possible as well.)
USE OF RELIABILITY AND RISK STANDARDS AS BASES FOR ACCEPTANCE IN LICENSING AND REGULATION OF NUCLEAR POWER PLANTS

R. VIROLAINEN
Finnish Centre for Radiation and Nuclear Safety, Helsinki, Finland

Abstract

The prevention and mitigation of accidents in PWR and BWR type reactor plants is essentially based on the sufficient operability of certain primary safety systems.

To ensure sufficient reliability, the authority sets forth numerical reliability goal for the most important safety functions of new nuclear power plants. The unreliability of the function in question shall remain below this goal. To calculate the reliability of systems, one uses a data base which has been collected from the operating experiences of similar plants. If a data base of this kind is not available, a generic data base is utilized.

However no fixed numerical acceptance standards are set forth in advance for the probabilities of a core melt, but the estimated probabilities are compared with the known probabilities of a core melt at other nuclear power plants.

As concerns the operating plants it is defined in the Technical Specifications under what conditions the operation of the plant can be continued when faults have been detected in components important to safety.

However, the Technical Specifications do not cover all situations in plant operation. Especially if there is a hidden potential fault discovered after the commissioning of the plant, for example an initiating event that may damage systems important to safety, the decision concerning the shutdown of the plant and the urgency of the repair must be made utilizing a probabilistic criteria.
In cases like this, the authority requires that the power company estimate the annual risk of a core melt caused by the safety deficiency in question. The authority will perform an independent estimate and considers the shutdown of the plant and the urgency of the repair by comparing the risk of a core melt caused by the safety deficiency with the risk of a core melt estimated in connection with the PSA.

1 INTRODUCTION

The Finnish licensing authority has drafted a regulatory guide on probabilistic safety analysis. The guide contains a procedure for performing PSA studies for licensing purposes but also some numerical safety standards that the new plant has to meet. For operating plants, the guide sets forth a procedure for decision making in such potential fault cases where the Technical Specifications do not apply.

The prevention and mitigation of accidents in PWR and BWR type reactor plants is essentially based on the sufficient operability of certain primary safety systems.

To ensure sufficient safety of the new plants, the licensing authority has planned to set forth numerical reliability targets for the most important safety functions. The unreliability of the function in question shall remain below this target. To calculate the reliability of systems, one uses a data base which has been collected from the operating experiences of similar plants. If a data base of this kind is not available, a generic data base is utilized.

However, no fixed numerical acceptance standards are planned for the probabilities of a core melt, but the estimated probabilities are compared with the known probabilities of a core melt at other nuclear power plants.
As concerns operating plants, it is defined in the Technical Specifications under what conditions the operation of the plant can continue when faults have been detected in components important to safety.

However, the Technical Specifications do not cover all situations in plant operation. Especially if there is a hidden potential fault discovered after the commissioning of the plant, for example an initiating event that may damage systems important to safety, the decision concerning the shutdown of the plant and the urgency of the repair must be made utilizing a probabilistic criterion.

In cases like this, the authority requires that the power company estimate the annual risk of a core melt caused by the safety deficiency in question. The authority will perform an independent estimate and considers the shutdown of the plant and the urgency of the repair by comparing the risk of a core melt caused by the safety deficiency with the risk of a core melt estimated in connection with the PSA.

2 CONTENT OF THE STANDARDS

2.1 Standards for safety functions /1/

The prevention and mitigation of accidents in PWR and BWR type reactor plants is essentially based on the sufficient operability of certain primary safety systems.

Of primary importance both in PWR and BWR are the reliable reactor trip and feed water supply, which are needed in dealing with numerous transients. Other important features at a PWR plant include the operability of emergency core cooling in the case of a small reactor coolant leak, and at a BWR plant, the automatic pressure reduction with pool cooling.
At both plant types it is naturally important to maintain the containment integrity and to be able to reduce the pressure in the containment.

To ensure the high reliability of these functions, the licensing authority requires that their unreliability be with 95 % confidence below the following reliability standards.

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

To calculate the reliability of a function, one uses a data base which has been collected from the operating experiences of similar plants. If a data base of this kind is not available, a generic data base is utilized. To determine the confidence limits of the data base, one can either use the Bayesian method or classical methods.

Auxiliary and support systems, as well as any dependences between systems and components affecting the reliability of safety functions shall be included in the analysis.

2.2 Standards for operation /1/

The following is a description of a procedure that is applied in making a decision in a situation in which the
authorities have detected a "significant" defect affecting safety in the safety systems of a NPP. The premise is that the deficiency is of the kind not included in the Technical Specifications. Deficiencies of this sort could include, for instance, initiating events not noticed before, which in themselves cause a defect in the safety systems intended for the prevention or mitigation of the consequences of the initiating event in question (i.e. reason for a common-cause failure).

The detection of a "serious" deficiency in safety is first followed by an assessment of the significance of the deficiency, which should be as objective as possible. One way to make an assessment is to utilize the probability of a core melt (1/year) caused by the accident sequence(s).

To estimate the urgency of a repair on the basis of probability criteria, one shall know the planned (accepted) probability of a core melt at the plant during its lifetime and determine how high "one-time risk" can be accepted for the repair.

**Procedure**

It is assumed that the core melt frequency is constant for the whole lifetime of the plant.

Let the design limit (highest acceptance limit) for the probability of a core melt be $10^{-3}/30 = 3 \times 10^{-5}$ 1/a.

Melt frequency $f = 3.8 \times 10^{-9}$ h

It is detected that there is a safety deficiency. Its analysis shows that the actual melt frequency is higher than the planned.

For consideration of urgency it is required as a boundary condition that, during the time needed for the elimination of the deficiency, the probability of a melt does not rise higher than $10^{-5}$ and, as an additional condition, that
the accumulation of this probability does not take place in less than two weeks. Otherwise the plant is immediately shut down.

The increase caused by the safety deficiency to the planned (estimated) annual melt probability is analysed to form a basis for decision making.

The known increase in the melt frequency is calculated:

\[ \Delta f = \frac{\Delta P}{8760 \text{ h}} \]

The consideration of the urgency of the repair is accomplished on the basis of the above calculated increased accident frequency and the "one-time" risk accepted by the authorities, \(10^{-5}/\text{repair}\), as follows

\[ (f + \Delta f) t_r \leq 10^{-5} \]

where \( t_r \geq 2 \text{ weeks} \)

3 APPLICATION OF THE STANDARDS

3.1 Use in licensing

A PSA analysis is needed to verify that the NPP design successfully copes with the reliability standards set forth above. To ensure a realistic approach to the problem, the authority assumes that no overly conservative approximations be used in the analysis and, the other way round, the dependences - functional or statistical - are taken into consideration. This implies that, in the analyses, also non-safety systems available to support the safety systems be included in the safety functions. On the other hand, the common auxiliary and support systems that result in dependences between safety systems are to be taken into consideration as well.
A brief example of the application of the standard as concerns the loss of off-site power is given here. The respective event tree describing the power failure transient at Loviisa 1 plant is drawn in Figure 1.

The crucial accident sequences in the event tree are $T_{1}R$ and $T_{1}IJQ$, but a brief comparison indicates that $T_{1}IJQ$ gives the major contribution to core melt probability.

The probability of the sequence $T_{1}IJQ$ is as follows:

$$\Pr (T_{1}IJQ) = \Pr (T_{1}) \times \Pr (AFWS \text{ fails to start} \mid T_{1}).$$
Pr (Make-up connection fails $| T_1, I$) $\times$ Pr (Recovery of off-site power fails within 2 hours or Operator fails to initiate MFW supply after recovery of off-site power $| T_1, I, J$).

a) Auxiliary feed water system

$$C_1 = (D_1 D_2 + P_1 + P_{IM} + V_1)(D_3 D_4 + P_2 + P_{2M} + V_2)$$

b) Make-up system connection to feed water system

$$C_2 = (D_1 + P_1)(D_2 + P_2) + (D_3 + P_3 + W_5)(D_4 + P_4 + W_6) + V_7 + V_8 + V_9$$

c) Recovery of main feedwater system

$$C_3 = R + \bar{R} \times O$$

FIG.2. Reduced reliability block diagram for Loviisa 1 feedwater supply.
The solution of $\Pr (T^U) \Omega$ is based on the reduced reliability block diagram of feedwater function presented in Fig 2 and on the following facts and procedures:

- plant specific data (Table 1) is used in analysis excluding the CCF parameters that stem from American experiences.

