ORGANISATION FOR ECONOMIC CO-OPERATION
AND DEVELOPMENT
NUCLEAR ENERGY AGENCY
MULTINATIONAL DESIGN EVALUATION
PROGRAMME
SAFETY GOALS SUBCOMMITTEE

PROJECT USE ONLY
DISTRIBUTED: January 2011
ENGLISH TEXT ONLY

The Structure and Application of High Level Safety Goals

A Review by the MDEP Sub-committee on Safety Goals

MDEP STC Sub-committee on Safety Goals – January 2011

Contents

The Structure and Application of High Level Safety Goals:

A Review by the MDEP Sub-committee on Safety Goals

Executive Summary:

One of the aims of MDEP is to work towards greater harmonisation of regulatory requirements. To achieve this aim, it is necessary that there is a degree of convergence on the safety goals that are required to be met by designers and operators. The term "safety goals" is defined to cover all health and safety requirements which must be met: these may be deterministic rules and/or probabilistic targets. They should cover the safety of workers, public and the environment in line with the IAEA's Basic Safety Objective; encompassing safety in normal operation through to severe accidents.

All regulators have safety goals, but these are expressed in many different ways and exercises in comparing them frequently are done at a very low level eg specific temperatures in the reactor vessel. The differences in the requirements from different regulators are difficult to resolve as the goals are derived using different principles and assumptions and are for a specific technology. Therefore MDEP set up a sub-committee to investigate a different approach. This approach was to start with the top-level goals and to derive a structure and means of deriving lower tier goals that can be seen to be clearly related to the higher level ones. This approach has the potential to greatly assist in the process of harmonisation of regulatory requirements.

The paper reviews the high level goals used in MDEP countries and the relevant work of international groups. From these it draws broad conclusions that the form of the framework should be an Hierarchical Structure of Safety Goals, incorporating an extended Defence-in-Depth approach. The basis concept is that the higher level safety goals can then developed, in a coherent and consistent manner, into lower level safety goals and targets that can be applied within the design and operation of reactors, with a clear connection between the different levels.

This structured approach is technology-neutral and is sufficiently flexible that it can be used for developing and applying safety targets to water-cooled and non-water cooled reactor designs. The paper gives some examples of the way this could be applied, by demonstrating how current safety goals, typically used for LWR reactors, can be fitted to it and indicates the way lower tier goals for other technologies can be derived. It is important to emphasise that this work is not attempting to derive safety goals per se, but to derive a framework, and the examples are not intended as anything more than demonstrative.

The paper proposes that this structure of safety goals can be incorporated in an integrated process that can be used to provide a balanced decision considering all aspects of safety. However, it is not the intention of this paper to define detailed safety goals and it concludes that , to develop this work further, more contact with other organisations doing similar or related work will be valuable and add synergy.

I. Introduction

Nuclear safety requirements were developed decades ago using deterministic approaches with a defence-in-depth (DID) philosophy as the foundation of the regulations/requirements. However, some explicit and implicit probabilistic considerations were used: these ranged from splitting the design basis faults into groups according to frequency with different acceptable consequences, the use of engineering safety margins which had been determined heuristically to overtly conservative requirements such as the single failure criterion. Different approaches were used in different countries, with some using more risk-based approaches than others, but in all cases, a DID philosophy, centred on several levels of protection including successive barriers and conservative considerations to prevent the release of radioactive material to the environment, was, and still, is employed. Overall, this philosophy has resulted in an excellent safety record of nuclear facilities.

Nuclear facilities pose a range of safety issues. These may be due to normal operational exposures of workers and discharges to the public and longer term issues of storage of spent fuel and radioactive waste, but much emphasis has been given to the consequences of accidents, particularly to the public. Determining how to balance the safety measures needed to prevent and protect against this spectrum of unwanted consequences was difficult and led, in many cases, to overly conservative requirements in some areas, whilst possibly too low a level in others. Whatever, it was difficult to be sure whether the levels of safety achieved were balanced and appropriate to the particular situation. Increasingly, the emphasis was placed on risk assessments to support decisions and to incorporate lessons learned from operating experience and research results to obtain a more balanced approach. This has been especially true in the development of methods to analyse accidents.

High Level Safety Goals

In considering the acceptability of a nuclear facility in relation to safety, Governments and regulatory bodies define a range of legal, mandatory requirements which are supplemented by regulatory requirements which may not have a mandatory nature.

All countries have established occupational and public dose limits during normal operation, and these generally conform to the IAEA Basic Safety Standard[1], which is derived largely from the ICRP recommendations. In addition, many countries have developed deterministic and probabilistic goals, which are frequently expressed as numbers e.g. doses, frequencies of core damage and release quantities.

As noted in INSAG 25[2], the design basis analysis uses deterministic assumptions by postulating a set of initiating events and scenarios against which the plant has to be protected and designed within the limits of specified acceptance criteria. The likelihood of postulated events is estimated in a conservative manner, and the acceptance criteria allow increasingly severe consequences for accidents of decreasing initiating event frequency. Conservative assumptions are made and scenarios bounding other potential accidents of similar nature are looked for to ensure that the results provide a generally robust protection against radiation hazards and other harmful consequences.

In addition, Probabilistic Safety Analysis (PSA) [also referred to sometimes as Probabilistic Risk Assessment (PRA)] is increasingly being used by many countries to assist in safety decisions by the

[1] IAEA Safety Series 115 (In revision as DS 379)

[2] In preparation

nuclear industry and by the safety authorities. Many countries have developed probabilistic safety guidelines to compare with the numerical risk estimates from PSA: these have generally been defined as targets or goals that are not mandatory. Taken together, these criteria range from normal operation risk, societal risk, offsite releases, core damage, whilst other, lower level criteria, have been used in various risk-informed applications over the last few decades. Some countries have also developed criteria for long–term restrictions on the use of extensive areas of land and water, should a major accidental release of radioactivity occur.

Starting some forty years ago, efforts to consider the possible faults, accident progressions (fault sequences) and their consequences in a range of industries led to the development of what is known in the nuclear industry as Probabilistic Safety Assessment (PSA) or. This methodology, which has now reached a relatively mature level of sophistication, provides:

- an integrated and systematic examination of safety aspects of design and operation
- methods for incorporating experience with engineered systems
- identification of weaknesses in the design or operation through for example examination of importance measures
- methods for assessing competing risks and balancing them to achieve an optimal set of safety measures
- relative safety significance and importance of , structures systems, components and human actions
- more effective means of configuration control and maintenance
- formal evaluation and characterization of uncertainties
- human-system interfaces
- measures of overall risk
- where appropriate, a formal structure for safety decisions which will facilitate dialogue between industry and regulators
- a basis for communication of safety decisions to the public.

Significant advances in the PSA methodologies have been achieved in the last three decades. However, it is recognized that PSAs do not model all aspects of design and operation. This adds an additional level of uncertainty to the bottom line numerical estimates, which by the nature of the modelling, contain aleatory and epistemic uncertainties. Accordingly, in using calculated numerical results it must be remembered these are risk metrics and care must be taken not to assume that they are accurate measures of risk that can be compared with frequentist data from, say, road traffic accidents. Nevertheless, integration of deterministic (e.g. DID) and probabilistic elements, using risk as a decision-making paradigm to determine a balanced approach, leads to more coherent decisions.

An extensive body of experience with the development and the application of PSAs has been generated by many countries. Basically, all countries' fundamental objective is to ensure that nuclear facility operation will not lead to significant additional risk to the health and safety of the public, and will not adversely impact the environment. All countries utilize a Defence-In-Depth (DID) concept to make safety decisions. INSAG 12[3], provides an excellent discussion of the DID concept. Most, if not all, countries generally follow the IAEA standards and guides. The structure of the IAEA standards and guides is discussed below.

While many countries use PSAs as a supplement to deterministic requirements, some countries use

[3] Basic Safety Principles for Nuclear Power Plants 75-INSAG 3 Rev.1, IAEA, 1999

PSAs as a complement to the deterministic requirements. The complementary use of PSAs leads to identifying areas for safety enhancement and also supports flexibility in eliminating requirements if the requirement is shown through probabilistic analyses to have very low risk. The supplementary use of PSAs would allow imposing additional requirements based on the PSA results but not eliminate any deterministic requirements irrespective of the risk. Of course, all countries have established limits for radiological releases during normal operation and the fundamental requirements are based on deterministic defence in depth safety philosophy.

An NEA review[4] provides some useful basic guidelines that the regulator can use to assist in the judgments on the use of risk information. It is important to ensure that the PSA used to generate risk information for decision-making is of high quality by following accepted standards (e.g. those proposed by organisations such as ASME and ANS) and that current best practices are utilized in the conduct of those portions of the PSA where such standards are not yet available. Further, it is important that the operator and the regulator have competence in the methodology and fully understand its strengths and limitations.

Although the predominant type of reactor that is currently used world-wide is the LWR (and mostly PWR) there are several other types of reactor in use in various parts of the world and advanced designs under consideration include a wide variety of technologies. In addition, other nuclear facilities exist in many countries. Hence, to ensure that the safety of the population is consistently achieved, high level safety goals which can be applied to all types and designs need to be defined. Thus, the term safety goals must be recognized as covering the whole range of safety issues that need to be addressed, from normal operation, through to major accidents. From this basis, lower level safety goals can be derived for specific types of facility and design, in a coherent manner.

This paper discusses the role that probabilistic and deterministic elements can play in enhancing safety and also how the probabilistic and the deterministic elements can be integrated for safety decisions within a basic DID framework (See Section III below).

II. International Safety Considerations

Increasingly, the international nuclear community (operators and regulators) is using risk considerations derived from PSAs to assist in safety decisions. The applications of this methodology range from limited explicit use to having an overt policy to use PSAs wherever practical in the decision-making process. Increasingly, more and more countries are also adopting probabilistic targets to further enhance safety as well as apply a more coherent means for regulatory decisions. This section summarizes the way in which some countries and international organizations use, or propose to use, probabilistic approaches in making safety decisions.. A recent survey by NEA[5] has collected data from several countries. In general, a core damage frequency limit of 1 E-5 per reactor year and a large release frequency[6] of 1 E-6 per reactor year are being applied by most countries for new LWR-

[4] "Nuclear Regulatory Decision Making", ISBN 92-64-01051-3, NEA 2005

[5] NEA/CSNI/WGRisk (WGRisk Task (2006)-2 - Probabilistic Risk Criteria)

[6] Note, the precise definition of "large release" varies between countries: in some cases the word "early" as a moderator of "release"is included, this has not been used here for simplicity. The more words that are used the more it becomes necessary to define what is meant by the limit and how to treat similar but apparently excluded events eg

type reactors.

II.1 International Atomic Energy Agency (IAEA)

II.1.1 Safety Standards

The IAEA are mandated to produce safety standards, which they use in their own activities and which form a baseline for Member States in considering their own requirements. There are three levels of safety standards: Fundamentals; Requirements; and Guides.

