
v1.0

Background

In 1991, the General Conference (GC) in its resolution RES/552 requested the Director General to prepare ‘a comprehensive proposal for education and training in both radiation protection and in nuclear safety’ for consideration by the following GC in 1992. In 1992, the proposal was made by the Secretariat and after considering this proposal the General Conference requested the Director General to prepare a report on a possible programme of activities on education and training in radiological protection and nuclear safety in its resolution RES1584.

In response to this request and as a first step, the Secretariat prepared a Standard Syllabus for the Post-graduate Educational Course in Radiation Protection. Subsequently, planning of specialised training courses and workshops in different areas of Standard Syllabus were also made. A similar approach was taken to develop basic professional training in nuclear safety. In January 1997, Programme Performance Assessment System (PPAS) recommended the preparation of a standard syllabus for nuclear safety based on Agency Safely Standard Series Documents and any other internationally accepted practices. A draft Standard Syllabus for Basic Professional Training Course in Nuclear Safety (BPTC) was prepared by a group of consultants in November 1997 and the syllabus was finalised in July 1998 in the second consultants meeting.

The Basic Professional Training Course on Nuclear Safety was offered for the first time at the end of 1999, in English, in Saclay, France, in cooperation with Institut National des Sciences et Techniques Nucleaires/Commissariat a l’Energie Atomique (INSTN/CEA). In 2000, the course was offered in Spanish, in Brazil to Latin American countries and, in English, as a national training course in Romania, with six and four weeks duration, respectively. In 2001, the course was offered at Argonne National Laboratory in the USA for participants from Asian countries. In 2001 and 2002, the course was offered in Saclay, France for participants from Europe. Since then the BPTC has been used all over the world and part of it has been translated into various languages. In particular, it is held on a regular basis in Korea for the Asian region and in Argentina for the Latin American region.

In 2015 the Basic Professional Training Course on Nuclear Safety was updated to the current IAEA nuclear safety standards. The update includes a BPTC text book, BPTC e-book and 2 “train the trainers” packages, one package for a three month course and one package is for a one month course. The “train the trainers” packages include transparencies, questions and case studies to complement the BPTC.

This material was prepared by the IAEA and co-funded by the European Union.

Editorial Note

The update and the review of the BPTC was completed with the collaboration of the ICJT Nuclear Training Centre, Jožef Stefan Institute, Slovenia and IAEA technical experts.
1 INTRODUCTION

Learning objectives
After completing this chapter, the trainee will be able to:
1. Describe the fundamental safety objectives.
2. Define design extension conditions.
3. Describe the integrated risk-informed decision making process.

IAEA Safety Fundamentals, SF-1 [1] states that the fundamental safety objective is to protect people and the environment from the harmful effects of ionizing radiation. In order to achieve this safety objective, a comprehensive safety analysis needs to be performed.

Historically, the guiding principles for design and operation of nuclear power plants (NPPs) were deterministic requirements. The main elements were defence-in-depth provisions, safety margins, compliance with the single failure criterion, and some others. The associated implications were that if deterministic requirements (or criteria) are met for an NPP, the plant is safe enough, and the residual risk of unacceptable radiological releases is sufficiently low. Thus, the deterministic safety assessment approach obviously provided a measure qualitative assurance that the risk of unacceptable radiological releases associated with operation of the nuclear installation is acceptably low. However, the answer to the question “how low is low enough?” is not answered with this approach. The known accidents occurring at NPPs showed that the qualitatively assured ‘low risk’ was not always the case.

Probabilistic Safety Analysis (PSA) technology that started in 1975 with the celebrated WASH-1400 study [2] provided the possibility to obtain new additional safety-related insights and unambiguously quantitatively assess the risk associated with operation of a particular NPP. In contrast to the deterministic approach, the probabilistic approach aims to answer the questions:
- What can go wrong?
- How likely is it?
- What are the consequences?

The main advantage of PSA is that it is capable of quantitatively assessing and representing the risks associated with undesirable consequences from operation of an NPP (e.g., core damage frequency, frequencies of radioactive releases, and frequencies of harmful health effects for the population, and other consequences). PSA allows compliance with quantitative safety goals, if defined, to be measured.