**Table 1** Plant specific reliability data for feed water systems of Loviisa 1 (1977-1983)

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure mode</th>
<th>Failure rate period $(10^4 \text{ h}^{-1})$</th>
<th>EF</th>
<th>Unavailability $A_{50}$</th>
<th>CCF parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1;P_2$</td>
<td>AFW pump fails to start</td>
<td>70</td>
<td>680</td>
<td>2</td>
<td>0.024</td>
</tr>
<tr>
<td>$P_{1M};P_{2M}$</td>
<td>AFW pump maintenance</td>
<td>234</td>
<td>-</td>
<td>2</td>
<td>0.0042</td>
</tr>
<tr>
<td>$V_1;V_2$</td>
<td>MOV fails to open</td>
<td>11</td>
<td>680</td>
<td>1.5</td>
<td>0.004</td>
</tr>
<tr>
<td>$D_1;D_2$</td>
<td>DG fails to start</td>
<td>128</td>
<td>336</td>
<td>1.5</td>
<td>0.022</td>
</tr>
<tr>
<td>$D_3;D_4$</td>
<td>DG fails to start</td>
<td>628</td>
<td>-</td>
<td>2</td>
<td>0.042</td>
</tr>
<tr>
<td>$P_1';P_2'$</td>
<td>Make-up pump fails to start</td>
<td>21</td>
<td>2160</td>
<td>2</td>
<td>0.025</td>
</tr>
<tr>
<td>$P_3;P_4$</td>
<td>Manual valve fails to open</td>
<td>1</td>
<td>8760</td>
<td>2</td>
<td>0.0044</td>
</tr>
</tbody>
</table>

- the Multiple Greek Letter Method (MGLM) is applied in CCF analysis
- functional dependences are dealt with by using the support state approach
- uncertainties are described by lognormal distribution

- propagation of uncertainties is made by methods of moments

- feedwater supply function has to be recovered within 2 hours after loss of offsite power

The probabilities \( Pr(IJ) \) and \( Pr(Q) \) are independent of each other and can be resolved separately. The probability \( Pr(IJ) \) is \( 3.8 \times 10^{-4} \) and the respective error factor 3.65.

\[
Pr(Q) = Pr(R + \bar{R} \times O), \text{ where}
\]

\[
R = Pr(\text{Offsite power is not recovered within 2 hours}) = 0.2; \ EF = 2
\]

\[
O = Pr(\text{Operator fails to initiate MFW supply given offsite power available}) = 0.05; \ EF = 3
\]

The probability \( Pr(Q) \) is 0.26 and the error factor 1.85.

The median unavailability of the feedwater supply function given loss of offsite power, \( Pr(IJQ) \), is \( 1.0 \times 10^{-4} \) and the error factor 3.95. The respective 95 % confidence value is \( 4 \times 10^{-4} \), which means that the unavailability of Loviisa 1 feedwater supply at power failure does not meet the proposed safety standard \( 10^{-4} \).

3.2 Use in operation

In the autumn of 1984, it was found out by the licensing authority that a violent fire of the main transformer at Loviisa 1 could result in a loss of auxiliary and main feedwater supply as well as off-site power if the turbine hall collapses due to the fire. To evaluate the consequences of this "new" initiating event the licensing authority performed a risk analysis on this subject as follows.
1  the frequency of the violent fire of the main
transformer

\[ f = 1.67 \times 10^{-3} \text{l/a} \]

\[ \text{EF} = 3.1 \]

2  the collapse of turbine hall 0.5

3  the loss of AFWS and MFWS given the collapse of
turbine hall 1.0

4  connection of make-up system (in primary system) to steam generators not accomplished within less than 2 hours

\[ \bar{\lambda} = 0.04 \]

\[ \text{EF} = 1.6 \]

The respective sequence probability is

\[ P_{50} = 1.4 \times 10^{-3} \times 0.5 \times 1 \times 0.04 = 2.8 \times 10^{-5} \]

\[ \text{EF} = 3.4 \]

\[ P_{95} = 9.5 \times 10^{-5} \] (the authority wants to have 95 % confidence for decision)

The safety standard for continuation of operation was given

\[(f + \Delta f) t_r \leq 10^{-5}, \text{ where} \]

\[ f = 3.8 \times 10^{-9} \text{ h}^{-1} \] (planned core melt frequency)

\[ \Delta f = \frac{\Delta P}{8760 \text{ h}} = \frac{P_{95}}{8760 \text{ h}} = 1.1 \times 10^{-8} \text{ h}^{-1} \]

The allowed repair time for the defect was

\[ t_r = \frac{10^{-5}}{1.5 \times 10^{-8} \text{ h}^{-1}} = 670 \text{ h} \]
Because $t_r$ is more than 2 weeks the authority decided not to shut the plant down, but required that the utility had to eliminate the defect in the given time period. As a consequence of the decision, the 110 kV transformers were transferred to a safer place as concerns the fire of the main transformer, and the fire protection of the turbine hall was rendered more effective as well.

4 CONCLUDING REMARKS

In spite of the minor experiences in employing the safety standards in practice, it seems to us that even the limited efforts in applying the PSA methods in the way presented can give a significant contribution to the decision making in the licensing and operation phases of NPPs.

The uncertainties of the risk estimates may be quite moderate also in the case of new plants if the data base of the similar plants is available. For the operating plants, with the operating experiences of several years, the statistical uncertainties are usually small, which gives a good confidence to the decision making.

From the point of view of the decision making even the limited safety standards, as presented above could be of value, because several PRA studies indicate that the few most important sequences usually cover 70-80% of the total core melt probability.

Further, the limited scope of the standard makes it easier to review the analyses more thoroughly.

REFERENCES

1. Probabilistic safety analysis in the licensing and regulation of nuclear power plants, Guide YVL 2.8, Draft 2, Finnish Centre for Radiation and Nuclear Safety, November 1985

COMPARISON OF DIFFERENT SOCIETAL RISKS:
A NEW LIMIT-LINE CONCEPT

H.A. MUNERA
Nuclear Engineering Laboratory,
Institute of Energy Technology,
Swiss Federal Institute of Technology,
Zürich, Switzerland

Abstract

Natural and technological risks capable of producing large scale accidents are typically described by listing the number of events (n) observed during a specified time-period (T, say 20 years) causing X or more victims. Following the Reactor Safety Study (RSS), most analyses of large scale accidents have adopted a graphical representation whereby n/T is plotted against X. These graphs are the so-called frequency-consequence (f-C) curves. No particular pattern appears in the f-C curves that could hint at what a societally tolerable risk level could be.

Many of the proposed and/or adopted quantitative safety criteria for nuclear power plants (NPPs) are based on limit-lines, somehow related to f-C curves as reviewed by the author elsewhere (Munera and Yadigaroglu, 1985).

An alternative interpretation of the same statistical data identifies two random components for each societal risk, namely:

1. The total number of accidents N during the observation period T. Although its probability distribution may be unknown, the accident rate \( \lambda = N/T \) provides a convenient descriptor.

2. The conditional probability distribution of X, given that an accident has occurred. A plot of \( F^* = n/N \) vs X immediately gives the empirical complementary cumulative probability distribution function (CCPDF).

In the context of this model, it is obvious that f-C curves are but plots of \( \lambda F^* \) vs X (Munera, 1985).

We re-analysed under the previous model the empirical data collated by Coppola and Hall (1981) for natural disasters (hurricanes, floods, earthquakes, tornadoes) and technological accidents (transport, mining, fire and explosion) with the following results:

a. There is no particular pattern for \( \lambda \), which spans a rather short interval: 4 to 24 events/year for the total world, and 0.1 to 5 events/year for the USA.

b. There is a striking pattern for the total world plots of \( F^* \) vs X. Indeed, three regions are clearly identified: natural disasters (above), technological accidents (below), and an intermediate empty zone.
It is suggested that the envelope of technological accidents constitutes a societally maximum tolerable technological accident (MTTA). Predictions of NPPs risks in the USA (US NRC, 1975; Margulies and Blond, 1984) and the FRG (Bayer, 1985) are compared against the MTTA.

Finally, for regulatory purposes it is necessary to aggregate \( F^* \) and \( \lambda \). A sufficient and technically feasible approach to get around the aggregation problem is to establish two separate and independent criteria: one for the probability of having a large scale accident (this is related to \( \lambda \) above); another for the consequences, given an accident (this may take the form of a limit-line below the MTTA).

I. INTRODUCTION

Firstly, we establish the scope of this analysis. We focus on one component of societal risk: large scale accidents leading to early fatalities. By large scale accident we understand an event causing at least 10 fatalities (which was the statistical data immediately available to us). Other definitions of "accident" are, of course, possible; for instance, events causing at least one fatality. Accidents leading to delayed deaths are not addressed herein; an analogous and separate analysis can be carried out for such a different dimension of risk.