The Fundamentals[7] provide the Safety Objective and ten Safety Principles emphasizing the need to assess and control the inherent risk. This document states "The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation".

This fundamental safety objective of protecting people — individually and collectively — and the environment has to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that facilities are operated and activities conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken:

(a) To control the radiation exposure of people and the release of radioactive material to the environment;
(b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
(c) To mitigate the consequences of such events if they were to occur.

Ten safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented in order to achieve the fundamental safety objective. The safety principles form a set that is applicable in its entirety; although in practice different principles may be more or less important in relation to particular circumstances, the appropriate application of all relevant principles is required. In considering safety goals, the following principles are of highest importance.

Principle 4: Justification of facilities and activities. For facilities and activities to be considered justified, the benefits that they yield must outweigh the radiation risks to which they give rise. For the purposes of assessing benefit and risk, all significant consequences of the operation of facilities and the conduct of activities have to be taken into account.

Principle 5: Optimization of protection: The safety measures that are applied to facilities and activities that give rise to radiation risks are considered optimized if they provide the highest level of safety that can reasonably be achieved throughout the lifetime of the facility or activity, without unduly limiting its utilization.

---

what is "large" and what is "early" and what are the regulatory requirements for a "small early release" or a "large late release". More explanation can be found in the WGRisk report.

[7] IAEA Fundamental Safety Principles [SF-1] 2006

The Safety Fundamentals add under this principle some further explanation: To determine whether radiation risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities. Where there are interdependences between related actions or between their associated risks (e.g. for different stages of the lifetime of facilities and activities, for risks to different groups or for different steps in radioactive waste management), these must also be considered. Account also has to be taken of uncertainties in knowledge

Principle 6, Limitation of risk to individual: Justification and optimization of protection do not in themselves guarantee that no individual bears an unacceptable risk of harm. Consequently, doses and radiation risks must be controlled within specified limits.

Principle 8, Prevention of accidents: The most harmful consequences arising from facilities and activities have come from the loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or other source of radiation. Consequently, to ensure that the likelihood of an accident having harmful consequences is extremely low, measures have to be taken:

Several IAEA Safety Requirements publications establish more specific requirements for risk assessment for nuclear power plants. The International Basic Safety Standards for Protection Against Ionizing Radiation develops the fundamental safety objective in terms of protecting people and the environment from harmful effects of ionizing radiation. Therefore, the system of protection and safety aims to assess, manage and control exposures to ionizing radiation so that radiation risks and health effects are reduced to the extent reasonably achievable.

The Safety Requirements publication on Safety of Nuclear Power Plants: Design [8] states that: "A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied. On the basis of this analysis, the design basis for items important to safety shall be established and confirmed". This document is currently at a late revision stage. A similar Requirements document[9] covers Commissioning and Operation of NPP has been recently published.

The recently published Safety Requirements on Safety Assessment[10] emphasizes the need for a comprehensive safety analysis stating that: "In most cases, the safety assessment includes a safety analysis, which consists of a set of different analyses for quantitatively evaluating and assessing challenges to safety under various operational states, anticipated operational occurrences and accident conditions, using deterministic and probabilistic methods as appropriate"

Actions, conditions or procedures for meeting safety requirements are defined in a new set of Safety Guides. These Safety Guides are prepared on the basis of a systematic review of all the relevant Requirements level publications. Currently, several of the documents are in the final stages of being published. In particular, there is a safety guide on deterministic analysis for NPP and two safety guides on PSA performance and application: Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants and Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants. The objective of these Safety Guides is to provide

[8] Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[9] Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards SSR Part,2/2 IAEA, Vienna (to be published).

[10] Safety Assessment for Facilities and Activities, IAEA, GSR Part 4, Vienna (2009).

recommendations for meeting the requirements of NS-R-1 and GS-R-4 in performing or managing deterministic, or Design Basis Analysis and a Level 1 and Level 2 PSA projects for a NPP[11].

A safety guide on severe accident management[12] provides recommendations on meeting the requirements of NS-R-1 and GS-R-4 for the establishing of an accident management programme to prevent and mitigate the consequences of beyond design basis accidents including severe accidents. The Safety Guide presents the overall concept of an accident management programme and the process of its development and implementation. The established requirements on severe accidents and accident management in the design and in the operation of nuclear power plants, as well as the requirement to determine whether adequate provisions have been made to accident management measures at each of the levels of defence in depth are addressed in the Safety Guide. A further safety guide [13]provides recommendations on meeting the needed radiation protection and radioactive waste management at nuclear power plants

The structure of safety standards relating to safety assessment and accident management is shown in Figure 1.

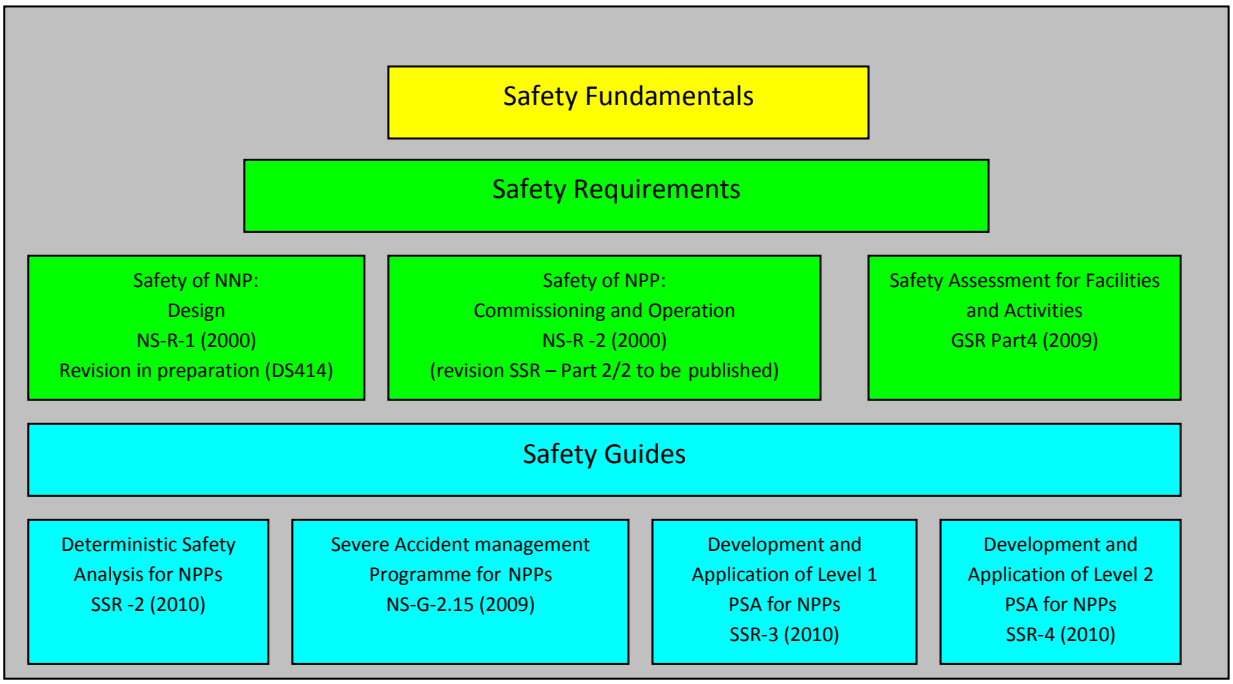

FIGURE 1 Structure of safety standards relating to safety assessment and accident management

II.1.2 INSAG

The International Nuclear Safety Group (INSAG) is a group of experts with high professional competence in the field of safety working in regulatory organizations, research and academic institutions and the nuclear industry. INSAG is convened under the auspices of the International Atomic Energy Agency (IAEA) with the objective to provide authoritative advice and guidance on nuclear safety approaches, policies and principles to the IAEA DG. In particular, INSAG will provide recommendations and opinions on current and emerging nuclear safety issues to the IAEA, the nuclear

[11] Safety Guides SSR-2, SSR-3 and SSR-4, cover Deterministic, Level 1 PSA and Level 2 PSA respectively.

[12] Severe Accident Management Programmes for Nuclear Power Plants NS-G2.15 IAEA Vienna 2009.

[13] GS-G-2.7 IAEA Vienna 2008.

community and the public. The INSAG has produced several reports relevant to the issues considered in this paper.

INSAG 12 (op cit) describes objectives (General nuclear safety objectives, Radiation protection objectives, Technical safety objectives) and principles (Fundamental safety management principles, Fundamental Defence in Depth (DID) principles, and General technical principles). The objectives define what is to be achieved and the principles state how the objectives could be met. In general, the concepts presented in the report are not new. Rather, the best current safety philosophy is put forward. The principles discussed include management responsibilities (safety culture, responsibility of the operating organization, regulatory controls and independent verification), DID and general technical principles (proven engineering practices, quality assurance, self-assessment, peer reviews, human factors etc.) In addition, the report discusses specific principles of siting, design, manufacturing and construction, operation, accident management, decommissioning, and emergency preparedness.

INSAG 12 includes a broad discussion of DID and INSAG 25 highlights some areas of DID. Defence-in-depth philosophy is a cornerstone of design/operational safety and the prevention of accidents. It provides for a series of successive barriers between the radioactive source and the harmful effects of radiation on people and the environment. Independence of the successive barriers provides protection against the risk of random failures of separate barriers although several barriers can be endangered in more serious accidents. As a whole, the set of barriers supported by independent reliable safety systems designed to protect their integrity provide a reliable containment of radioactive material within the NPP. INSAG 12 illustrates the concept and how it has been refined and strengthened through years of applications. In principle, all countries utilize the DID safety philosophy in the design and operation of nuclear power plants.

INSAG 12 also reflects on the use of PSA. For new nuclear power plants, it expects they will incorporate features such that the core damage probability will not exceed 1 E-5 per reactor year and that accident sequences that could lead to large early releases could be practically eliminated. Severe accidents that could imply late containment failure should be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and time. The analyses should include consideration of uncertainties.

The IAEA has recognized a need to consider both deterministic and probabilistic considerations to optimize public protection. This approach was presented to INSAG for discussion in a recent paper[14] by IAEA staff discusses the concept of tolerability of risks (see discussion under UK) and recommends that a) with level 1 PSA, a 'tolerability limit' for CDF of 1E-5/year may be used for new reactors, with lower risk to be aimed for where reasonable, and b) for level 2 PSA, for large release frequency 1E-6/year should be used as a reference level but it should be noted that INSAG 12 recommends "practical elimination" of accident sequences that could lead to large releases.

Adoption of INSAG 12 approach, in conjunction with additional considerations discussed later, may be an excellent initial step in achieving harmonization in safety requirements by the international safety community. It is recognized that INSAG 12 focus was on water reactor designs.

