MDEP Position Paper

PP-STC-01

Related to: STC's subcommittee on Safety Goals activities

MDEP Steering Technical Committee Position Paper on Safety Goals

Multi-National Design Evaluation Programme

Steering Technical Committee

1. **MDEP expects that higher levels of safety will be achieved in the design and operation of new reactors.**
2. **MDEP strongly supports the structure of safety goals and targets, as set out in this paper, for consideration of its members and IAEA and other organisations, in moving towards international harmonisation of regulatory requirements;**
3. **MDEP strongly supports the use of integrated decision-making for design evaluation and operational safety**
4. **MDEP recognises the need to develop the process, through continued interactions with other international organisations, to further harmonise regulatory requirements**.

1) Background

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 and expectations which may not have a mandatory nature. The term "safety goals" is used to cover all health and safety requirements and expectations 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[1] encompassing safety in normal operation through to severe plant states.

Although all regulators have safety goals, these are expressed in many different ways and exercises in comparing them frequently are done at a very low level e.g. specific temperature limits in the reactor core. The differences in the requirements from different regulators are difficult to resolve as the goals are derived using different principles and assumptions and are usually for a specific technology. Therefore MDEP set up a sub-committee to investigate a different approach. This approach was to start with the high level safety goals and try to derive a structure and means of deriving lower level safety goals that can be seen to be clearly related to the higher level ones. The work will greatly assist in the process of harmonisation of regulatory requirements and enhance coherence and consistency between goals for different technologies.

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

2) Fundamental Requirement

It is recognized that the fundamental basis for protecting the health and safety of the workers and the public as well as 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.

Many countries considered in this position paper subscribe to the view that operation of NPP should only add insignificantly to the risks to which the population is exposed and in many cases this is based on 1% or 0.1% of risks of death of individuals or cancer. The safety goals and targets developed to meet these requirements usually cover normal operational exposures of workers, radioactive emissions and discharges to the environment as well as accidents. Although many safety goals and targets are based on the effects on individuals, all countries recognise that the consequences of a nuclear accident can affect wider societal aspects such as effects on use of land or food production.

In the following sections a structure for developing safety goals and targets, which can be applied to different technologies in a consistent and coherent manner, is proposed.

3) Defence-in-Depth

All countries utilize a Defence-In-Depth (DID) concept, which has proved to be a useful concept for considering deterministic safety requirements and the reliability of safety systems. However, some explicit and implicit probabilistic risk considerations were used. These included: dividing the design basis faults into groups according to frequency with different acceptable consequences and the use of engineering safety margins, which had been determined heuristically. Different approaches were used in different countries, with some making greater use of formal risk analyses 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. Increasingly, the techniques of Probabilistic Safety Assessment (PSA) [sometimes referred to as Probabilistic Risk Assessment (PRA)], which explicitly consider the possible faults, accident sequences and their likelihoods and consequences, are used to develop risk metrics and insights.

4) 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. The figure sets out an 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.

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 a generally agreed aim that there should be a continual aim of improving safety, building on the current high levels. The following goals have been developed to ensure that higher levels of safety will be achieved in the design and operation of new and future reactors:

4.1) *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.

Figure: Hierarchical Structure of Safety Goals and Targets

4.2) ***High level DID goals***

1. Occupational and public dose during normal operation, should be as low as reasonably achievable (ALARA[2]) 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[3].

4. The frequency of large offsite releases due to accidents should be as low as reasonably practicable.

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

4.3) ***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.

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

[3] "reasonable practicability" requires a comparison of the sacrifice (time, trouble and money) in implementing a safety measure with the risk averted by its implementation.

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

VIII. Arrangements to make future decommissioning easier should be considered at all stages of the reactor lifecycle including the design stage.

5) 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. It is recommended that this approach is extended to new reactors and other technologies. Further work, building on experience from the existing technologies to develop more detailed lower level goals and targets that can be considered within the MDEP group, would be valuable before involvement with the IAEA Safety Standard development.

5.1) *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.

5.2) *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

5.3) *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.

5.4) *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).
- 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.

5.5) *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.

5.6) *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.

5.7) *Technology Specific Safety Goals and Targets*

The development and application of technology specific safety goals and targets are the responsibility of the designers/operators of the plant and this 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.

6) Integrated Decision-making

All countries have established occupational and public dose limits during normal operation, and these generally conform to the IAEA Basic Safety Standard[4], which is derived largely from the ICRP recommendations. 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 risk-informed 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. A recent report by INSAG on integrated risk-informed decision-making is summarised in the annex.

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

Annex

INSAG-25, "A Framework for Integrated Risk-Informed Decision-Making Process" (about to be published)

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 states that risk-informed 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.

The INSAG report considers a wide range of deterministic and probabilistic elements that should be included in an integrated risk-informed decision-making process. It sets out a methodology 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 can result in the identification of new design/licensing basis events and criteria for deterministic safety classification of structures, systems, and components as a result of risk insights.

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*

The integrated decision making process is based on understanding the strengths and limitations of probabilistic and deterministic analyses. 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. To utilise the integrated process, it is necessary to determine a suitable set of safety goals and targets of the sort proposed in the main text.