Natural and technological risks capable of producing large scale accidents are typically described by listing the number of events \( n \) observed during a specified time-period \( T \) (say, 20 years) causing \( X \) or more victims. Following the Reactor Safety Study, RSS (US NRC, 1975), most analyses of large scale accidents have adopted a graphical representation whereby \( n/T \) is plotted against \( X \). These graphs are the so-called frequency-consequence (f-C) curves. No particular pattern appears in the f-C curves; that could hint at what a societally tolerable risk level could be.

Many of the proposed and/or adopted quantitative safety criteria for nuclear power plants (NPPs) are based on limit-lines, somehow related to f-C curves as reviewed by the author elsewhere (Munera and Yadigaroglu, 1985).

In this paper we advance an alternative interpretation of the same actuarial database used by the RSS and updated by Coppola and Hall (1981). This exercise suggests a maximum tolerable technological accident (MTTA). For regulatory purposes, it is argued that a limit-line based on the MTTA plus a second criterion for the accident probability could eventually be acceptable to society at large.

II. UNDERLYING PROBABILISTIC MODEL

Munera (1985) has suggested that f-C curves may be rationalized as formed by two random components, namely:

1. The total number of accidents \( N \) during the observation period \( T \).
The empirical probability distribution of \( N \) typically is unknown; in some cases, however, it is reasonable to assume a Poisson law. For the case of one parameter probability laws, the distribution may be characterized by the expected value (mean). It is assumed in this work that the mean is described by the accident rate \( \lambda \), whose empirical estimate is \( \frac{N}{T} \).

The accident rate in a given geographical area reflects, among other things, the probability of accident per (conveniently selected) unit and the number of units.

2. The conditional probability distribution of \( X \), given that an accident has occurred. An empirical probability distribution can be immediately obtained from historical data. The observation period \( T \) should be long enough to have a significant number of events, but short enough to reflect current technological and safety practices. For example, Coppola and Hall (1981) used \( T = 20 \) years for technological accidents, and \( T = 40 \) years for natural disasters.

The distribution of \( X \) may be obtained, for instance, by plotting \( F^* = n/N \) vs \( X \). Such graphs are empirical complementary cumulative probability distribution functions, CCPDF (see Figs. 1 and 2).
In the context of this model, it is obvious that $f$--$C$ curves are but plots of $\lambda F^*$ vs $X$ (Munera, 1985).

III. THE EMPIRICAL DATA REVISITED

We re-analysed under the previous model the empirical data collated by Coppola and Hall (1981) for natural disasters (hurricanes, floods, earthquakes, tornadoes) and technological accidents (transport, mining, fire and explosion) with the following results:

a. There is no particular pattern for $\lambda$, which spans a rather short interval: 4 to 24 events/year for the total world, and 0.1 to 5 events/year for the USA, as seen in Table 1. Differences between the USA and the total world may be explained by the different number of units and—possibly in some instances—by a lower unit probability of accident.

b. There is a striking pattern for the total world plots of $F^*$ vs $X$. Indeed, three regions are clearly identifiable: natural disasters (above), technological accidents (below), and a transition empty zone (see Figure 1).
<table>
<thead>
<tr>
<th>Natural disasters during 1938–77. T = 40 years</th>
<th>HISTORICAL ACCIDENT RATE, events/year*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total World</td>
<td>USA</td>
</tr>
<tr>
<td>A. Hurricanes</td>
<td>5.20</td>
</tr>
<tr>
<td>B. Floods</td>
<td>8.15</td>
</tr>
<tr>
<td>C. Earthquakes</td>
<td>4.22</td>
</tr>
<tr>
<td>D. Tornadoes</td>
<td>1.98</td>
</tr>
<tr>
<td>E. Meteorites</td>
<td>1.x 10^{-4}**</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technological accidents during 1959–78. T = 20 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Aircraft</td>
</tr>
<tr>
<td>2. Marine</td>
</tr>
<tr>
<td>3. Motor–vehicle</td>
</tr>
<tr>
<td>4. Rail–road</td>
</tr>
<tr>
<td>5. Mining</td>
</tr>
<tr>
<td>6. Fire and explosion</td>
</tr>
<tr>
<td>7. Dam failure</td>
</tr>
<tr>
<td>8. LNG transport</td>
</tr>
<tr>
<td>New York harbor</td>
</tr>
<tr>
<td>California sites</td>
</tr>
<tr>
<td>9. Nuclear power plants</td>
</tr>
</tbody>
</table>

* All figures from the actuarial data compiled by Coppola and Hall (1981), except as noted.
** Calculated (from US NRC, 1975).
*** Calculated (from Coppola and Hall, 1981).

Since the technological accidents shown in Fig. 1 are due to familiar technologies, it is suggested that the envelope of $F^*$ constitutes a societally maximum tolerable technological accident, MTTA. This suggestion does not imply that accidents are acceptable, but just endured, by society. Indeed, efforts should be made to decrease the severity of the consequences of both natural and technological disasters; a good example is the USA, as discussed next.

c. The CCPDFs for technological accidents in the USA are slightly lower than those for the total world shown in Fig. 1, but not enough to justify a separate analysis. The same observation is implicit in Coppola and Hall (1981): they noted that $f-C$ curves in the USA are more or less parallel to the rest of the world.

1 The typical societal reaction to a familiar technological accident is to ask for more safety, but not to stop or forbid the technology.
Contrarywise, the CCPDFs for natural disasters are significantly lower than the rest of the world, as shown in Fig. 2. It is conjectured that this is a result of preventive measures (flood control, for instance) and sophisticated warning and rescue systems (not always available elsewhere).

It is noteworthy that the curves for tornadoes and floods lie below the MTTA, and are qualitatively similar to technological CCPDFs. Given that tornado and flood-prone areas are inhabited and have undergone recent urban development, it is reasonable to argue that such risks are also tolerable to the U.S. society. These remarks lend further support to the concept of MTTA.

IV. COMPARISON WITH OTHER TECHNOLOGICAL ACCIDENTS

Risk studies of technologies without a sufficient accidental database typically report calculated $f$–$C$ curves. According to our definition of accident, $F^* = 1$ at $X = 10$. Then, the frequency at $X = 10$ equals $\lambda$. Dividing the different frequencies by $\lambda$ the CCPDF immediately obtains. Fig. 3 shows several curves for the USA (US NRC, 1975; Coppola and Hall, 1981; Margulies and Blond, 1984), and Fig. 4 shows nuclear CCPDFs according to the German Risk Study (Bayer, 1985).

![Figure 3. Technological accidents estimates in the USA](image-url)
The CCPDF for dam failures (Fig. 3) obtained from the RSS (US NRC, 1975) is almost identical to the total world curve for earthquakes (Fig. 1), excepting the very-high-consequence tail. The four events reported in the USA in the period 1959-1978 (Table 13, Coppola and Hall, 1981) agree fairly well with the same curve. Since societal concern for dam failures is not particularly strong (see, e.g., Munera, 1984), it may be conjectured that such accidents are perceived as closer to Nature than to technology.

The CCPDFs for LNG transport obtained from Fig. 12 of Coppola and Hall (1981) lie above the MTTA, but below natural accidents. These curves are very similar to the average curve for nuclear power plants (NPPs) obtained from the RSS, also shown in Fig. 3. Considerable public controversy has surrounded the development of and/or site-selection for both LNG and NPPs. Again, this fact lends support to the concept of "tolerable" accident, represented here by the MTTA. We note in passing that the upper part of the uncertainty band for NPPs reported by the Sandia Siting Study (Fig. 1, Margulies and Blond, 1984) lies well inside our region for natural accidents, whereas the lower limit is below the MTTA.

The most recent risk analysis for NPPs in the Federal Republic of Germany (Bayer, 1985) suggests that the nuclear accident is well below the MTTA. It is instructive to compare G3 in Fig. 4 to curve 3 (motor-vehicles) in Fig. 1.
V. POTENTIAL REGULATORY APPLICATIONS

For regulatory purposes it is necessary to combine $F^*$ and $\lambda$. One current limit-line approach multiplies the two components and selects an arbitrary shape of $\lambda F^*$ vs $X$, that purportedly takes into account the so-called "societal risk-aversion". All steps in this procedure are potentially controversial: the multiplicative aggregation, the linearity of the components, the shape of the curve and its relative position.

A sufficient and technically feasible approach to get around the aggregation problem is to establish two separate and independent criteria:

1. **Probability-consequence limit-line.** This limits the consequences given an accident. The upper-limit to this line is provided by the empirically determined MTTA. Depending upon her particular circumstances, every society would choose her regulatorily acceptable technological accident ($F^*$ vs $X$). Fig. 5 gives an example.