Currently, it is widely recognized that both approaches (i.e. Deterministic Safety Analysis - DSA and PSA) need to be engaged in assessing the safety of NPPs [3]. The IAEA Safety Standards also highlight the need for integrated assessment in decision making. The
IAEA General Safety Requirement GSR Part 4, on Safety Assessment for Facilities and Activities [4], states in para. 5.8:

“The results of the safety assessment have to be used to make decisions in an integrated, risk informed approach, by means of which the results and insights from the deterministic and probabilistic assessments and any other requirements are combined in making decisions on safety matters in relation to the facility or activity.”

Increasingly, during recent years PSA has been broadly applied to support numerous applications that have been traditionally based on deterministic requirements/rules; these are risk-informed changes to technical specifications, risk-based plant configuration control, maintenance programme optimization, etc. [5].

Comprehensive deterministic safety assessments and probabilistic safety assessments are carried out throughout the design process for a nuclear power plant to ensure that all safety requirements for the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets the requirements for manufacture and for construction, and as built, as operated and as modified. The question how far is far enough in expanding or going beyond the design basis has been tackled by the introduction of the concept of design extension conditions. A set of design extension conditions is derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions can be used to identify the additional accident scenarios to be addressed in the design, and to plan practicable provisions for the prevention of such accidents, or mitigation of their consequences if they do occur.

Deterministic and probabilistic analyses yield outputs that are complementary to each other. There is thus a need to use a structured framework for consideration of deterministic and probabilistic techniques and findings. In this process, it is appropriate to encourage a balance between deterministic approaches, probabilistic analyses and other factors in order to achieve an integrated decision making process that serves in an optimal fashion to ensure nuclear reactor safety. This framework is termed ‘integrated risk-informed decision making’ (IRIDM). IRIDM depends on the integration of a wide variety of information, insights and perspectives, as well as the commitment of designers, operators and regulatory authorities to use risk information in their decisions.

PSA and probabilistic safety targets provide a measure of risk to support decisions on nuclear safety matters. Targets may be set for the
probability of core damage and for early releases. Apart from deterministic and probabilistic insights, other aspects such as good engineering practices, consideration of operating experience and sound management arrangements, etc. have to be taken into account in the integrated risk informed decision making process.

In applying the IRIDM process, there is also a need for good documentation, communication and follow-up on the implementation of the decisions, including performance monitoring and corrective actions. The IRIDM process also brings transparency to complex decisions involving several key factors.

However, in any application of deterministic and probabilistic safety assessments their strengths and weaknesses need to be clearly identified. Therefore Chapter 2 addresses this issue, followed by Chapter 3 which discusses the approaches to the regulatory requirements for combining DSA and PSA, which also addresses probabilistic safety targets.
2 ADVANTAGES AND LIMITATIONS OF DSA AND PSA

Learning objectives
After completing this chapter, the trainee will be able to:
1. List the advantages and limitations of DSA.
2. List the advantages and limitations of PSA.

As pointed out in the introduction, before addressing the IRIDM process in detail, it is important to define the strengths and limitations of DSA and PSA.

2.1 Advantages of using DSA

Nuclear safety is based traditionally on rules applied to design, operation and safety analysis. These rules are translated into the high level safety requirements of Defence in Depth, Safety Margins, Multiple Barriers, etc. These high level requirements specify lower level requirements:

- For design: redundancy (single failure criterion), diversity, fail-safe actuation, spatial separation, equipment qualification, limits on plant operators (30 minute rule), etc.
- For operation: technical specifications, operating procedures, maintenance, surveillance and inspection requirements, etc.

The deterministic approach is based on postulated accident scenarios. The design is such that the plant is capable of coping with a set of postulated initiating events. Conservative assumptions and safety margins are used to compensate for uncertainties if they have not been calculated. Sustained improvement in safety and safety performance is pursued by following upgrading plans after operational events (incidents) and accidents. Sometimes, new deterministic requirements emerge as a feedback from the operational events.

Deterministic safety assessment, practiced over a long period since the beginning of the nuclear energy industry, has accumulated a vast amount of experience in its application and is well understood by all parties involved in the design, operation, and regulation of NPPs.

2.2 Limitations of DSA

DSA implicitly includes some judgements (sometimes arbitrary) on probabilities (e.g. exclusion of accidents from the design basis, classification of systems, structures and components (SSCs), etc.); this may lead to possible inconsistencies in requirements and decisions, unbalancing safety measures and introducing an excessive burden.
DSA analysis might not be able to account for all the dependencies existing at such a complex facility as an NPP, including those that are either due to interconnections in support systems, or caused by an initiating event, an internal and external hazard or human action.