[14]"Safety Assurance and Goals of Generic NPP Designs", NSNI/SAS/2007,

II.2 Western European Nuclear Regulators' Association (WENRA)

The WENRA working group on Reactor Harmonization issued a report on WENRA Reactor Safety Reference Levels in January 2008. The report describes the WENRA views regarding safety of existing, operating NPP and includes a discussion of 18 areas (see Annex)

The report describes the safety strategy as follows:

"Defence-in-depth shall be applied in order to prevent, or if prevention fails, to mitigate harmful radioactive releases. The design shall therefore provide multiple physical barriers to the uncontrolled radioactive material to the environment, and an adequate protection of the barriers.

The design shall prevent as far as practicable:

- Challenges to the integrity of the barriers;
- Failure of a barrier when challenged;
- Failure of a barrier as a consequence of failure of another barrier"

The report goes on to discuss the importance of establishing the design basis and a set of design basis events to be considered. The report notes that engineering judgment and probabilistic methods can be used for the selection of the event combinations. In addition, the report notes the need to protect the containment against selected severe accidents. Further, classification of Structures, Systems and components (SSC) should be primarily based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment. The WENRA report proposes that for each existing plant design, a specific PSA should be developed for Levels 1 and 2[15] including all modes of operation and all relevant initiating events. The PSA should utilize up to date proven methodology. The PSA should be used to assess overall risk and to demonstrate balanced design, safety enhancements, training programs, and verification and test programs for risk significant items.

Currently, WENRA are developing Safety Objectives for new reactors. The objective of the present study is not to develop reference levels for new reactors nor to benchmark projects or designs.

The ongoing study addresses projects that are planned in the short term. The proposed safety objectives will have to be reviewed no later than 2020.

The IAEA Fundamental Safety Principles was found to be a sound basis for the safety objectives for new reactors. Based on that, common safety objectives for new reactors are proposed that are

- at high level and qualitative
- formulated in terms of safety improvements and
- cover technical issues and safety management

No consensus values for quantitative safety targets are presented. The need to be aware of differences in methodologies as well terminology, when making comparisons between numerical results in different countries, was emphasised.

The proposed safety objectives cover the following areas

[15] NB the definitions of level 1, 2 and 3 PSA are clear for LWR-type designs of reactor, for other designs these definitions may need to be revised.

- normal operation, abnormal events and prevention of accidents
- accidents without core melt
- accidents with core melt
- independence between all levels of defence-in-depth
- safety and security interfaces
- radiation protection and waste management
- management of safety

WENRA has approved the document for stakeholders comments by the end of June 2010.

II.3 United States

The fundamental requirements are based on deterministic defence-in-depth safety philosophy complemented by operating experience, research results and other studies.

For more than three decades USNRC has used probabilistic safety analyses to risk inform many of its' safety decisions. Following the accident at the Three Mile Island plant, many safety enhancements were imposed to further improve safety of the operating plants. However, the USNRC recognized that there was a need for better means to test the adequacy of proposed regulatory improvements. The USNRC believed that there was a need for more coherent and consistent regulation of nuclear power plants, a more predictable regulatory process, a public understanding of the regulatory criteria that USNRC applies, and public confidence in safety of operating reactors.

In 1986, after extensive deliberations, the USNRC issued a policy statement[16] . The safety goals focus on the risks to the public from accidents at nuclear power plants. The policy includes two qualitative goals which are supported by two quantitative objectives.

The qualitative goals are as follows:

- 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 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.

The intent of the first qualitative goal is to require such a level of safety that individuals living or working near nuclear power plants should be able to go about their daily lives without special concerns by virtue of their proximity to these plants. In fact, application of the first qualitative goal in the US would automatically lead to satisfaction of the second qualitative goal. The USNRC established the quantitative health objectives (QHOs), described below, in such a way that nuclear risks are not a significant addition to other societal risks.

- 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

[16] "Safety Goals for the Operation of Nuclear Power Plants" (http://www.nrc.gov/reading-rm/doc-collection/commission/policy/51fr30028.pdf)

the sum of prompt fatalities risks resulting from other accidents to which members of the U.S. population are exposed.

- The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0,1%) of the sum of cancer fatality risks resulting from all other causes.

The USNRC believes that this ratio of 0.1 percent appropriately reflects both of the qualitative goals-to provide that individuals and society bear no significant additional risk from accidents at nuclear power plants. The 0.1 percent ratio to other risks is low enough to support an expectation that people living or working near nuclear power plants would have no special concern due to the plant's proximity.

In applying the objective for individual risk of prompt fatality, the USNRC defined vicinity as the area within 1 mile of the nuclear power plant site boundary, since calculations of the consequences of major reactor accidents (accidents resulting in substantial core damage) suggests that individuals within a mile of the plant site boundary would generally be subject to the greatest risk of prompt death attributable to radiological causes.

In applying the objective for cancer fatalities as a population guideline for individuals in the area near the plant, the USNRC has defined the population generally considered subject to significant risk as the population within 10 miles of the plant site. The bulk of the significant exposure of the population to radiation would be concentrated within this distance, and thus this was considered to be the appropriate population for comparison with cancer fatality risks from all other causes. This objective would ensure that the estimated increase in the risk of delayed cancer fatalities from potential releases at a plant would be a small fraction of cancer deaths from non-nuclear causes. Moreover, the prompt fatality objective for protecting individuals generally provides even greater protection to the population as a whole. Using the US data, the QHOs expressed in the safety goals translate to 5E-7/ry individual risk for early fatalities and 2E-6/ry individual risk for cancer fatalities. It should be noted that these quantitative guidelines for early deaths and cancers are based on the US data base available during early 1980s. Advances in medical and other technologies along with improved understanding of the causes of cancers have likely reduced the likelihood of early deaths and cancer incidence as well as cancer fatalities from non-nuclear causes.

The average individual risk of prompt (or early) fatality and latent cancer fatality that is calculated in a PSA to compare with the QHOs is the total plant risk (e.g., accidents from full power, shutdown, internal and external events) incurred over a reactor year. However, the risk from security related events is not explicitly included since the likelihood of the threat is not known. This means the PSA results need to demonstrate that the total plant risk, i.e., the risk summed over all of sequences in the PSA, need to satisfy both the latent cancer QHO and the early fatality QHO. The USNRC adopted subsidiary quantitative objectives to act as surrogates for the QHOs that focus on designs. The surrogates are a core damage frequency (1E-4/reactor-year) and large release frequency (1E-5/reactor-year) for use in regulatory decisions on operating reactors. In the context of new reactors, the USNRC expects new reactor designs to provide higher levels of safety as compared to the current operating plants in the US.

Design certification of AP-1000 was based on satisfying the deterministic requirements based on DID considerations and the expectation that the design will satisfy a core damage frequency of 1 E-4 per reactor year utilizing safety systems only, and a large release frequency of 1 E-6 per reactor year utilizing safety systems only. Any reliance on non-safety systems to satisfy these metrics required some regulatory oversight (e.g. Technical specifications) over those non-safety systems. In addition, a Containment Performance Goal (CPG) was adopted by NRC to ensure that the containment structure has a high probability of withstanding the loads associated with severe accident phenomena, and that

the potential for significant radioactive releases is small. The CPG includes both a deterministic goal that containment integrity be maintained (stresses below ASME service level C limits for metal containments or factored load category for concrete containments) for approximately 24 hours following the onset of core damage for the more likely severe accident challenges. It should be noted that controlled venting of containment would not constitute containment failure, provided the venting occurs after approximately 24 hours following the onset of core damage. The availability of 24 hours provides considerable time for integrated emergency plans to be carried out. In addition, a probabilistic goal that the conditional containment failure probability (CCFP) be less than 0.1 for the composite of all core damage sequences assessed in the PSA is also applied. In the case of AP-1000, essentially all of the containment failure frequency results from either containment bypass, containment isolation failure, or early containment failure. For these sequences, the CCFP is estimated to be less than 0.1.

The surrogates of core damage frequency and large release frequencies are utilized to gain insights of risks from operation of LWRs. For certain non-LWR designs it may be very difficult to define core melt accidents and a different approach may be necessary to understand accident risks. NRC is considering an option to test an alternative approach of using a technology neutral probabilistic framework in conjunction with a deterministic DID approach using a pilot study. After experience is gained from this pilot program, more risk informed requirements could be developed for any commercial applications. One conceptual approach under consideration is documented in a recent report [17]The USNRC has not yet made its' decision to utilize any aspects of this report as it is still undergoing internal discussions. The report proposes an approach to integrate deterministic DID considerations along with probabilistic considerations to develop potential requirements and regulations. In terms of probabilistic aspects of licensing requirements, the following process was proposed:

- Specify the acceptability of the estimated plant risk,
- Develop criteria and guidance for identifying and selecting a complete set of licensing basis events (LBEs),
- Develop a frequency-consequence (F-C) curve to be used in establishing criteria for the LBEs to meet,
- Develop a procedure for classifying risk–significant systems, structures and components (SSCs) to ensure that the reliability and functionality of the SSCs are consistent with their design, and their intended maintenance and operation, and
- Ensure that adequate margin exists

An F-C curve, shown in Figure 2 below[18], was proposed based on the expectation that the QHOs and other NRC requirements [19]will be satisfied with the selection of this curve. The principle underlying the F-C curve is that event frequency and dose are inversely related. This principle, and the F-C curve, is broadly consistent with the approach of ICRP 64. Recommendations on the annual frequencies and doses to individual members of the public from accidental exposures are provided in ICRP 64.The doses cover a wide range of severity, from small exposures that are within regulatory limits to very high exposures that can lead to an early fatality. While the F-C concept has useful application as

[17] "Feasibility Study for a Risk-Informed and Performance Based Regulatory Structure for Future Plant Licensing", NUREG-1860, December 2007.

[18] (Figure 6-2 of NUREG-1860, modified to eliminate reference to 10CFR 50.34 and change "unacceptable" region to ALARP region)

[19] (10CFR Part 20, Part 50, Appendix I, etc.)

acceptance criteria for PSA event sequences, it is not a direct measure of risk and, therefore, cannot be used in the assessment of risk goals. It is, however, useful for helping to ensure that the doses which present the most risk to the public are of low likelihood. Event sequences with high frequencies need to lead to no consequences or very minor ones; event sequences that are rather infrequent can have somewhat higher doses associated with them. Chapter 6 of NUREG-1860 provides further details on Licensing Basis Events selection process and the utilization of the F-C curve.

Currently, USNRC is evaluating this and other alternatives in support of the development of regulatory requirements for new reactor designs.