![Diagram](image-url)  
**FIGURE 5.** Regulatory limit-line similar to marine accidents
2. Probability of large scale accidents. As mentioned in section II this is related to \( \lambda \). A detailed analysis of empirical data may suggest the order of magnitude of a societally tolerable probability of accident.

The proposed approach is "objective" in the sense that there is historical experience and data for a gamut of different societal risks that may suggest limits for both criteria. On the other hand, it may be unnecessarily restrictive by leaving out the possibility of trading off accident rates against the severity of consequences. In common with all other limit-line approaches, it has the additional limitation that it does not provide means to decide whether the CCPDF of a project that crosses the regulatory limit-line is acceptable or not.

From the point of view of public perception of risks, the most salient component is the first one, i.e. the consequences given an accident. Indeed, when there is an accident the immediate reaction is to ask for the total number of victims. Concern for the accident rate usually comes up as an afterthought.

VI. CONCLUSION

The empirical data underlying the widely used frequency-consequence curves was reinterpreted as an accident rate and a conditional probability of consequences, given an accident. Three regions were identified in the graph of the complementary cumulative probability distribution function of \( X \) (CCPDF): natural disasters, technological accidents and a transition empty region. It was suggested that the envelope of the CCPDFs for technological accidents constitutes a maximum tolerable technological accident (MTTA).

For regulatory purposes, the problem of aggregating accident rates and CCPDFs can be circumvented by establishing two independent criteria, one for each component. Historical data may be used as a guide for the numerical targets.

Our analysis was based on the periods 1938-77 for natural disasters and 1959-78 for technological accidents. Use of more recent data may add detail to the high-consequence low-probability region, where some events have recently occurred (e.g., aircraft accidents and chemical explosions).

Ongoing additional work includes the extension of this approach to allow comparison of all CCPDFs to a regulatory risk-index, but this process requires the explicit introduction of subjective value-judgements as discussed elsewhere (Munera, 1985).

ACKNOWLEDGEMENTS

This research was partially supported by Research Contract between the International Atomic Energy Agency (Vienna) and the Nuclear Engineering Laboratory at the Swiss Federal Institute of Technology (ETH-Zurich). The views expressed herein are those of the author and do not necessarily represent the opinion of the IAEA or ETH.
REFERENCES


The paper addresses the following questions:

- To what extent are PSA's used in the nuclear safety?
- Does a risk approach imply a philosophical change in the traditional methods of design and regulations?
- Are PSA's formally incorporated in the licensing procedure and does the Federal Republic use, or does it plan to use, some type of quantitative probabilistic safety criteria or risk targets?

To what are PSA's used in nuclear safety?

In the Federal Republic there are two areas which are to be distinguished regarding PSA and nuclear safety

- the design basis area
- the beyond design basis area

Within the design basis area PSA's are required in the licensing for the assessment of sufficient reliability of the engineered safeguards and of the balance of the safety concept. In this context reliability analyses are performed for important systems and selected initiating events. Also, probabilistic analyses of more general nature and being not very detailed were conducted for specific rare external and internal hazards (e.g. airplane crash, earthquake, turbine disintegration).

Other important items are e.g. the application of the single failure concept with respect to admissible maintenance and repair times or with respect to design requirements of engineered safety features in case of events or combinations of events having a very low frequency of occurrence. Probabilistic evaluation methods are also allowed - but not required - in assessing the distribution, fall-out and activity deposition on ground and vegetations of the released radionuclides in case of design basis accidents for subsequent dose calculations.
Concerning the beyond design basis area, severe accidents are being investigated in extensive research programs. In this context, full-scope risk studies have been and are being performed. These works are sole research activities being neither directly nor indirectly part of the licensing. Results of such studies have carefully been analysed by industry and authorities. Discussions likewise took place in the deliberations of the Reactor Safety Commission. The discussions yielded the result that particular alterations are desirable from the safety point of view. As a matter of fact, some changes and improvements of systems were introduced by the utilities or vendors as an outcome of such recommendations. These measures were implemented after safety evaluation by technical experts and appraisal by the respective authorities. A formal incorporation of full-scope risk studies into licensing is judged to be neither necessary nor helpful at the moment.

Does a risk approach imply a philosophical change in the traditional methods in design and regulations?

In the traditional deterministic approach the safety of passive or active systems and components is achieved by conservative assumptions and adequate safety factors. Moreover, important deterministic engineering concepts have been established such as e.g. single failure criteria, physical separation, diverse and redundant designs and fail-safe principles.

Practical applications of these principles and criteria, however, could usually not be performed without considerations of frequencies of occurrence of initiating events which should be coped with, and their loads. In fact, many decisions in the past were based on an unspoken qualitative probabilistic concept.

Lack of experience and gaps of knowledge, however, very often forced to adopt an extremely conservative approach. So, the concepts of safety factors, single failure or diverse designs were very often formally applied to all relevant components and systems irregardless how frequent the specific component or system is called upon, how reliable it is and irregardless of the consequences of its failure.
Experience with reactor safety in the past has shown, that the deterministic safety concept should be implemented in a more differentiated way. To this end, probabilistic approaches are needed as supplementary tools. They have proven to be useful in many instances. It can be stated, that the real advances in nuclear safety have been achieved by a combination of deterministic and quantitative probabilistic approaches. Qualitative probabilistic arguments which are hidden in the traditional deterministic concept become explicit and quantitative.

Traditional methods in design and regulations are playing their dominant role and will continue to do so. The probabilistic methods will help to optimize a basically deterministic design and regulation to achieve a well-balanced safety concept.

In this way, PSA's are considered in the Federal Republic as an important additional tool to support, but not to replace conventional design and safety assessments.

PSA's are used in a process in which conventional approaches - including deterministic technical analyses and continued emphasis on defense in depth, siting and performance of personnel - retain their dominant and continuing value.

There are no needs to change such an approach.

Are PSA's formally incorporated in the licensing procedure and does the Federal Republic use, or does it plan to use, some type of quantitative probabilistic safety criteria or risk targets?

Again, we have to differentiate two areas, the design basis area and the beyond design basis area.

The design basis area

Although PSA's are not formally incorporated in licensing yet, there is a common practice to use PSA's in specific, selected areas. At present, quantitative safety targets or formal guidelines how to compare
the PSA-based results with design objectives have not been established. PSA results are used informally to yield qualitative and relative insights.

However, as far as system reliability analysis is concerned, more precise regulations are feasible in the near future.

Studies are being performed aiming at guidance which systems and events are to be investigated in the reliability analyses, which methods have to be adopted in this context and which reliability figures can be considered acceptable. The outcome of these studies will be deliberated by the respective authorities and expert commissions. No specific conclusions can be forwarded at the moment.

The beyond design area

The only comprehensive fullscope PRA for LWR’s is the German Risk Study. Phase B of this study is underway and will be completed this year.

In the judgement of an acceptable or unacceptable public risk the licensing authorities or courts orient themselves along the risk considered acceptable in other areas of life or - on a comparative basis - by the level of safety which is achieved by modern power plants as displayed in the German Risk Study.

Studies concerning risk oriented safety goals are being performed. These are solely research activities. Risk oriented safety goals which have been established in other countries or being in an exploratory stage, will be analysed carefully by the industry, authorities and respective technical experts. The Federal Republic is not as close to formulating probabilistic risk targets as other nations. It is not foreseen that quantitative safety goals will be developed or even introduced in the near future for regulatory purposes. As outlined before, a formal incorporation of full-scope PRA’s in the licensing procedure is not intended at the present time.
Summary

Within licensing the probabilistic safety assessment is an established and well-proven tool. It is, however, restricted to some specific items concerning the design basis area. PSA's are used to provide background information which supports decision making. No formal guidelines or quantitative safety targets have yet been established.

Full-scope risk analyses have been performed purely as research activities. They are not part of the licensing. Nevertheless, they did stimulate several changes and improvements in the plants.

Results of full scope risk studies are carefully studied by industry, authorities and legal bodies. However, a formal quantitative approach in the final appraisal of risk study results is not adopted. There are no needs to change this attitude.