Application of solely deterministic concepts to the design provisions may not lead to a balanced design, or to overprovision in same areas. Where improvements are proposed, it may not be possible to determine which options give greater risk reduction. In addition, DSA has difficulties in considering a broader set of safety threats, ranking them, and identifying and assessing uncertainties.

### 2.3 Advantages of using PSA

Deterministic analyses cover a subset of initiating faults and fault sequences, chosen as representative of more extreme events in the expectation that they will provide information relevant to safety requirements, including the less extreme faults and sequences. PSA evaluates a much wider set of accidents and thus gives a better balanced assessment of the installation and can complement the deterministic approach. The output of a PSA is usually given as the frequency or probability of a particular consequence. However, the value of PSA does not lie only in the numerical estimation of risk. As it is a structured approach to the way faults may develop, it can provide valuable information on the balance of risks, point out areas of weakness where improvements can be sought, and confirm the adequacy of defence in depth provisions. This means that it may be possible to reduce unnecessary conservatisms in areas less relevant to risk and provide additional requirements in areas not covered by the deterministic analyses.

One of the major advantages of PSA is that it allows holistic consideration of different types of dependencies including common mode failures.

 Whilst it is apparent that PSA results can contribute to maintaining and improving designs insights from PSA can be used in a wide range of regulatory and safety decisions. The use of risk information, drawing on all sources of relevant information, can contribute to a more balanced approach. This in turn leads to proportionate consideration of situations according to their significance to safety. It further assists in targeting effort on important areas of weakness and leads to a more consistent decision making process. Besides being a more thorough method of decision making, the more explicit consideration of risk also makes the process more transparent and auditable. The use of PSA insights also allows a more robust decision making process by assisting in identifying and perhaps quantifying sources of uncertainty, and by providing a framework for considering the effect of uncertainties on key assumptions by testing the sensitivity
of the results.

### 2.4 Limitations of PSA

Not all factors can be estimated quantitatively, and even a good PSA has limitations. Such issues as completeness of fault identification and fault sequence development, availability of data, particularly plant-specific data, uncertainties in phenomenological modelling, data, and quantification of human factors contribute to these limitations. The structured approach often allows greater clarity of where these limitations exist, which may be disguised in other approaches, but they mean that a careful consideration when using PSA results is needed depending on the application.

PSA outputs are an estimate of the risks and the numerical values obtained carry uncertainty as they are dependent on the assumptions and data employed. They are theoretical constructs which should be seen as a measure of the risks, not as values of some intrinsic properties of the installation. Thus a re-estimation using different assumptions may give different values, but this should not be taken as meaning that the actual risk has changed. In particular, increased knowledge may allow conservatisms to be reduced, which may mean the calculated risks decrease, whereas in practice there has been no change, but the increased knowledge of the installation and its behaviour would suggest that in fact safety has been improved.
3 REGULATORY REQUIREMENTS FOR COMBINING DSA AND PSA

Learning objectives

After completing this chapter, the trainee will be able to:
1. Define high level safety goals and health objectives.
2. Recognize the terms core damage frequency, large early release frequency and conditional containment failure probability.
3. Describe the concept of the frequency-consequence curve.
4. Define safety goals for existing and new reactors.

As already mentioned in the Introduction, an important input to the IRIDM process in some member states can be probabilistic safety targets, goals or criteria.

A possible framework for the definition of such criteria was given by INSAG [6]. This defines a “threshold of tolerability” above which the level of risk would be intolerable and a “design target” below which the risk would be broadly acceptable. Between these two levels, there is a region where the risk would only be acceptable if all reasonably achievable measures have been taken to reduce it.

3.1 High level goals or health objectives

In some countries, high level goals or health objectives are specified by the regulatory body in terms of limits for the individual risk of prompt fatality and the risk of cancer from nuclear accidents.

Examples are US NRC Health Objectives which specify as follows: “The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed 0.1 percent of the sum of prompt fatality risks resulting from other accidents to which members of the US population are generally exposed (approximately 5 x 10^{-7}/year). The risk to the population in the area of a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed 0.1 percent of the sum of cancer fatality risks resulting from all other causes (approximately 2 x 10^{-6}/year).”