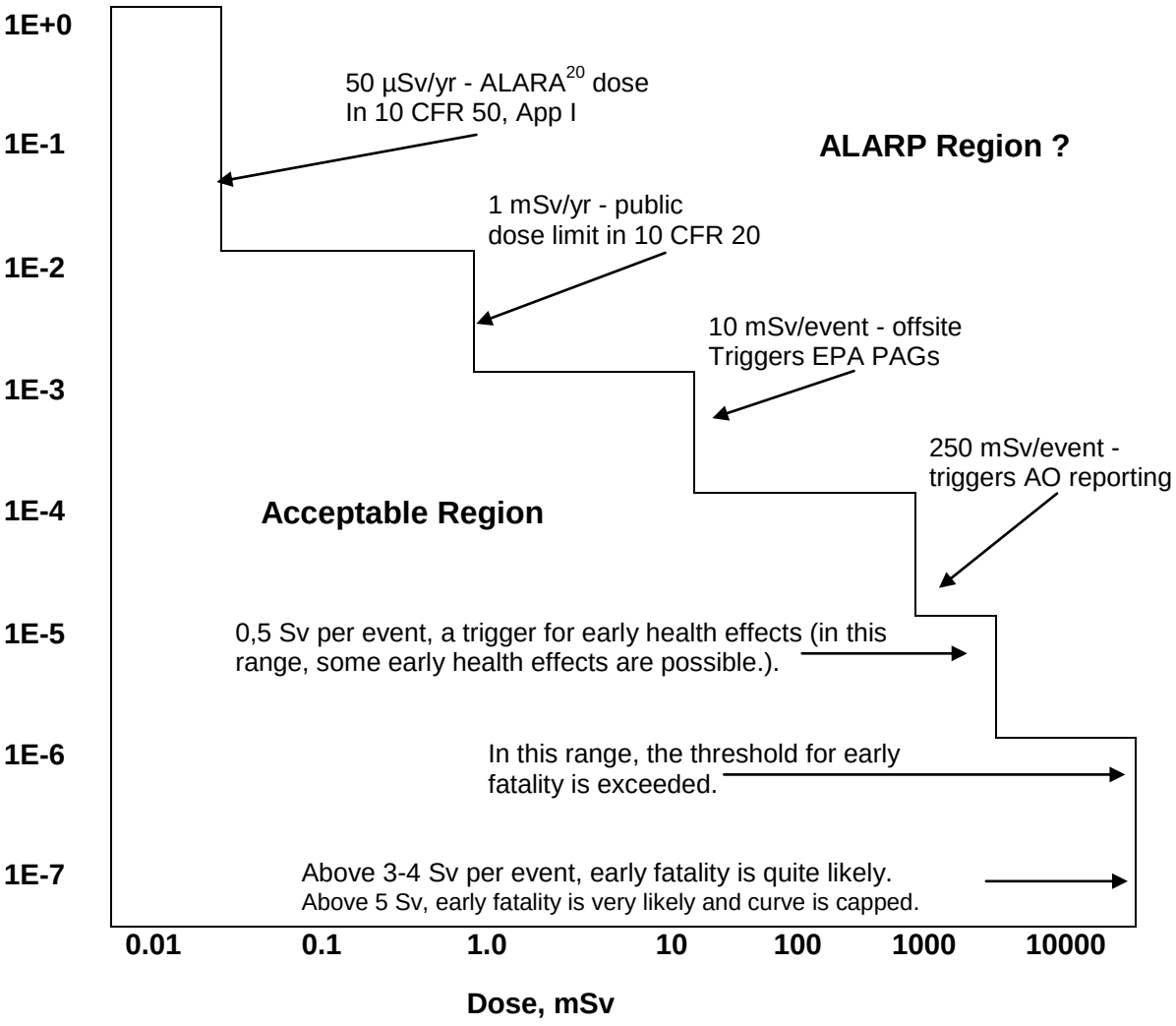

Figure 2 - Frequency Consequence Curve

II.4 France

On September 28, 2004 the Director General for Nuclear Safety and Radiation Protection sent a letter to EdF notifying them of the technical guidelines for the design and construction of the next generation nuclear power plants with pressurized water reactors such as the EPR.

[20] In applying the ALARA concept, social and economic factors should be taken into account

The significant improvement of the safety of the next generation of nuclear power plants, compared to existing plants, is specified by the following objectives.

a) For normal operation and abnormal occurrences, one objective is the reduction of individual and collective doses for the workers, which are largely linked to maintenance and in-service inspection activities. Reduction of the occupational exposures shall be aimed at by an optimization process taking into account the data obtained from operating experience. Consideration must also be given to the limitation of radioactive releases within the corresponding dose constraints, and to the reduction of quantities and activities of radioactive wastes.

b) Another objective is to reduce the number of significant incidents, which involves seeking improvements of the equipment and systems used in normal operation, with a view to reducing the frequencies of transients and incidents and hence to limiting the possibilities of accident situations developing from such events.

c) A significant reduction of the global core melt frequency must be achieved for the nuclear power plants of the next generation. Implementation of improvements in the "defence-in-depth" of such plants should lead to the achievement of a global frequency of core melt of less that 10-5 per reactor operating year, uncertainties and all types of failures and hazards being taken into account.

d) Moreover, an important objective is to achieve a significant reduction of potential radioactive releases due to all conceivable accidents, including core melt accidents. For accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant (no evacuation, no sheltering). Accident situations with core melt which would lead to large early releases have to be "practically eliminated" : if they cannot be considered as physically impossible, design provisions have to be taken to design them out. This objective applies notably to high pressure core melt sequences. Low pressure core melt sequences have to be dealt with so that the associated maximum conceivable releases would necessitate only very limited protective measures in area and in time for the public. This would be expressed by no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in consumption of food.

II.5 Finland

The Nuclear Energy Act requires that the safety of nuclear energy use shall be maintained at as high a level as practically possible. The Government Decree on the Safety of Nuclear Power Plants presents limits for the annual dose of an individual in the population for normal operation, for an anticipated operational occurrence and for accidents.

The limit for an anticipated operational occurrence is 0.1 mSv . The limits for accidents are:

- 1 mSv for Class 1 postulated accidents
- 5 mSv for Class 2 postulated accidents and
- 20 mSv for a design extension conditions (multiple failure situations and rare external events)

Class 1 postulated accident can be assumed to occur less frequently than once during hundred operating years but at last once during thousand years . Class 2 postulated accident can be assumed to occur less frequently than once during thousand years.

The Decree also presents the limit for the release of radioactive materials arising from a severe accident by stating that the limit is a release which causes neither acute harmfull health effects to the population in the vicinity of the nuclear power plant , nor any long-term restrictions on the use of

extensive areas of land and water. The requirement applied to long-term effects will be satisfied if there is only an extremely small possibility that, as the result of a severe accident , atmospheric release of cesium-137 will exceed the limit of 100 TBq .

As a plant level deterministic safety objective specific design requirements have been set forth for containment functions such that the containment is supposed to withstand the loads from severe accidents as well as challenges from various external threats.

In addition to the DID based deterministic requirements, Finland has also established probabilistic safety objectives that the new designs have to satisfy. For building a new NPP the applicant for the construction license has to submit level 1 and 2 design phase PRAs to STUK. These analyses have to meet the requirements for PRA scope, methods, and quality set forth in the STUK Guide YVL 2.8.

Among other things, the design phase PRA has to ensure that the safety of the plant is in compliance with the numerical safety objectives. The following high level design objectives are set forth in YVL 2.8:

-mean value of a core damage frequency, as estimated from a comprehensive level 1 PRA, is less than1.0E-5/yr

-mean value of a large radioactive release frequency (more than 100 TBq Cs-137), as estimated from a comprehensive level 2 PRA, is less than 5.0E-7/yr.

The Finnish nuclear legislation and the regulatory guides issued by STUK, the Finnish regulator, are available at www.stuk.fi. The STUK Guide YVL 2.8 provides the specific quantitative objectives.

II.6 United Kingdom (UK)

The UK employs Safety Assessment Principles (SAPs)[21] to establish their expectations for safety for nuclear facilities. Licensees are expected to use three forms of analysis to establish adequate safety for fault and accident conditions, namely design basis analysis, probabilistic safety assessment and severe accident analysis. They are intended to check that the necessary high level of safety has been achieved and provide important input to the design, operation and emergency preparedness of the facility. The fundamental requirement in relation to health and safety in the UK is to do whatever is reasonably practicable to control and reduce risks to employees and the public.

Reasonable practicability effectively requires a comparison of the reduction in risk with the sacrifice (time, trouble and money) involved in implementing further safety measures and if the latter is so large it is grossly disproportionate, then implementation is not required. This is often known as the requirement to reduce risks as low as reasonably practicable (ALARP). The demonstration of ALARP does not necessarily mean that a cost-benefit calculation employing a numerical risk analysis is needed, and there are many factors that contribute to a demonstration besides PSA. Indeed, there is a clear statement that such an approach should not be used to argue against good practices. Note that this requirement of UK predates the invention of PSA – the earliest reference being in 1878.

Some years ago, HSE, NII's parent body, was asked to spell out what the application of ALARP meant in

[21] The principles are documented in "Safety Assessment Principles for Nuclear Facilities", 2006 Edition, Revision 1.(www.hse.gov.uk/nuclear/saps/saps2006.pdf)

terms of the residual risk to people and it developed the concept of tolerability of risk[22]. The fundamental concept is that the there are risks that the public will just tolerate for the benefit gained from the activity and there are also lower risks which the public will accept with little or no concern. Between these levels efforts should be made to reduce the risks, ALARP. However, it is important to note that at the lower end, the level is used by regulators to determine when they will turn their attention to other greater risks, but a licensee must always reduce further if it is reasonably practicable to do so. There is no minimum level in law. Similarly, although it is policy in HSE to require risks to be less than the tolerable level, this is not a legal figure (except in a few specific cases, including radiation dose levels). The numerical values for these risk levels were determined mainly through a process of considering the rates of fatality in the UK. For example the tolerable level for workers was set at about the level of the most risky occupational deaths (ie deaths per worker per year), for the public this was set by road accidents. Acceptable figures were based on accidental death rates that did not seem to cause concern. This is all explained in the HSE documents quoted. The concept of tolerability of risk is represented in Figure 3.