Probabilistic concepts are under development in the Federal Republic aiming at an harmonization and concretization of various vague legal terms translating the legislation into practice. Ultimate goal is a more differentiated deterministic concept where probabilistic arguments play a supplementary role. Presently, the details of such a concept and how it will eventually be implemented cannot be anticipated.
The Regulatory Use of Probabilistic Safety Analysis in Argentina*

(abstract)

A.J. Gonzalez**
Comision Nacional de Energia Atomic, Buenos Aires, Argentina

This paper describes the regulatory use of probabilistic safety analysis by the Argentine competent authority. A historical background of the use of probabilistic approaches in the Argentine nuclear safety programme is presented. A probabilistic safety criterion enforced by the authority for the purpose of licensing nuclear power plants is described. The logic of the criterion is based on probabilistic safety goals derived from the individual-related requirement of the dose limitation system used for radiation protection purposes. The use of the criterion in the licensing process of the Atucha II Power Plant is described. Finally, the paper analyzes the limitation of the criteria, as an individual-related requirement, to take appropriately into account the overall expected impact from the source and the theoretical difficulties involved in the complementation of the criteria.

---


** Present address: Division of Nuclear Safety, International Atomic Energy Agency, Vienna.
Prospect Theory and Limit Lines*

(Abstract)

Jya Syin Wu-Chien, G. Apostolakis
School of Engineering and Applied Science,
University of California,
Los Angeles, California,
United States of America

Risk acceptance criteria in the form of limit lines are investigated in the context of prospect theory. This theory departs from utility theory in several respects, an important one being the use of weights other than probabilities in the evaluation of the expected impact of uncertain outcomes. Hypothetical functions reflecting certain attitudes toward consequences and rare events are developed and combined to produce several limit lines.

Key Words: Risk acceptance criteria; frequency-magnitude limit lines; utility theory; prospect theory.

RISK AVERSION IN RISK ACCEPTANCE CRITERIA*

(Abstract)

Jya Syin WU-CHIEN, G. APOSTOLAKIS
School of Engineering and Applied Science,
University of California,
Los Angeles, California,
United States of America

The risk aversive attitude that is included in some proposal risk acceptance criteria is examined. It is shown that it is a weaker attitude than risk aversion, as is commonly defined in decision theory. Consequently, the boundary curve separating acceptable and unacceptable regions does not have to be a straight line on the logarithmic frequency consequence space. A curve of variable slope would express the same attitude as long as the slope is less than -1.

RISK MANAGEMENT APPLICATION OF
FIRE RISK ANALYSIS*

(Abstract)

M. KAZARIANS, N. SIU
Pickard, Lowe and Garrick, Inc.,
Newport Beach, California

G. APOSTOLAKIS
School of Engineering and Applied Science,
University of California,
Los Angeles, California

United States of America

Probabilistic risk assessment (PRA) has shown that the contribution of fires
to the frequency of core damage and radionuclide release in some nuclear power
plants can be significant. This article discusses the use of PRA results in
fire risk management. The decomposition of these results leads to the
identification of the most important contributors to the risk and, thus,
allows for the identification of potential modifications that can have the
greatest impact on risk. This paper discusses the process of generating these
options and offers several insights that have been gained from an actual study.

Key Words: Risk management, fire risk, nuclear power plants.

* Presented at the First International Symposium on Fire Safety Science
Fire Safety Science
National Bureau of Standards
Gaithersburg, Maryland, USA
October 9-11, 1985
PRISIM is an IBM personal computer program that translates probabilistic risk assessment (PRA) information and calculates additional PRA type information for use by those who are not PRA experts. Specifically, PRISIM was developed for the U.S. Nuclear Regulatory Commission for use by their resident inspectors at nuclear power plants. Inspector activities are either scheduled or are in response to a particular status of a plant. PRISIM is useful for either activity.

To use PRISIM in response to a given plant status, the inspector calls on an interactive routine and designates which plant components are out of service. Results include:

1. a measure of instantaneous risk increase above the plant's average risk
2. an updated listing of plant components in order of decreasing importance
3. a listing of groups of events and component outages that will result in core melt arranged in order of decreasing importance
4. the decrease in instantaneous risk as the individual components that are designated as out of service are returned to service

In addition, when individual safety system components are removed from service, PRISIM will display a listing of plant components that are not covered by the plant's technical specifications and whose individual outage
will disable the safety system. Considerable additional component information is also available from PRISIM.

PRISIM also contains vast amounts of pre-processed information relevant to inspection planning and inspector training. In addition to instantly available licensee event report data, dominant accident sequence explanations and other data base information, PRISIM has routines that are directly related to the NRC inspection modules, i.e., the guidelines for scheduled inspection activities. For each module, PRISIM provides all the PRA type information that can be useful in making decisions required in executing the module activities. New component "importance" measures had to be derived for this portion of the program.

PRISIM is the most advanced software of its type available. All information is virtually instantaneously available even though a 20 mega bite hard disk is required for storing the information for one plant.

The first version of PRISIM was developed for the Arkansas Nuclear One - Unit 1 (ANO-1) Plant and is currently being updated to reflect the plant's changes that have been made to the design since the PRA for ANO-1 was completed. This paper describes PRISIM and its application to ANO-1 in detail.

A Probabilistic Risk Assessment (PRA) of a nuclear power plant is supported by a large body of information and wisdom that has not been fully utilized. This paper describes a computer program, called PRISIM, that allows a higher degree of utilization of such a PRA. PRISIM, in effect, translates many aspects of a PRA for use by those who are not PRA experts.

The results of PRISIM are formulated so that the effect of the uncertainty in the PRA failure data is minimized. This is accomplished by formulating results from the qualitative aspects of the PRA, such as the
failure logic models, and by binning probabilistic results in broad categories.

PRISIM was designed for the U.S. Nuclear Regulatory Commission (NRC) for use by their resident inspectors at nuclear power plants. The first application of PRISIM was to the Arkansas Nuclear One -Unit 1 (ANO-1) Plant. This version is currently being updated to reflect the changes that have been made to the plant's design since the PRA for ANO-1 was completed.

The program was written for an IBM XT personal computer with special high resolution graphics and a 20 mega-byte hard disk. To ensure success, PRISIM had to:

1. present dependable information useful in making inspection decisions
2. use the inspector's nomenclature, not PRA jargon
3. be convenient and fast

Present PRA documentation does not accomplish any of the above objectives; PRISIM accomplishes them all.

PRISIM aids U.S. NRC resident inspectors in activities that include:

1. determining an appropriate response to a given plant status
2. scheduling required activities
3. preparing inspection reports
4. training

To use PRISIM to decide how to respond to a given plant status, the inspector calls on an interactive routine and designates which plant components are out of service. He identifies the components on system schematics that are displayed on the computer screen. An example of such a schematic is shown in Figure 1.
Within 8 seconds the following information is available.

1. The factor by which the instantaneous core melt frequency increases above the average plant value because the specified components are out of service. This factor is a relative measure of the significance of the simultaneous outages of the specified components, and it gains additional meaning when compared to the factor for other groups of components that could be specified out of service.

2. A ranking of the components that are specified to be out of service according to the factor of decrease in the instantaneous core melt frequency when the components are individually returned to service. This ranking then gives the relative benefit of restoring each component to service.

3. A ranking of the components that are not specified to be out of service according to their contribution to the updated instantaneous core melt frequency. Since this list potentially contains an extremely large number of components, the list is truncated when the contribution to risk is very small. This list then ranks the components with respect to their impact on core melt frequency if added to the list of components specified to be out of service.

4. A ranking of core melt scenarios (each with a specified initiating event and possible additional component outages) according to their contributions to the updated instantaneous core melt frequency. This lets the inspector know, for the specified plant status, what the "weak links" are for core melt.
The interactive routine has limitations. The routine uses only those failure scenarios that comprise 85% of the plant's total core melt frequency. Therefore, it is possible that PRISIM will give incorrect, optimistic results. We estimate that such a misleading result will be encountered once every 3 or 4 years if the routine is used once a day. Misleading results would most probably be obtained when multiple front-line system components are failed, a situation where the inspector would not usually bother to query a personal computer for guidance.

In addition to the interactive routine, PRISIM has an efficient data base manager. The data base contains pre-processed screen images that are independent of the plant's status. The screen images contain both text and graph material. The data base manager selects a screen image from hundreds in the PRISIM data base and displays the image on a monitor in less than 1 second.

When the user enters the program, he is presented a series of screens with only menu options that allow him to quickly "zoom in" on the information of interest. Subsequent screens present information and provide options that allow the user to see more detailed information relevant to his needs. The following are examples of pre-processed information stored in the program.