However, because of the complexity of verifying these goals, subsidiary risk objectives were introduced. For example, surrogate risk objectives were defined in terms of limits for:
- Core Damage Frequency (CDF);
- Large Early Release Frequency (LERF);
- Conditional Containment Failure Probability (CCFP).

The above limits refer only to a single parameter; however, in some
countries reactors are designed to comply with a dose/frequency curve as shown in Figure 3.1. The curve illustrates that the more likely is an event to happen, the more stringent are requirements for the acceptable dose.

In addition to requiring the design to comply with a dose/frequency ‘curve’ such as Figure 3.1, some regulatory bodies require the societal risk to be controlled by specifying a frequency limit for the release of a specified amount of $^{137}$Cs or the equivalent. In addition, some countries specify a frequency limit for applying countermeasures such as banning local food and evacuating members of the public.

![Figure 3.1: Frequency-Consequence (F-C) curve compatible with ANSI-18.2.](image)

3.2 Safety goals

The term ‘safety goal’ is often perceived as a quantitative value characterising the level of risk that is viewed as a goal to be achieved by NPP designers and operators in their efforts to minimize the radiation risk to the population.

The approaches to establishing and using safety goals are different in various member states.

The safety goals for NPPs are stated in the IAEA publication INSAG-12 [6]. These are formulated as follows:

- The target for existing nuclear power plants … is a frequency of occurrence of severe core damage that is below about $10^{-4}$ events per plant operating year. Severe accident management
and mitigation measures should *reduce by a factor of at least ten the probability of large off-site releases* requiring a short term off-site response. Application of all safety principles and the objectives … to future plants could lead to the achievement of an improved goal of not more than $10^{-5}$ severe core damage events per plant operating year. Another objective for these future plants is the *practical elimination of accident sequences that could lead to large early radioactive releases*, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and in time.

Health effects to members of the public: INSAG has given no guidance on the targets for health effects to members of the public.

- In some countries the target for the risk of death of a member of the public is taken to be $10^{-6}$ per reactor-year.

Non-compliance with the safety goals does not mean that the operating plant will necessarily need to be shut down; in fact there is variety in regulatory practices in this respect. However, a common perception currently is that operating plants should pursue plant modifications aimed at achieving the respective safety goal.
4 INTEGRATED RISK-INFORMED DECISION MAKING

Learning objectives

After completing this chapter, the trainee will be able to:
1. Define the basic elements of the IRIDM process.
2. Identify all elements that need to be taken into account when performing the IRIDM process.
3. Explain the advantages of performing the IRIDM process.

When making a decision on any issue dealing with NPP safety, DSA and PSA results are not the only determinants in the decision making process. It is widely recognized that other important considerations have to be addressed. The process of decision making that takes into account many aspects in a robust and unambiguous way is called Integrated Risk-Informed Decision Making (IRIDM) [7, 8]. Along with PSA and DSA considerations, other factors influencing the decision include:

- Organizational factors (management systems and operational experience);
- Security considerations;
- Existing standards and good practice;
- Other considerations including personnel radiation doses, economic factors, research results.

Weighting coefficients are assigned for each factor to assist in this decision making process. A multi-disciplinary team of experts needs to be formed to be able to arrive at a sound and optimum decision.

The IRIDM process is a systematic approach aimed at integrating major considerations influencing nuclear power plant safety. Its goal is to optimize the safety decisions without unduly limiting nuclear power plant operation. The output from IRIDM should satisfy the following basic safety principles [8]:

- 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 development, and state of the art methodologies are taken into account;
- Adequate integration of safety and security is ensured;
- Relevant regulations are met.

The general IRIDM process is depicted in Figure 4.1 and described in more detail below.
Figure 4.1: Integrated Risk-Informed Decision Making Process.

The process starts by clearly defining the issue to be considered. Once defined, all relevant regulatory and utility considerations have to be evaluated. The inputs to the decision then need to be established. These include standards and good practices, operating experience, deterministic and probabilistic considerations, organizational considerations, security considerations and any other considerations like radiation doses, economic factors etc.

It should be noted that the importance of each of the above elements depends on the issue to be considered and can change as the selected issue changes. Once the evaluation has been completed, the decision can be taken and implemented. However, this is not the end of the process. After implementation, the performance should be monitored and corrective actions taken if necessary to ensure that the decision has achieved the desired outcome.
Looking at the process depicted in Fig. 4.1, it is evident that none of the elements involved in the process is new. It is their integrated consideration that might not be practiced by the nuclear power plant management. Below we briefly describe each of these elements, even though they are all described in much greater detail elsewhere in the training course material.