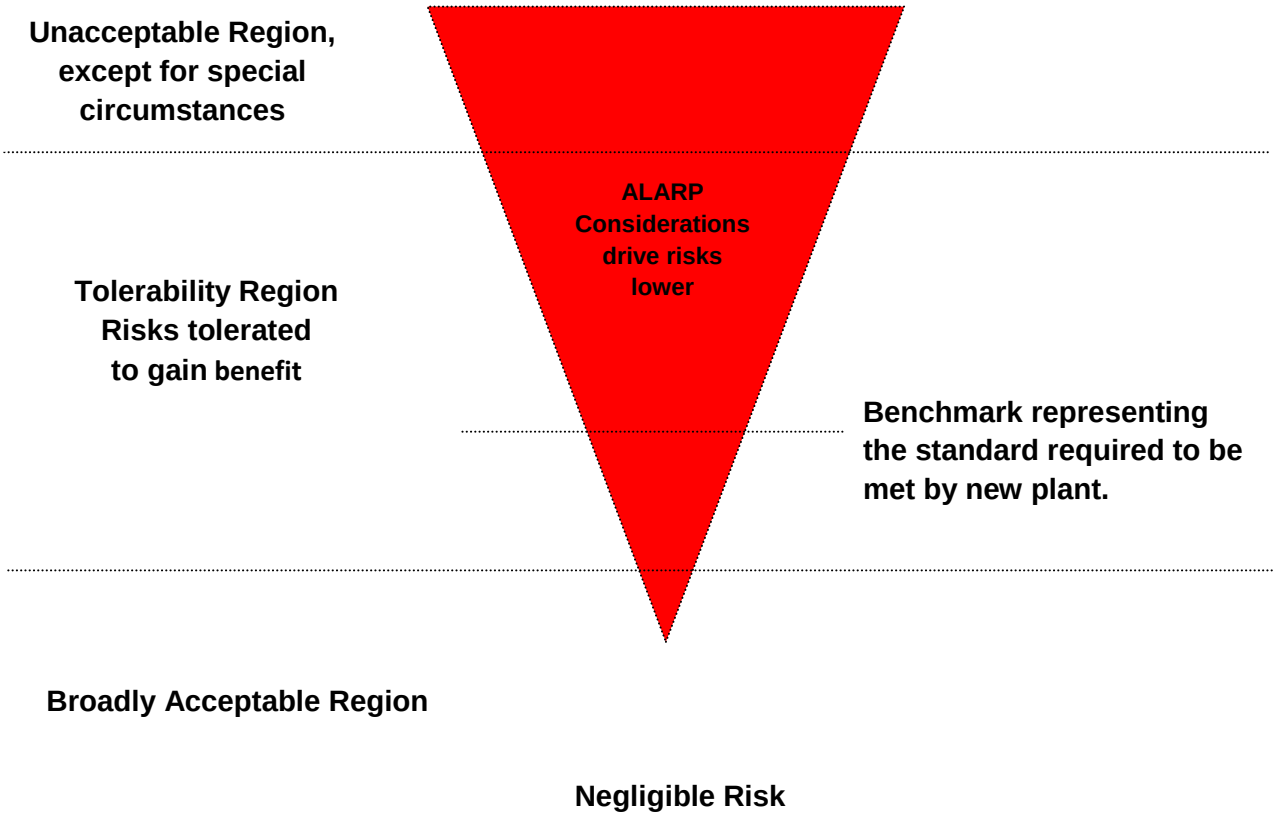

Figure 3 - Levels of Risk and ALARP

Within the nuclear regulatory area, the general approach has been developed and targets have been produced for a normal operation, design basis accidents and risk for both workers and the public. These are set out in SAPs and a general explanation is in paragraphs 568 to 584. An explanatory

[22] See "The Tolerability of Risk From Nuclear Power Stations", HSE, 1992 (www.hse.gov.uk/tolerability.pdf) and "Reducing Risks, Protecting People", HSE, 2001 www.hse.gov.uk/risk/theory/r2p2.pdf

note[23] describes in more detail how the targets have been developed from the overall UK targets.

The approach is to define Basic Safety Limits (BSLs) and the Basic Safety Objectives (BSOs) that translate the tolerability of risk framework and guide decision-making. HSE policy is that new facilities should meet BSLs. It is pointed out that the BSO doses/risks have been set at a level where HSE considers it not to be a good use of its resources nor consistent with a proportionate regulatory approach, to pursue further improvements in safety. The BSLs and BSOs have been developed for any person onsite and offsite during normal operation and accident conditions. Both individual and societal consequences are considered in establishing BSLs and BSOs. The target values for normal operation during a calendar year are established for employees working with ionizing radiation (BSL 20 mSv and BSO 1mSv) and other employees on the site (BSL 2mSv and BSO 0.1mSv). Similarly, target values, during calendar year of normal operation, are established for other persons onsite (BSL 10 mSv and BSO 0.5 mSv) and offsite (BSL 1mSv and BSO 0.02 mSv). The aim of design basis analysis is used to demonstrate that the design is robust and that there is no release of radioactivity or a dose, to workers and the public, above those allowed in normal operation. However, for infrequent initiating faults higher doses may be allowed, if it is not reasonably practicable to prevent them. Hence, dose targets, based on initiating fault frequencies, are also established (see table 1).

The targets for effective dose received by any person arising from a design base sequence are		
	BSL (mSv)	BSO (mSv)
On-site		
Initiating fault frequency exceeding 1 E-3 pa	20	0.1
Initiating fault frequency between 1 E-3 pa and 1 E-4 pa	200	0.1
Initiating fault frequency less than 1E-4 pa	500	0.1
Off-site		
Initiating fault frequency exceeding 1E-3 pa	1	0.01
Initiating fault frequency between 1E-3 pa and 1E-4 pa	10	0.01
Initiating fault frequency less than 1E-4 pa	100	0.01

Table 1: Dose targets for design basis accidents for workers and the public

In addition, targets for the individual risk of death to a person onsite or offsite from onsite accidents, resulting from radiation exposure are given as a BSL of 1 E-4 pa and a BSO of 1 E-6 pa. More detailed dose ladders are given such as the target values from accidents resulting in offsite releases presented in Table 2. The targets for societal risk of 100 or more fatalities, within the UK over 100 years, are presented in Table 3. Note that in the UK the definition of "severe accident" is different from that used by the IAEA which is an "accident beyond the design basis involving severe core degradation". The UK definition is "a fault sequence which leads to consequences [either to workers or the public] in

[23] "Numerical Targets and Legal Limits in Safety Assessment Principles for Nuclear Facilities", HSE, December 2006 (www.hse.gov.uk/saps/explanation.pdf

exceeding the highest radiological doses given in the BSLs … [for design basis sequences (see Table 1) or to a substantial unintended relocation of radioactive material within the plant which places a demand on the integrity of the remaining physical barriers".

It is important to recognise that some targets are for a plant, whereas others are for a site. In the UK the licence is for a site, regardless of the number of plants on it, so that the safety requirements must reflect the totality of plants on it. However, by also giving targets for single plants it is possible to carry out a design review independent of the site, but when a site is chosen, the presence of other plants, including potential interactions with them, must be taken into account in deciding whether it is acceptable to site the plant there.

The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site, are:

Effective dose, mSv	Total predicted frequency per annum (pa)	
	BSL	BSO
0.1 - 1	1	1 E-2
1 - 10	1 E-1	1 E-3
10 - 100	1 E-2	1 E-4
100 - 1000	1 E-3	1 E-5
> 1000	1 E-4	1 E-6

Table 2: Frequency dose targets for accidents on an individual facility - any person off the site (UK Target)

The targets for the total risk of 100 or more fatalities, either immediate or eventual, from on-site accidents that result in exposure to ionizing radiation are:

BSL	1 E-5 pa
BSO	1 E-7 pa

Table 3: Total risk of 100 or more fatalities (UK Target)

II.7 Canada

The Canadian Nuclear Safety Commission (CNSC) has established qualitative and quantitative safety goals and these goals are articulated in Regulatory Document RD-337. The qualitative goals are as follows:

- Individual members of the public are provided a level of protection from the consequences of nuclear power plant operation such that there is no significant additional risk to the life and health of individuals: and
- Societal risks to life and health from nuclear power plant operation are comparable to or less than the risks of generating electricity by viable competing technologies, and should not significantly add to other societal risks

•

The Canadian practice, [24]has been "… the incremental contribution to public health risk from nuclear accidents is a small fraction (<1%) of the background risk from cancer." For practical application, surrogate quantitative safety goals are established for the new designs to achieve the intent of the high level goals as follows:

1. Core Damage Frequency: Less than 1 E-5 per reactor year for significant core damage
2. Small Release Frequency: Less than 1 E-5 per reactor year for a release to the environment of more than 1 E 15 Becquerel of iodine-131 (potential for temporary evacuation of the local population)
3. Large Release Frequency: Less than 1 E-6 per reactor year for a release to the environment of more than 1 E 14 Becquerel of cesium-137 (Potential for long term relocation of the local population)

II.8 Japan

The Nuclear Safety Commission issued the "Interim Report on the Investigation and Review on Safety Goals" in December 2003, and the performance goals were established for nuclear installations in March 2006. The outlines of the goals are as follows.

Safety goals

The safety goal should be established for all activities in the utilization of nuclear energy that may have an adverse influence of radiation exposure on the public.

The objectives to establish the safety goals are as follows;

- To make it possible to assess regulatory activities in utilizing nuclear energy at various fields with same standards for reasonable and consistent evaluation among them,
- To make it possible to exchange opinions on the way of nuclear regulatory activities of national governments, such as establishment of guidelines and standards, among the national government and people more effectively and efficiently, and
- Make it possible for licensees to implement their independent risk management activities more effectively and efficiently to meet the expectation of the regulatory authority.

Along with these objectives, first of all, the safety goals are applied as reference to make judgment on the whole regulatory activity, in terms of rationality and consistency, and it is considered as appropriate to start with more general applications, on a specific facility, after abundant experience for the safety goals are accumulated.

The safety goal is of two fold. One is the qualitative goal, which is a controllable level of risk due to an accident that licensees must observe under the nuclear safety regulations. The other is the quantitative goal that specifies the numerical value corresponding to the acceptable level of the risk. In this context, the risk during the normal operation of nuclear power reactor facilities is excluded. And as the indices for quantitative goals, the death risk of the average individual of the public who lives in a certain range is used.

The proposal on safety goals are made of the following configurations.

[24] As reflected in "A Risk Informed Safety Assessment Framework for CANDU Reactors-NSS, March 2003",

1. Qualitative Goal

The possibility of health damage to the public by emission of radiation or release of radioactive materials accompanied with activities for utilization of nuclear energy should not meaningfully increase the risk of damage to the public's health in daily life.

2. Quantitative Goal

The mean value of acute fatality risk by radiation exposure resultant from an accident of a nuclear installation to individuals of the public, who live in the vicinity of the site boundary of the nuclear installation, should not exceed the probability of about 1E-6 per year. And, the mean value of fatality risk by cancer caused by radiation exposure resulting from an accident of a nuclear installation of individuals of the public, who live in the area but some distance from the nuclear installation, should not exceed the probability of approximately 1E-6 per year.

Performance Goal

It is reasonable to review and indicate the level that will be understood as the performance goal to conform with the safety goal, according to the characteristics of each accident that could occur at nuclear installations.

1. Indices for the Performance Goal

The following indices are also used, because they well represent the facility performance on the integrity of a reactor core and the integrity of the confinement function of a containment unit, and are clearly defined and appropriately quantified.