Safety-Related System Importances

The PRISIM data base provides four types of risk importance measures for safety-related systems: safety assurance importance, risk reduction importance, risk sensitivity importance, and risk significance importance. Since inspection personnel are most concerned with preventing core melt, the measures of importance in PRISIM are based on core melt frequency. Table 1 defines these four importance measures.
<table>
<thead>
<tr>
<th>Measure of Importance</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Assurance</td>
<td>The factor by which risk increases when the equipment is out of service</td>
</tr>
<tr>
<td>Risk Reduction</td>
<td>The decrease in risk when the equipment is assumed to be perfectly reliable. (When normalized to the average risk, these results represent the likelihood that the equipment would contribute to a core melt if a core melt were to occur.)</td>
</tr>
<tr>
<td>Risk Sensitivity</td>
<td>The rate at which risk changes with changes in equipment failure probabilities (or frequencies)</td>
</tr>
<tr>
<td>Risk Significance</td>
<td>The combined risk reduction importance and risk sensitivity importance. (Equipment is grouped according to risk reduction importance. Equipment with a high risk sensitivity importance is then moved to the next higher group.)</td>
</tr>
</tbody>
</table>

**Safety-Related Subsystem Importances**

PRISIM provides the same four types of risk importance measures for safety-related subsystems that it provides for systems. It also lists the surveillance tests for each subsystem and indicates whether each test is an integral test. If a test is not integral, the components that are not tested are identified.

**Safety-Related Component Importances**

In addition to the same four importance measures, PRISIM provides information that is based on a particular component being out of service. This information includes lists of single component failures for the system when the specified component is out of service. These failure modes are of two categories: those that are covered by the licensee in response to the plant's technical specifications and those that are not.
Support System Interfaces

To identify dependencies among front-line safety systems and support systems (e.g., electrical power and service water) and among different support systems, PRISIM provides, for each system, a table that shows the support services required by components in that system.

Component Failure Data

Two types of information on component failure data are incorporated in the PRISIM data base. First, PRISIM includes summaries of licensee event reports (LERs), by component type, for the plant. Second, there are comparisons of plant-specific failure data with industry-averaged failure data for plant equipment. These comparisons highlight plant equipment that is more or less reliable than the industry average for equipment of the same type.

Fire Zones

PRISIM provides a ranking of fire zones at the plant with respect to their importance to risk. An assumption that is inherent in these rankings is that a fire will fail all equipment in the zone where it occurs.

Accident Sequences

The accident sequences that make the largest contributions to a plant's risk are listed in PRISIM. An inspector can command PRISIM to display information on a particular accident sequence. He will then see a description of the accident sequence and a listing of the most important causes of the sequence.

As an example of the use of the interactive routine in PRISIM, an inspector has specified a valve in the Emergency Feedwater System (EFS), shown in Figure 1, is out of service. The valve highlighted in Figure 1 being out of service will disable Train A of the EFS. Also, the inspector
has similarly specified a component in the Battery and Switchgear Cooling System is out of service. The effect is to disable Train A of this system. Using PRISIM to specify the plant status requires about 1 minute.

The program, in about 8 seconds, displays Figure 2. The instantaneous core melt frequency is 70 times higher for this plant status than it is under average conditions. The program user can now obtain additional information on the "Ranking of Safety-Related Equipment" is pursued in this example. The results shown in Figure 3 are available in less than 1 second. This list can be scrolled to obtain additional components of decreasing importance.

RISK IMPLICATIONS OF THE CURRENT PLANT STATUS

70 IS THE RISK FACTOR WITH THE FOLLOWING EQUIPMENT OUT OF SERVICE

- Emergency Feedwater System--Train A fails
- Battery and Switchgear Room Cooling System--CW Train A fails

RANKING OF EQUIPMENT NOT KNOWN TO BE OUT OF SERVICE

1. Battery and Switchgear Room Cooling System--CW Train B fails
2. Blockage of EFW Train A-to-Train B Crossover Line
3. Both safety/relief valves fail to reclose
4. Auxiliary Cooling Water System Isolation Valve CV2643 fails
5. Intermediate Cooling Water System Isolation Valve CV3828 fails
6. EFW Initiation and Control--Vector Signal Path 1D-22D fails
7. EFW Initiation and Control--Vector Signal Paths 2D-22D and 3D-22D fail
8. Both safety/relief valves open and fail to reclose
9. High Pressure Injection System Pump P36C fails
10. EFW Initiation Signal Paths AC01-AC04 and BD01-BD04 fail

ESC to return to the Selection Menu.

FIG. 2.

FIG. 3.
Demonstrating the dozens of features and information types available from PRISIM is far beyond the space limitations of this paper. The menu-driven program is user friendly and fast. The response to the program by the U.S. NRC and U.S. utilities has been extremely favorable. Plans include application to additional plants and implementation of an efficient system to keep the PRISIM versions for different plants updated.
After consultation within the Working Group on the Safety of Light Water Reactors, the Commission of the European Communities appointed a special group (February 1982) with the task to report on the status of the need, possibilities and limitations for overall safety objectives for nuclear power plants.

The mandate of this so called Task Force on safety goals/objectives included the following:

- To consider on a technical basis the need, possibilities and limitations of overall safety objectives for nuclear power plants, taking stock of various trial-approaches.
- To examine the merits and implications of the various approaches and to determine the degree of coherence and the divergencies in their possible applications.
- To summarise this by establishing a status report which comprises an outline of the degree of coherence and of the divergencies in the experts opinions.
- Depending on the outcome of item 1) to 3) advise the CEC on how and to what extent feed-back into USA-efforts presently underway is opportune and feasible.

In may 1983 the Task Force presented its first status report which contained general conclusions and perspectives for further activities among which one may quote the following:

- Important efforts have been and are being devoted to the development of explicit safety goals/objectives and their implementation in European countries and elsewhere. The emphasis lies on the quantification of these safety goals.
- This task is difficult for various reasons amongst which the most important being the uncertainties in the calculational tools i.e. probabilistic safety analysis (PSA). However the great importance of this approach is that it exhibits the risk of nuclear energy generation for individuals and for the public. This would enable a proper balancing of the benefits of this technology against the risk involved.
- It is not expected on a short-term basis regulatory requirements will be significantly influenced by a concerted approach in this matter.
- The Task Force gives the following major recommendation for further activities:
  - It should be investigated if it is possible to reach a coherent classification of incidents, frequency of incident sequences and related radiation dose limits and to reach agreement on standard models to be used for the calculation of the radiation doses.
With regard to this recommendation the Task Force pointed out that there appeared to be a considerable degree of coherence between the dose-frequency targets used in different member states but cautioned that the coherence might be more apparent than real, because of the different models and assumptions used in the different countries.

As a first step in the process to determine the extent of real agreement between the various dose-frequency targets used by regulatory groups/bodies, the Task Force agreed at its meeting in April 1985 to investigate the possibility of carrying out a benchmark exercise on the atmospheric dispersion, health effects models used in the member states. A special restricted meeting of the Task Force took place in December of 1985 during which the detailed aspects of the proposed benchmark exercise were classed out.

The objective of the benchmark exercise is to compare the various estimates of dose for the release of radionuclides to the atmosphere in particular conditions. Consideration is limited to the individual dose in close proximity to the nuclear installation and the methodology used for the calculation of radiologically relevant design basis accidents is generally applied.

The benchmark exercise was organised into a form which was as unambiguous as possible allowing to investigate all the parameters and variations on assumptions and models that are built into the calculations of dose which are used for regulatory purposes. The exercise is also structured in a way to present the parameters and results in a very comprehensive fashion so that comparisons can readily be made at intermediate stages in the calculation. Furthermore the very wide range of calculations will allow individual member states and organisations to reach a better judgement about the degree of conservatism in the approach that they have accepted for regulatory purposes and it is hoped that it will provide useful information about similarities and differences between the models used in the different countries.

Outline of benchmark exercise:

In the first stage of the benchmark exercise participants are asked to describe the atmospheric dispersion model used and to specify in considerable detail the assumptions that are built in the atmospheric dispersion model.

It is hoped that the type of release scenarios that are used by member states in their design basis calculations are covered by four release conditions; two of these release conditions are for point sources (release height 50m) and two are for releases into building wake. For each of these sets of two, one will have different durations:
  . a short release of half an hour and
  . a longer release of 10 hours.

The next stage of the exercise will be to calculate the contamination resulting for a unit release of $10^{10}$ Bq of a very long-lived nuclide. Participants have to calculate for each of the release conditions 3 different things:
  . the theoretical air concentration
  . the concentration of dry deposited material
  . the concentration of wet deposited material
Then the participants are asked to go through a reference case which has been established to give a standard set of parameters with regard to windspeed, rain intensity and deposition velocity so that one might see essentially differences in the modelling calculations rather than differences in assumptions.