Standards and good practices
The standards to be taken into account include standards developed by international organizations, national regulatory bodies, engineering organizations, international standards groups, vendor owner groups and many others.

Good practices include practices from personal or specific operating experience, from the experience of other utilities, and from the nuclear industry in general.

Operating experience
The feedback of operating experience is one of the major factors for improving the design and operation of nuclear power plants. It includes learning from events that happened at the plant itself, at similar plants or other industrial facilities. For an effective feedback of operating experience it is essential to determine root causes correctly, as only then can effective corrective actions be established and adequate lessons learned [9].

Deterministic considerations
Deterministic safety assessments address the requirements that serve to reduce the potential hazards identified, to ensure that the design is fault-tolerant to adequately meet the defence in depth philosophy, to assure compliance with deterministic acceptance criteria [10], and to maintain adequate safety margins [11, 12]. Much more detail can be found in Module VI.

Other deterministic considerations that might be considered in the IRIDM process include, among others, requirements for equipment qualification, physical and material analyses, prevention of common cause failures, fail-safe design provisions, redundancy and diversity for safety functions and systems, and physical separation of redundant systems.

Probabilistic considerations
A major contribution to probabilistic analyses in complementing deterministic safety analysis is the identification of failure sequences that otherwise might be overlooked. This is a structured approach that includes Level 1 [13], which calculates the conditional core damage frequency, Level 2 [14], which deals with the containment performance, and Level 3, which calculates the potential doses to the population. It provides both qualitative and quantitative outputs [15]. Qualitative outputs will show up weaknesses in the design or
operation, whereas quantitative results allow for comparison with the
established safety targets. As with all other methodologies, it is
important to assure high quality in the analyses performed [16], if
results are to be used in the decision making process. Much more
detail on PSAs can be found in Module VII.

Figure 4.2: Integration of deterministic and probabilistic elements.

Figure 4.2, taken from [8], depicts the integration of deterministic and
probabilistic elements in the IRIDM process. It is an iterative process,
repeated before arriving at a final safety decision.
**Organizational considerations**

Safety management covers a variety of aspects including leadership, control, competence, communication and cooperation between staff [17]. Management should ensure that among other matters maintenance, inspection, testing, training and managerial supervision are properly conducted within the nuclear power plant. Again, more details on this subject can be found in Module XXI.

**Security considerations**

Security at the nuclear power plant site needs to be included in the IRIDM as it might have a positive or negative impact on nuclear safety. In some cases, security measures support safety, as for example when enhanced protection against malicious acts would also protect the installation from environmental hazards. In other situations security measures may hinder or delay the necessary safety actions that should be taken promptly in response to an abnormal situation. Such considerations should be taken into account in the design and when developing operating and security procedures [18]. More on this topic can be found in Module III.

**Other considerations**

Other considerations that should be taken into account during the IRIDM process include:

- The effect of operational or design changes on the normal operational doses;
- Doses during maintenance or modifications;
- Requirements to minimize radioactive waste and discharges to the environment;
- And last but not least, the economic effects.

**Performance monitoring and feedback**

Performance monitoring is an essential element of the IRIDM process. The consequences of decisions need to be monitored and feedback provided on their effectiveness. If not satisfied with the results, corrective actions should be put in place and the entire process repeated until satisfactory results are obtained. The feedback needs to be properly documented and communicated to all involved. A periodic reassessment such as a Periodic Safety Review (PSR) [19] can be useful in confirming that the IRIDM process is successful in the long run.
5 QUESTIONS

1. Historically, which type of safety analysis was used for the design of NPPs?
2. Which questions does PSA aim to answer?
3. Define design extension conditions.
4. Name some advantages of DSA.
5. Name some limitations of DSA.
6. Name some advantages of PSA.
7. Name some limitations of PSA.
8. Describe the basic principle of the dose/frequency curve (no need to provide numbers).
9. What are the safety goals for CDF and LERF for existing and for new nuclear power plants?
10. Describe the basic principles of IRIDM.
11. Which elements need to be considered when performing the IRIDM process?
12. What are the advantages of using the IRIDM process?
6 REFERENCES


[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety


The views expressed in this document do not necessarily reflect the views of the European Commission.