Index 1: Frequency of core damage (CDF)
Index 2: Containment loss-of-function frequency (CFF)

2. Safety Indices Values

The knowledge obtained from the PSA for domestic nuclear installations implemented by the national government, research organizations, licensee and the PSA results in the U.S. and other countries were studied as references, and the following indices values were proposed as the performance goals corresponding to the proposed safety goals.

Index value 1: CDF: 1 E-4 per reactor-year approximately.
Index value 2: CFF: 1 E-5 per reactor-year approximately.
These indices values shall be satisfied concurrently.

From now, studies for preparing a framework for use of performance goals in safety regulations, application to nuclear installations other than commercial nuclear installations, and a high safety level in future reactors are required

II.9 South Africa

In South Africa regulations on safety standards and regulatory practices lay down principle radiation and nuclear safety requirements which are applied to all nuclear installations and other regulated actions, and include the following:

1. Radiological dose and risk limits for the public and workers
2. Defence-in-depth
3. ALARA
4. Good engineering practice
5. Safety Culture.

These requirements are further expanded upon in regulatory documents, which address in addition to the above, requirements on the organization and safety related processes and programmes.

The radiological dose and risk limits for the public and workers (attached table) relate directly to the objectives of nuclear and radiation safety, and are therefore considered the most fundamental yardsticks against which to assess nuclear safety, contributing towards a more consistent and transparent basis for regulatory decision making. The dose limits are consistent with the Basic Safety Standards and are updated in line with ICRP/BSS recommendations. The risk limits were established in the 1970s in relation to other industrial and man-made hazards.

Basic principles underlying the risk criteria are as follows:

- The risks presented by a nuclear plant must not increase significantly the total population risk.
- The nuclear risks must compare favorably with those associated with other major industrial enterprises.
- Allowance must be made for a possible increase in the standards of safety demanded by society over the period – usually several decades - represented by the working life of the plant.

It is recognized however, that given the challenges of performing dose and risk analyses, including the issue of completeness of such analyses, these criteria are complemented by the above-mentioned requirements on defence-in-depth, ALARA and safety culture.

For imported technology the design basis and operating rules approved in the vendor country have typically been enforced in the nuclear installation licence so as to ensure a common basis with international practice. This is however required to be consistent with the dose and risk limits, which may result in additional requirements. In principle the holder may apply for changes to the licensing basis using risk arguments. For important changes this process would typically involve extensive analysis and consultation with international partners.

PRINCIPAL SAFETY CRITERIA

	NORMAL OPERATION	ACCIDENTS
ASSESSMENT TYPE	**DETERMINISTIC**	**PROBABILISTIC**
PUBLIC		
Average Annual Population Risk	Risk to be controlled to a trivial level by limitation of the ALARA principle.	1 E-8 fatalities per person per year per site (one fatality per one hundred million per year) Nb This is based on an annual population risk of 1 E-7 fatalities/year applied to all facilities, with a factor 10 reduction used to account for the expectation of a maximum of 10 sites in total. Societal risk (f-N) curve (unit slope on log-log scale, normalized to 1 E-8).
Maximum Annual Individual Risk	250 μSv $year^{-1}$ $site^{-1}$ individual dose limit for the average representative of the critical group.	5 E-6 fatalities per year (one fatality per two hundred thousand per year) due to all authorised actions in South Africa.
WORKERS		
Average Annual Risk to Workers due to all authorised actions in South Africa	Risk to be controlled by the application of the ALARA principle. An ALARA target for the annual average individual dose of radiation workers on a site is required which must not exceed 4 mSv.	1 E-5 fatalities per year (one fatality per one hundred thousand per year).
Maximum Annual Individual Risk to Workers	The occupational exposure of any radiation worker on a site shall not exceed the following: - An average effective dose of 20 mSv per year averaged over five consecutive years. - A maximum effective dose of 50 mSv in any single year.	5 E-5 fatalities per year (one fatality per two hundred thousand per year) due to all authorised actions in South Africa.

In the context of the MDEP forum the above mentioned principle radiation and nuclear safety requirements, in conjunction with requirements on the organization and safety related processes and programmes, are essentially the “safety goals” in the nuclear regulatory framework in South Africa. These safety goals are further used in conjunction with a system of safety indicators linked to a compliance assurance and enforcement process.

II.10 Russia

There are no clear definitions of NPP qualitative safety goals in Russian regulatory documents. A basis for regulation and safety assurance is the following definition of the federal norms and rules OPB-88/97 General regulations on ensuring safety of nuclear power plants: "NPP Safety, nuclear and radiation (hereinafter – Safety) is quality of NPP to control radiation impact to the staff, population and the environment by predefined limits in normal operation state and in violations of normal operation including accidents". Mentioned limits are presented in safety regulations approved by Health ministry.

Quantitative goals are formulated as probabilistic goals no matter for operated or new NPP designs.

The normative requirements define that all severe beyond design basis accidents have equally low probability, and the integrated probability of a severe beyond design basis accident (of reaching normative safety limits for the reactor core) should not exceed 1 E-5 per year (p. 4.2.2 of OPB-88/97).

Evacuation is considered as the most radical protective measure for the population in case of a severe radiation accident at NPP. In this connection the primary safety goal is directed toward practical exclusion of the necessity for the evacuation of the population residing beyond the boundaries of the site protective actions planning area, defined by the NPP design, in case of any accident. Quantitative equivalent of the "practical exclusion" is probability less than 1 E-7 per year (p. 1.2.17 of OPB-88/97).

According to p. 1.2.19 of OPB-88/97 an applicant should perform probabilistic safety analysis of the NPP. Features of PSA acceptable for the regulator are described in a set of guidelines and procedures.

II.11 Summary

Many countries subscribe to the view that NPP should only add insignificantly to the risks which the population is exposed. In many cases this is based on 1% or 0.1% of risks of death of individuals or cancer, respectively. These considerations should cover normal operational exposures of workers, radiation and radioactivity discharges to the environment as well as accidents. Although many safety goals are based on the effects on individuals, all countries recognise that the consequences of a nuclear accident can affect wider aspects such as effects on use of land or food production. For this reason, countries all propose that, for new reactors, offsite releases of radioactivity should be reduced to a low level (i.e. the ALARP concept).

In addition, safety goals for damage states are proposed that will provide higher level of safety than previously. According to a survey by NEA (NEA/CSNI/WGRisk (WGRisk Task (2006)-2 - Probabilistic Risk Criteria) relating to new reactors, in general, a core damage frequency target of 1 E-5 per reactor year is being applied by most countries for new LWR-type reactors. Large offsite releases are either "practically eliminated" or must be of a low frequency, typically, 1 E-6 per reactor year (are also being applied by many countries. However, it is important to remember that when deriving values for comparison with these targets, the assumptions and models used may be different in different countries. Hence, when comparing analyses with targets it is essential to ensure that the underlying assumptions are consistent.

III. Safety Goals

III.1 Background

The fundamental safety requirements of most countries are based on deterministic considerations that employ DID safety philosophy. As discussed in Section II, defence-in-depth philosophy is a cornerstone of design/operational safety and the prevention of accidents. It provides for a series of successive barriers between the radioactive source and the harmful effects of radiation on people and the environment. Independence of the successive barriers provides protection against the risk of random failures of separate barriers although several barriers can be endangered in more serious accidents. As a whole, the set of barriers supported by independent reliable safety systems designed to protect their integrity provide a reliable containment of radioactive material within the NPP. INSAG 12 illustrates the concept and how it has been refined and strengthened through years of applications. In principle, all countries utilize the DID safety philosophy in the design and operation of nuclear power plants.

The discussion in Sections I and II also clearly reflects the international view that PSA is a powerful tool to make better decisions on reactor safety. PSA along with a definition of safety targets/goals provides the capability to make more coherent and transparent safety decisions

III.2 Fundamental Requirements

It is recognized that the fundamental basis for protecting the health and safety of the workers and the public as well as the protection of the environment requires that normal exposures and discharges are controlled, accidents are prevented and, should they occur, mitigation measures are provided to protect people and the environment by limiting any radiological releases.

These fundamental requirements need to be developed, in a coherent manner, into safety goals that can be used in regulatory decision making. It is proposed that this can be achieved by setting the safety goals within a hierarchical structure, in which each successive level of safety goals and targets can be clearly related to the level above. One advantage of this approach is that the high level safety goals are typically technology neutral. In this section a hierarchical structure is proposed that can be used to integrate the elements of safety desired to protect health and safety during normal operation and accident conditions for the whole plant lifecycle.

Many of the reference documents quoted in this paper have been implicitly, if not explicitly, focussed on LWR-type reactors. Whilst some countries employ technology neutral regulatory requirements, or are considering such approaches, there is no international agreement on the details. It is also the case, that whilst the high level safety goals may be technology neutral, it will be necessary to develop lower tier goals which are specific to the technology used so that designs and operations can be determined. These specific goals may be significantly different, as may be the methodologies used to demonstrate they are met, but they should still be traceable to the high level safety goals so that a consistent level of safety is achieved regardless of the technology. It is also important that a balanced view on applying the full set of safety goals is achieved, so that all aspects of safety and all people at risk are treated equitably and the design and operations do not put too great a reliance on a few SSC.

III.3 Hierarchy of Safety Goals: Extended DID Approach

To achieve a balanced view on applying the full suite of safety goals and targets they should be considered within a structure that encompasses the basic DiD approach. It is proposed here that the established form of DID structure should be extended to include a wider range of elements, including both deterministic and probabilistic safety goals and targets. Figure 4 illustrates a Hierarchical Structure for Safety Goals, with a top level safety goal and a set of high level safety goals, that can be

used to integrate the elements of safety desired to protect health and safety during normal operation and accident conditions for the whole plant lifecycle. The high level safety goals need to be developed, in a coherent and consistent manner, into lower level safety goals and targets that can be applied within the design and operation of reactors, with a clear connection between the different levels. This structured approach is technology-neutral and is sufficiently flexible that it can be used for developing and applying safety targets to water-cooled and non-water cooled reactor designs.