In the next step participants are asked to calculate the whole body cloud dose on the plume center line for a release of $10^{10}$ Bq of each of Kr-88, Xe-133, I-135 (elemental) as a function of distance and stability category. The models used for regulatory purposes should be adopted for these calculations.

In a further step the participants are asked to present a table of their dose conversion factors for inhalation and ingestion dose calculations for the nuclides strontium, iodine and cesium.

The next step comprises dose calculations for unit air concentration and deposition level. The purpose of this exercise is to enable an intercomparison of dose predictions that is independent of the models adopted for atmospheric dispersion.

The last two calculations i.e. the overall intercomparison, comprise a calculation for unit release and a calculation for a notional source term which has a radionuclide composition broadly representative of design basis accidents for PWRs. As unit release, again, $10^{10}$ Bq of each of the following nuclides Kr-88, Sr-90, I-131, I-135, Xe-133, Cs-134, Cs-137 have been chosen in each of the four release conditions. Also for the notional source term, the cloud dose, inhalation dose, ingestion dose and deposited dose and the total dose from all sources are determined for the four release conditions.

The calculations are expected to be finished by end October 1986. It is not yet clear how long it will take a consultant to sort out the information into a comprehensive report. At the next Task Force meeting one will probably decide how to progress and fix the time scale for the publication of the report.

The following countries and organisations have agreed to participate on the benchmark exercise:

- Italy : ENEA/DISP
- France : CEA - CEN Fontenay-aux-Roses
- Federal Republic of Germany : GRS
- United Kingdom : HM NII
- The Netherlands : TNO

Other countries were considering to join in the exercise:
- Spain, Sweden and Finland.

Other activities of the Task Force comprise the following:

- Inventory of system performance targets
  - Performance criteria at plant function/system level
  - Overall system design criteria.
- Consultant work - Exploration of safety topics identified as contributing towards the development of a systematic approach to safety goals/objectives
  Chapter 1 - Plant performance targets
  Chapter 2 - Aspects of cost/benefit analysis
Main conclusions in the above said report by the consultant are:

1. The application of cost-benefit analysis to more severe accidents has reached a state of maturity. The difficulty is to get regulators and decision makers to actually specify the convention and rules for carrying out cost-benefit analysis, for instance to specify which things should be added to the benefit and which things should be added to the cost.

2. The best type of safety goals for the nuclear industry would appear to be one based on individual dose rather than societal risk as goals linked to societal risk depend heavily on site specific aspects.

The members of the Task Force recognise that the benchmark exercise described will only help to sort out the atmospheric dispersion-health effects part of the problem. The front end part, i.e. the modelling and assumptions relevant to releases within the primary circuit and the reactor containment are much more difficult to compare because this is so very plant specific. Nevertheless it has been suggested that members should submit their assumptions and fission product source terms for two accident sequences of major significance for the PWR. If the members would supply such information, then the Task Force will start a very tentative comparison some time in the future.
SOME QUESTIONS ON THE DEVELOPMENT OF PROBABILISTIC SAFETY CRITERIA

D.J. HIGSON
Australian Safeguards Office,
Australian Atomic Energy Commission,
Kings Cross, New South Wales,
Australia

Abstract

The paper addresses some basic questions, related to the development of probabilistic safety criteria, including:

(1) Is it possible to use the same criteria for nuclear and non-nuclear safety?

(2) What type of health effects should the criteria be based upon?

(3) What form should the criteria take?

(4) How should optimization be applied?

1. Is it possible to use the same criteria for nuclear and non-nuclear safety?

This is a crucial question and the answer may well be "no", because of the bearing which public acceptance has upon it. To most people, perceptions of risks are more important than the actual risks. The public generally sees in nuclear reactors a potential for disaster which it does not perceive in relation to any other source of risk. Therefore, I believe, there is certainly no future for uniform criteria if they are based on individual risk alone.

2. What type of health effects should criteria be based upon?

Possibilities include:

(i) Early deaths from acute effects.

(ii) Delayed deaths from latent somatic effects.

(iii) Cancer induction generally. This is a particular cause of dread. It is not at all clear to me whether the risk of delayed cancer is regarded generally with greater or lesser fear than immediate death. A complicating factor in the case of nuclear risk is that it may be dominated by the risk of thryoid cancer, which is rarely fatal.
(iv) Genetic and teratogenic effects which are also a particular source of dread.
(v) Other non-fatal illnesses and injuries.
(vi) Composite measures such as "life shortening" and "person-days lost".

I would expect the relative numbers of the different health effects to vary widely between one source of risk and another, e.g. for a nuclear power station compared with an LNG handling plant. It would therefore be inappropriate to use, say, the risk of cancer as the basis for uniform criteria.

I suggest using the total number of deaths (including untreatable cancers) which are attributable to the source of risk. Perhaps serious teratogenic effects should be added to this, but the problem of definition then arises. Death is, at least, clearly definable.

"Person-days lost" would also be a useful measure in cost-benefit analysis.

3. What form should the criteria take?

I believe that two types of limitation are required, viz:

(i) limitation of the risk to individuals at greatest risk; and

(ii) limitation of the collective risk to the general population (or some section of it as discussed in 5(ii) below).

It has been suggested to me that collective risk is adequately treated by optimisation. This may be so in the case of controlled exposures to risk e.g. the use of ALARA as recommended by the ICRP. In the case of accidents, I believe that criteria should reflect the public's dread of high-consequence events, which is not proportional to the sum of individual risks. There should therefore be a form of collective limit line (a CCFD would be best) discriminating against the likelihood of high-consequence accidents, i.e. with a slope steeper than 45 degrees in the high-consequence range. The attached figure illustrates a possible relationship.

It is important to distinguish clearly between worker safety and public safety. In relation to individual risk, I suggest that we cannot be concerned with worker safety because voluntary acceptance of risk would then come into the question. In any case, there are too many variable factors between industries to make it practicable. However, workers should probably be included in collective risk.
4. How should optimisation be applied?

It might even be asked "should optimisation be applied?". When limits are specified, there is a tendency to work exclusively to them, and to ignore optimisation. For example, in radiation protection it is far more common to find reference to the ICRP's recommended dose limits than it is to find an application of the ICRP's ALARA recommendation. On the other hand, when no limits are specified, it is often the practice to reduce risks to "as low as reasonably practicable" (ALARP), often without any formal decision method. Canvey Island might be seen as an example of this.

I believe that limits and an optimisation strategy should both be applied, so that risks do not exceed certain levels and are as far below these levels as is reasonably practicable. This suggests a parallel with the ICRP's recommendations for controlled exposures to radiation. In the case of accidents, however, there are a number of difficulties in the way of applying the ICRP's ALARA methodology, viz:

(i) it depends on a linear relationship between risk and exposure, which is not valid for some risks incurred in accidents;
(ii) the variety of health effects involved in optimisation of accident risks makes it virtually impossible, and perhaps inappropriate, to assign a general cost-equivalence to detriment (e.g. $1000/person-rem);

(iii) cost-benefit analysis tends in practice to be open ended.

In relation to (iii), it should be noted that the USNRC (in its safety goals) and the UKNII (in its safety assessment principles) impose a lower "limit" to the application of optimisation of accident risk. In effect they invoke the "de minimis" principle, whereby trivial risks are ignored. They do not nominate upper limits to accident risk and there is therefore a danger that their "de minimis" levels will become regarded as upper limits. This would be unduly restrictive.

What is required, therefore, is:

(i) a limit above which all risks are regarded as unacceptable;

(ii) a method for cost-effectiveness evaluation, for reduction of risks as far as reasonably practicable below the limit; and

(iii) a maximum practical objective for risk reduction, below which risks are regarded as insignificant (i.e. a "de minimis" level).

The attached figure illustrates this proposal for the case of collective risk.

5. Population groups

(i) Individual risk

For controlled exposures to radiation, the ICRP recognises that it is usually not possible to identify the actual individual at greatest risk. It therefore recommends the postulation of a hypothetical critical group, representative of those individuals in the population expected to receive the highest dose.

The same approach might be taken to the application of the safety criteria for individuals in accident situations.

(ii) Collective risks

Definition of the relevant population group for the estimation of collective risk presents no problem
for health effects which have a threshold. For effects to which the linear hypothesis applied, however, some means of defining the limits of the group is necessary, otherwise effects extend indefinitely into space and time.

One approach would be to ignore contributions to collective risk from individual risks below a nominated cut-off. This cut-off might be the "de minimis" level mentioned above.

Alternatively, for power stations, assuming everyone in an industrial society benefits from electricity generation, consideration could be confined to the number of people served in proportion to generating capacity. Thus, for a 1000MW (e) power station, it would be reasonable to apply a collective safety criterion to approximately a million people at greatest risk from the station.