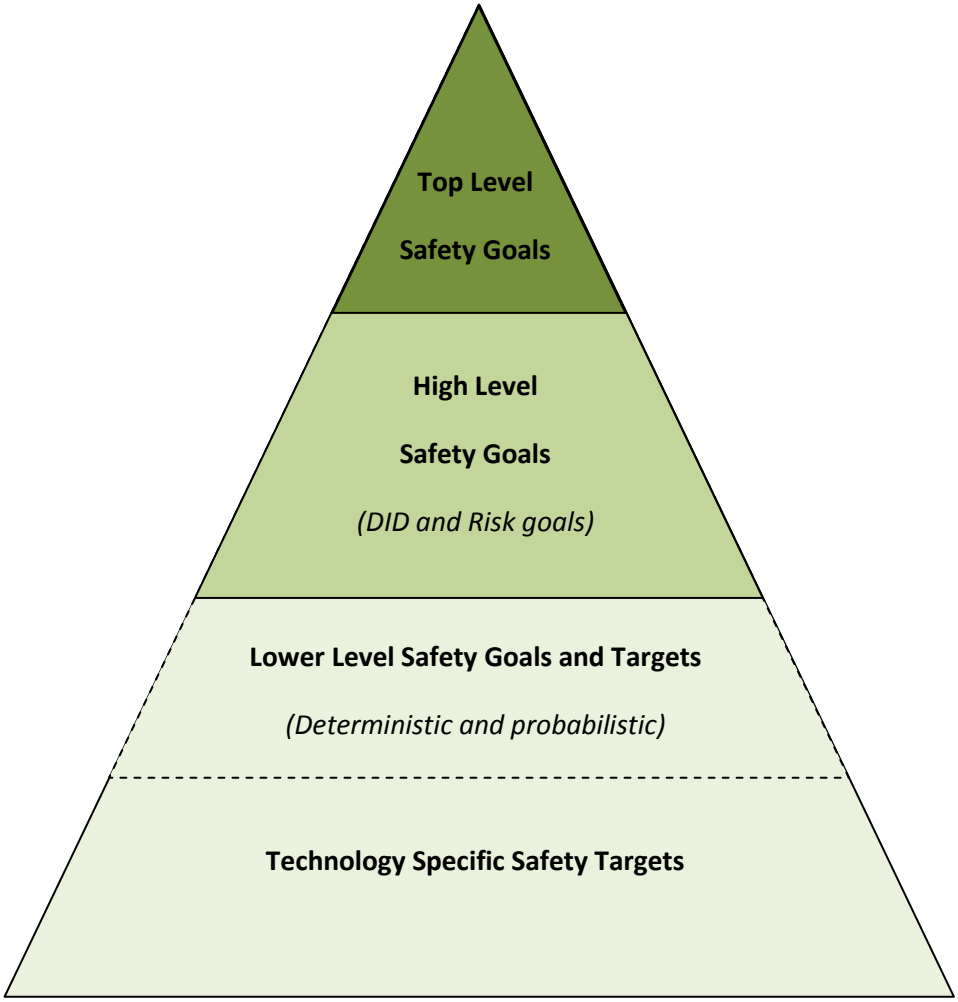

Figure 4: Hierarchical Structure of Safety Goals and Targets

Both qualitative and quantitative safety goals and targets are necessary in developing a technology-neutral approach and the difference between safety goals and targets, as used in this paper, should be understood. Goals are generally qualitative, or define upper limits, and set out what has to be achieved. Targets, which are usually quantitative and developed from the goals, set out the measure of achievement. Safety cases should address the way the goals have been achieved: failure to address all of the goals could result in regulatory enforcement. Failure to meet a target must be justified and may result in regulatory enforcement; failure to do better than a target must be explained.

It is generally agreed that there should be a continual aim of improving safety, building on the current high levels that exist. The following safety goals have been developed to ensure the maintenance of these high levels of safety whilst setting goals that will drive towards the aim of the expectation that higher levels of safety will be achieved in the design and operation of new and future reactors.

The safety goals are stated in the next three sections. In part IV more detail of the goals is given and

the application to developing lower tier goals is described.

III.3.1 Top-level Safety Goal

Provide a level of safety such that the risks to people and environment from the whole lifecycle of a nuclear power plant is only a small fraction of the risks from other hazards to which these are otherwise subjected.

III.3.2 High level DID goals

1. Occupational and public dose during normal operation, should be as low as reasonably achievable and below regulatory limits, consistent with the IAEA Basic Safety Standard, which is derived largely from the ICRP recommendations.

2. Prevention should be the focus by designing for fault tolerance through application of good engineering principles.

3. For all accident sequences taken into account in the design basis, there should be no offsite effects and no significant onsite doses for workers as far as reasonably practicable.

4. Large offsite releases due to accidents, should be as infrequent as reasonably practicable.

5. Any offsite releases that could occur should only require limited offsite emergency response.

III.3.3 Extended DID high level goals

I. Integration of safety and security measures should ensure that neither compromises the other.

II. Siting factors, in addition to being considered within the design should also be taken into account in considering emergency arrangements.

III. Where improving safety is, or over the lifetime of the plant becomes reasonably practicable, then this improvement should be implemented.

IV. Where an exposure occurs, the likelihood should decrease as the potential magnitude increases.

V. Independence of the barriers and systems that form the protection at the different DID levels is a fundamental aspect of the safety concept, which should be ensured and enhanced in new and future reactors, as far as practicable.

VI. Consideration of the management of radioactive waste during the design and operation and decommissioning phases of the reactor lifetime should be such that the generation of waste is minimized.

VII. Arrangements to ensure effective management of safety should be made at all lifecycle phases of a reactor.

VIII. Arrangements to make the future decommissioning easier should be considered during the design stage

IV Application of the Safety Goals Structure

The hierarchical structure incorporates a great many features which are expressed in general terms. It is not the purpose of this paper to define detailed safety goals that should be used for LWR or any other reactor technology, though in the later section examples of how it can be applied to current LWR designs taking account of proposed safety goals and targets from various sources, as well as some suggested results of the application to other technologies. In this section some general indication of how the how level safety goals can be developed towards lower tier goals is given. In essence, there are three stages in this process: a level of goals which are still essentially technology neutral; the technology specific goals; and, thirdly, the balancing and integration of these goals, which is touched on in Part V and is the subject of INSAG 25.

The approach to safety analysis and the methods of analysis employed are closely linked to the application of the safety goal structure and this is reflected also in the approach that is taken in this paper to DID.

IV.1 General Features

The implementation of DID is centred on the use of several barriers (usually physical) to prevent the release of radioactive material or radiation shine. It is fundamental to the DID approach that the barriers are designed to provide a high level of integrity and reliability. This demands that good engineering practices (quality assurance, materials qualification, use of accepted codes and standards, use of validated safety analysis tools, fault-tolerance, good human factors etc.) are applied in the designs and the level of independence between the barriers should be very high; therefore the deterministic engineering and safety concepts of redundancy, diversity, separation and segregation must be applied during development of the design. These should ensure, as far as is reasonably practicable, that failure or damage to one barrier should not result in failure or damage to another. Should a barrier fail or be damaged it is essential that this is revealed to the operators.

By carrying out a design basis analysis, the ability of the design to robustly meet the requirements of DID should be demonstrated. The implementation of this concept should ensure that:

1) the design provides capability to prevent (or at least minimize the likelihood of) accidents and to mitigate accidents should they occur,

2) the important safety functions are not dependent on a single element of design, construction, maintenance or operation,

3) appropriate safety margins are provided to account for uncertainties human performance, and

4) capability to contain radioactive releases.

The implementation of this strategy has led to an excellent safety record of the operating nuclear power plants.

Many probabilistic risk analyses conducted to date have attempted to consider the design basis events and other possible initiating events to holistically understand the capability of the SSCs and humans to prevent accidents and mitigate the consequences. The probabilistic analyses, with consideration of uncertainties, can provide a quantitative understanding of the DID philosophy. These studies have also identified some gaps in requirements for water-cooled designs (that have since been modified) in the achievement of very high level of safety. These analyses, for example, have shown how the protective

measures impact the frequencies and consequences of events.

all the High Level Goals proposed in III.3.2 are technology neutral. So, in essence, as are the DID levels. It is possible, in an approximate way, to relate the High Level DID Safety Goals, numbered 1 through to 5, to the five levels of DID. This is shown in the following table (Table 4) where, for simplicity, the descriptions of the DID levels have been summarised.

DID Level	Proposed High Level Safety
1 – Prevention of Abnormal Operation	1, 2, 5,
2 – Control of Abnormal Operation	3,
3 – Control of Design Basis Accidents	3, 5
4 – Control of Beyond Design Basis Accidents: Prevention and Mitigation	4, 5,
5 – Mitigation of Off-site Releases	4, 5

Table 4: DID Levels and High Level Safety Goals

The relationship is not one-to-one and clearly shows the need to deal not only with each level of DID separately, but also holistically. The Extended DID High Level Safety Goals, numbered I through to VIII, are more over-arching and set down goals that have a wider application. This serves to emphasise the need to treat safety in an integrated manner and that the concept of risk, in its widest sense, provides a basis for decision-making.

To show how these concepts then develop in a particular technology, the following example chooses some requirements from various countries in relation to LWR. The particular goals explained, do not provide a full set, nor are they necessarily appropriate as a set.

IV.2 Developing Lower Level Safety Goals and Targets

Some examples of how the framework can be developed to the lower level safety goals and targets, both qualitative and quantitative, are given in the following paragraphs. Lower level goals and targets for existing technology have been developed for many years and can be seen to fit into the extended DID framework.

IV.2.1 Defence-in-Depth

The implementation of DID is centred on the use of several barriers (usually physical) to prevent the release of radioactive material or radiation shine. It is fundamental to the DID approach that the level of independence between the barriers should be as high as possible; therefore the deterministic engineering and safety concepts of redundancy, diversity, separation and segregation must be applied during development of the design. These should ensure, as far as possible, that failure or damage to one barrier should not result in failure or damage to another. Should a barrier fail or be damaged it is essential that this is revealed to the operators. By carrying out a design basis and severe plant state analysis, the ability of the design to meet the requirements of DID should be demonstrated.

IV.2.2 Normal Operation

Safety in normal operation due to worker (or other persons on site) exposure or discharges to the

public is usually expressed as a dose limit with the requirement to further reduce them using ALARA principle. This approach is based on the IAEA's Basic Safety Standard (op cit) which is itself based on the recommendations of the ICRP. Currently, the dose limits are 20 mSv/yr for workers and 1 mSv/yr for the public, with ALARA applied in both cases to drive doses lower.

IV.2.3 Abnormal Operation

The design and operation should be such that deviations from a safe state are minimised and where they occur are either self correcting or raise alarms, which allow sufficient time for corrective action to be taken. There is a hierarchy of these actions, with passive systems, preferred to automatic ones and then operator actions: engineered systems are generally preferred to administrative systems. An example of this is that in many countries any required action should not require operator input in less than 30 minutes.

IV.2.4 Design Basis Accidents

The response to faults relies on a sound definition of the requirements on SSC and operators. To ensure the design and operations are resilient and robust the safety functions that need to be met need to be determined and the requirements on all equipment and operators defined. Equipment qualification and operator training must be aligned with the safety functional requirement. SSCs should be designed against a suitable standard or code and in many LWRs the ASME codes are used, or codes derived from them. The design basis to which these requirements apply is defined in different ways in different countries: in the UK all fault sequences[25] with an initiation frequency of greater than 1 E-5 per year (except natural hazards where the initiation frequency lower limit is 1 E-4 per year) should be considered, though the analysis can be performed in suitable groups, and success targets are defined dependent on the frequency (see table 1)

IV.2.5 Accident Prevention

There is broad international consensus that prevention of accidents is the first means of protection. The following have been considered in relation to new water-cooled reactor designs safety targets for accidents (assuming a single reactor on a site):

- WENRA propose that the potential for escalation to accident situations for new NPP should be reduced by enhancing the capability to control abnormal events
- An NEA survey (WGRisk Task (2006) - 2 - Probabilistic Risk Criteria) showed, in general, a core damage frequency target of 1 E-5 per reactor year is being applied for new reactors, by most countries which use this metric (cf 1 E-4 per reactor year for most current applications).
- The same NEA survey showed that large offsite releases should be either "practically eliminated" or must be of a very low frequency, typically figures of 1 E-6 to 1 E-7 per reactor year are used for this metric.

[25] A design basis fault sequence should include, as appropppriate: failures consequential upon the initiating fault and failures due a common cause, single failures in accordance with the single failure criterion, worst normally permitted configuration of equipment outages and the most onerous operating state.

IV.2.6 Accident Mitigation

Albeit that the first means of protection is prevention, it is not possible to ensure the elimination of accidents completely, hence, designers should also include features to minimise the potential for large releases. The following have been considered in relation to new water-cooled reactor designs safety targets for accidents (assuming a single reactor on site):

- All countries propose that, for new reactors, offsite radioactive releases should be reduced to a low level (i.e. the ALARA concept).
- Large offsite releases are either "practically eliminated" or must be of a very low frequency, typically, 1 E-6 per reactor year are also being applied by many countries, in many countries "large" is not defined, but in Finland a figure of 100 TBq of Cs-137 is given.
- WENRA have suggested that limited off site emergency response could be defined "no permanent relocation, no need for emergency evacuation outside immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption".
- Ensuring containment integrity for the more likely accident scenarios will provide protection from accidents that could lead to early containment failure and sufficient time to plan and implement any additional accident management measures.
- Quantitative health objectives for risk to members of the public in the US are set at:
    - 2 E-6 per year cancer fatality; and
    - 5 E-7 per year early fatality.
- Risks to society: for example, in the UK a target of 1 E-7 per year for accidents leading to100 or more fatalities (immediate or eventual).
- On the basis of extensive studies conducted as part of Level 3 PRAs, it is clear that adoption of these target goals to:
    a) limit radioactive releases. will ensure that the risk to public health and safety will be a very small fraction of the other risks and,
    b) limit core damage likelihood, will ensure high focus on preventing accidents.

In addition, containment integrity should be assured for 24 hours and the ALARP concept applied to identify additional safety enhancements.

IV.2.7 Multiple Plant Sites

Where more than one unit is built on the same site, consideration should be given to the possible interactions between the plants and whether safety is adequately ensured by using goals for single units.

IV.2.8 Continual Improvement

As noted, it is generally agreed that there should be continual effort to make reasonably practical safety improvements, building on the current high levels. On the basis of extensive Level 3 PSA studies, it is apparent that adoption of the proposed goals and targets for limiting radioactive releases and core damage likelihood will, respectively, promote reducing risks to public health and safety to a very small fraction of other risks and a high focus on preventing accidents. However, improvement should not be limited to the initial design considerations. Where improving safety beyond the goals is, or over the lifetime of the plant becomes, feasible at reasonable cost, this improvement should be implemented.

IV.2.9 Frequency-Consequence Curves

Considerable effort is underway, as part of Gen-IV and other initiatives, to develop significantly different NPP designs than the current water reactor designs. It is important to develop safety goals to allow full up front consideration of the above safety objectives in these developing designs. A frequency-consequence (F-C) curve specifies low doses for high frequency events with larger allowable doses for lower frequency events. Doses should be consistent with international standards and calculated so as to correspond to the maximum dose any member of the public could receive from an individual event. The curve should ensure that various elements of the proposed probabilistic goals will remain internally consistent. This concept is independent of any specific nuclear power plant design technology. This curve can also support the siting and emergency planning policy decisions. This F-C concept can also be applied to establish the level of safety for water cooled designs but there is limited experience with such an application.

IV.3 Technology Neutral Application of the Structure

The claim has been made that the structure proposed is technology-neutral and can be applied to developing lower tier safety goals and targets to other technologies. Some examples of the way that it is envisaged that this can be done are outlined in the next paragraphs. Clearly these examples are only indicative and in no way exhaustive.

- DID Level 1: aspects of prevention of abnormal operation include: (a) requirements on core stability which would be set to ensure to a high degree of confidence that abnormal operation does not occur – they would need to be considered differently if on-load refueling were to be part of the operational philosophy or for reactors with positive temperature or void coefficients [eg in the case of a fast reactor, where the Doppler feedback is important they put requirements on the mixing of the plutonium and uranium oxides and the stoichiometry which can affect species migration in the fuel] (b): limiting discharges to the environment would be driven by doses to the public but would lead to requirements on delay tanks, radwaste minimization and ultimately fuel clad failure rates – all these would be interlinked and depend on the actual technology.
- DID Level 4: situations that develop beyond design basis accidents may result from either failure of the safety systems included in the design base or from more rare initiating faults (or hazards): whilst the latter can be controlled to some extent by siting and so limits applicable to all types of reactor can be determined in relation to seismic for example, or design changes made to accommodate extremes of meteorology, the former lead to different requirements, with issues such as diversity, segregation and separation for systems and components front-line – methods to interrupt the progression from source to people such as the role of an independent containment and pressure suppression systems in some technologies become important, whereas in other technologies they may not eg gas-cooled systems or sodium cooled where fire suppression is key.

The development and application of technology specific safety goals and targets are the responsibility of the designers/operators of the plant and, therefore, is not the subject of this paper. However, any proposed goals and targets adopted in the design process should be clearly derived from higher levels in the hierarchy. The design approach should include a demonstration that it is capable of meeting and complying with all the safety goals and targets in the hierarchy.

V. Integrated Decision-Making

As has been noted, all countries have established occupational and public dose limits during normal operation, which generally conform to the IAEA Basic Safety Standard. In addition, all countries have developed deterministic goals in relation to accidents and many have also developed probabilistic targets (in the form of risk metrics which are expressed as frequencies of fatalities, doses, and core damage or release quantities). In the past, combining these into a single decision-making process has typically not been carried out in a formal, systematic manner.

The more recent development of integrated decision making provides a systematic process taking into account all major considerations affecting safety, to achieve a balanced safety decision. In this context, risk should be considered to cover the whole range of safety concerns from normal operational exposure through to severe accidents. The recent INSAG report,INSAG 25, on Integrated Decision-Making seta out a framework for this process.

The report states in its preamble:

"There is general international agreement, as reflected in various IAEA Safety Standards for nuclear reactor design and operation, that both deterministic and probabilistic analyses provide insights, perspective, comprehension, and balance to reactor safety. Accordingly, the spectrum of applications for integration of these approaches continues to increase. Such applications support design, construction, safety assessment, licensing, operation, and regulatory oversight. Additionally, applications related to physical security are now being considered by member states.

Increasingly there is interest in using a structured framework for optimal decisions, which is based on taking account of deterministic and probabilistic techniques and findings. It is timely, therefore, to establish international good practice on the balance between deterministic approach, Probabilistic Risk Analysis (PRA), and other factors, in an integrated decision making process for ensuring nuclear safety…"

INSAG 25 notes that integrated decision-making applications must satisfy the following objectives:

- Relevant regulations are met;
- Defence-in-depth is maintained;
- Safety margins are maintained;
- Engineering and organizational good practices are taken into account;
- Insights from relevant operating experience, research and advances in methodologies are taken into account;
- An adequate integration of safety and security is established.

To determine if these objectives are met, a wide range of deterministic and probabilistic elements should be included in an integrated decision-making process. INSAG 25 sets out a framework for integrating these elements to ensure a balanced, high level of safety is achieved. The integration of the elements is part of an iterative process, which needs to balance the different safety requirements.

The key elements are considered under the following headings:

- *Standards and Good Practice*

- *Deterministic Considerations*: Safety Criteria, Defence-in-Depth, Safety Margins
- *Probabilistic Considerations*: Probabilistic targets; PSA Quality and Scope
- *Organisational Considerations:* Management Systems, Operational Experience, Training and Procedures
- *Other Considerations*: Radiation Doses, Economic Factors, Research Factors
- *Security Considerations*

Making a decision requires success criteria but INSAG 25 does not attempt to recommend any safety goals or targets. The structure developed in this paper proposes a method to do this, but also does not develop detailed goals. It is important to note that in making a balanced decision it may not be possible for all the quantitative targets to be met as there could be conflicted requirements. In addition, the integrated decision making process must take into account the strengths and limitations of the analysis methodologies and data available. The results of applying these methods of analysis can be compared with quantitative safety goals, but it is recognized that security threats, organizational factors and areas such as software reliability are difficult to quantify and therefore the decisions cannot solely be based on quantitative estimates. Hence, the process of integration cannot be a fixed one, of an algorithmic nature, but must be based on a judgement of the relevant importance of the different safety goals. It is important to remember the mantra: Numbers should always guide rather than decide!

VI. Summary

This paper has reviewed the existing approach to defining safety goals in several countries. The review showed that the fundamental safety requirements are generally based on a deterministic, defence-in-depth safety philosophy. The use of risk based safety goals, in combination with deterministic safety goals, provides a way to develop balanced, technology neutral, expectations for the protection of worker and public health and safety and a means for an independent and integrated assessment of plant safety. The paper proposes a structure for how high level safety goals, which are in general qualitative, can be developed into lower tier goals, qualitative and quantitative safety goals in a consistent and coherent manner, whilst retaining a fundamental technology-neutral approach.

The structure supports clearer communication of expectations in a more transparent manner and allows more coherent decision-making. The proposed high level safety goals emphasize the importance of controlling normal operational risks and preventing accidents as well as insuring that measures will be in place to protect the public in the unlikely case of an emergency. These goals in used in conjunction within an integrated decision making framework above will ensure a high level of safety is achieved.

This is still “a work in progress”: it is clear that more contact with other organisations, doing similar or related work,will be valuable and add synergy and is essential in moving towards the aim of greater global harmonisation.

Annex: WENRA Reference Levels for Existing Reactors

The report describes the WENRA views regarding safety of operating facilities and includes a discussion of 18 areas

- Safety Policy
- Operating Organization
- Management System
- Training and Authorization of NPP Staff
- Design Basis Envelope for Existing Reactors
- Safety Classification of Structures, Systems and Components
- Operational Limits and Conditions
- Ageing Management
- System for Investigation of Events and Operational Experience Feedback
- Maintenance, In-Service Inspection and Functional Testing
- Emergency Operating Procedures and Severe Accident Management Guidelines
- Contents and Updating of Safety Analysis Report
- Probabilistic Safety Analysis
- Periodic Safety Review
- Plant Modifications
- On-site Emergency Preparedness
- Protection against Internal Fires