6. Application to Engineering

The risk to people around a potentially hazardous plant depends upon the distribution of population around the plant, the meteorological and other environmental characteristics of the site, the emergency measures which would be taken in an accident, the way in which the plant is maintained and operated, the engineering of the plant and the nature of the hazardous material etc. in the plant. Good engineering is crucial for safety.

Each engineering decision on the plant may effect the risk, but it would be impossible to check every decision against the overall criteria. Hence, it is necessary to be able to interpret the criteria in terms of the required performance and reliability of equipment, and standards of quality. These requirements and standards would be specific to the plant. Only the criteria could be general.

7. Treatment of Uncertainty

A high level of confidence is generally required in verifying compliance with limits. The shift of emphasis away from strict compliance with limits in the development of the US reactor safety goals appears to have been due to the substantial uncertainties associated with probabilistic analysis. Compliance with the much lower objectives of the safety goals (see 4 above) should generate a high level of confidence that unacceptable risks are averted.

This is another reason why plant-specific applications of probabilistic risk limits should be approached with caution. Probabilistic criteria may prove to be more applicable to the
review of the generic, deterministic safety requirements (as discussed in 6 above) than to the review of specific plants.

Uncertainties in estimating the number (or probability) of health effects may be greater in the case of non-nuclear risks than nuclear risks, particularly in relation to delayed effects.

The application of probabilistic analysis to optimisation presents less problems than compliance with limits because optimisation generally deals with the relative risks of different options, rather than the absolute values needed for a compliance-type of comparison with a numerical standard of acceptability.
<table>
<thead>
<tr>
<th>Country</th>
<th>Name</th>
<th>Organization/Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>Mr. A.J. González</td>
<td>ENACE S.A.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Casilla de Correo 1589</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(1000) Buenos Aires</td>
</tr>
<tr>
<td>Australia</td>
<td>Mr. G. Higson</td>
<td>Australian Safeguards Office</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P.O. Box 261</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kings Cross</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sydney, N.S.W. 2011</td>
</tr>
<tr>
<td>Austria</td>
<td>Mr. H. Böck</td>
<td>Atom institute of the Austrian Universities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schüttenstrasse 115</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1020 Vienna</td>
</tr>
<tr>
<td></td>
<td>Mr. C. Preyssl</td>
<td>Atom institute of the Austrian Universities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schüttenstrasse 115</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1020 Vienna</td>
</tr>
<tr>
<td>Canada</td>
<td>Mr. Z. Domaratzki</td>
<td>Atomic Energy Control Board</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P.O. Box 1046</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ottawa, Canada K1P 5SP</td>
</tr>
<tr>
<td></td>
<td>Mr. F.K. King</td>
<td>Ontario Hydro</td>
</tr>
<tr>
<td></td>
<td></td>
<td>700 University Avenue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Toronto, Ontario</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Canada M5G 1X6</td>
</tr>
<tr>
<td></td>
<td>Mr. V.B. Snell</td>
<td>Atomic Energy of Canada Ltd.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CANDU Operations – Sheridan Park 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mississauga, Ontario</td>
</tr>
<tr>
<td>Finland</td>
<td>Mr. R. Virolainen</td>
<td>Finnish Centre for Radiation and Nuclear Safety</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kalevankatu 44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>00180 Helsinki</td>
</tr>
<tr>
<td>France</td>
<td>Mr. P. Candès</td>
<td>CEA – I.P.S.N.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Centre d’études nucléaires</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Boîte postale no. 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>92265 Fontenay aux Roses</td>
</tr>
<tr>
<td>Germany, Fed. Rep.</td>
<td>Mr. P. Gottschalk</td>
<td>Gesellschaft für Reaktorsicherheit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Glockengasse 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>50000 Köln</td>
</tr>
<tr>
<td>Hungary</td>
<td>Mr. I. Gaacs</td>
<td>Technical University</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Budapest</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Budapest</td>
</tr>
<tr>
<td>Italy</td>
<td>Mr. A. Ferrelli</td>
<td>ENEA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Casella Postale 2358</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Viale Regina Margherita, 125</td>
</tr>
<tr>
<td></td>
<td></td>
<td>I-00100 Rome</td>
</tr>
</tbody>
</table>
Japan

Prof. Y. Nishiwaki
Atomic Energy Research Institute of Kinki University
Kowakae 3-4-1
Higashi-Osaka City

Netherlands

Mr. H.J. van Grol
Netherlands Energy Research Foundation
P.O. Box 1
1755 ZG Petten

Mr. M.F. Verstegen
Ministry of Housing, Physical Planning and Environment
Dr. von de Stamstraat 2
Leidschendam

Poland

Mr. T. Jackowski
Central Laboratory for Radiological Protection
ul. Konwaliowa 7
03-194 Warsaw

Sweden

Mr. U. Baeverstam
National Institute of Radiation Protection
Karolinska Sjukhuset
Box 60 204
104 01 Stockholm

Mr. Lennary Carlsson
Swedish Nuclear Power Inspectorate
P.O. Box 27106
102 52 Stockholm

Switzerland

Mr. S. Chakraborty
Swiss Federal Nuclear Safety Inspectorate
5303 Würenlingen

Mr. H. Munera
Eidg. Technische Hochschule
Institute für Reaktortechnik
ETH-Zentrum
8092 Zürich

United Kingdom

Mr. B. Edmondson
Nuclear Operations Support Group
Central Electricity Generating Board
Sudbury House
Newgate Street
London EC4P 4EB

Mr. M. Hayns
UKAEA/SRD
Wigshaw Lane, Culcheth
Warrington WA3 4NE

Mr. G. Webb
National Radiological Protection Board
Chilton
Didcot OX11 ORQ
United States of America

Prof. G. Apostolakis
University of California (UCLA)
5532 Boelter Hall
Los Angeles, CA 90024

Mr. J. Sniezek
USNRC
Washington D.C. 20555

Mr. J. Russell
JBF Associates, Inc.
1 Technology Park Center
Knoxville, TN 37932

International Organizations

CEC
Mr. W. Essler
Commission of the European Communities
Rue de la Loi 200
1049 Brussels

Mr. S. Harbison
Nuclear Installations Inspectorate (NIi)
St. Peter's House
Stanley Precinct
Balleol Road
Bootle L20 3H2
Liverpool, UK

OECD
Mr. J. Caisley
Nuclear Safety Division
38, boulevard Suchet
75016 Paris, France

IAEA Participants

Mr. M. Rosen/DTR-NEWS
Mr. F. Niehaus/Head, RRA-NENS
Mr. R. Aso/RRA-NENS
Mr. M. Cullingford/RRA-NENS
Mr. J. Ahmed/RPS-NENS
Mr. J. Fischer/SNI-NENS
Mr. E. Tansiti/SNI-NENS
Mr. G. Linsley/WM-NENF
HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed in the following country:

UNITED STATES OF AMERICA  •  UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA  •  Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA  •  Hunter Publications, 58 A Gips Street, Collingwood, Victoria 3066
BELGIUM  •  Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE  •  Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA  •  IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing
           IAEA Publications other than in Chinese: China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing
CZECHOSLOVAKIA  •  S.N.T.L., Mikulandska 4, CS-116 86 Prague 1
                  Alfa, Publishers, Hurbanovo námestie 3, CS-815 89 Bratislava
FRANCE  •  Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05
HUNGARY  •  Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1389 Budapest 62
INDIA  •  Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016
        Oxford Book and Stationery Co., Scindia House, New Delhi-110 001
ISRAEL  •  Heiliger & Co. Ltd., 23 Keren Hayesod Street, Jerusalem 04188
ITALY  •  Libreria Scientifica, Dott. Lucio de Biasio “seiou”, Via Meravigli 16, 1-20123 Milan
JAPAN  •  Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International
PAKISTAN  •  Mirza Book Agency, 85, Shahrah Quaid-e-Azam, P.O. Box 729, Lahore 3
POLAND  •  Ars Polona-Ruch, Centrala Handlu Zagranicznego, Krakowskie Przedmiescie 7, PL-00-068 Warsaw
ROMANIA  •  Ilexim, P.O. Box 136-137, Bucharest
SOUTH AFRICA  •  Van Schaik Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001
SPAIN  •  Díaz de Santos, Laguna 95, E-28006 Madrid
        Díaz de Santos, Balma 417, E-08022 Barcelona
SWEDEN  •  AB Fritz's Kungl. Hovbokhandel Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm
UNITED KINGDOM  •  Her Majesty's Stationery Office, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
USSR  •  Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200
YUGOSLAVIA  •  Jugoslovenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria