IAEA-TECDOC-1436

# *Risk informed regulation of nuclear facilities: Overview of the current status*

IAEA
International Atomic Energy Agency

February 2005

# IAEA SAFETY RELATED PUBLICATIONS

## IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (i.e. all these areas of safety). The publication categories in the series are **Safety Fundamentals, Safety Requirements** and **Safety Guides**.

Safety standards are coded according to their coverage: nuclear safety (NS), radiation safety (RS), transport safety (TS), waste safety (WS) and general safety (GS).

Information on the IAEA's safety standards programme is available at the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at P.O. Box 100, A-1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by e-mail to Official.Mail@iaea.org.

## OTHER SAFETY RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other publications series, in particular the **Safety Reports Series**. Safety Reports provide practical examples and detailed methods that can be used in support of the safety standards. Other IAEA series of safety related publications are the **Provision for the Application of Safety Standards Series**, the **Radiological Assessment Reports Series** and the International Nuclear Safety Group's **INSAG Series**. The IAEA also issues reports on radiological accidents and other special publications.

Safety related publications are also issued in the **Technical Reports Series**, the **IAEA-TECDOC Series**, the **Training Course Series** and the **IAEA Services Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. Security related publications are issued in the **IAEA Nuclear Security Series**.

IAEA-TECDOC-1436

# *Risk informed regulation of nuclear facilities: Overview of the current status*

IAEA
International Atomic Energy Agency

February 2005

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

RISK INFORMED REGULATION OF NUCLEAR FACILITIES:
OVERVIEW OF THE CURRENT STATUS
IAEA, VIENNA, 2005
IAEA-TECDOC-1436
ISBN 92–0–100105–3
ISSN 1011–4289



Printed by the IAEA in Austria
February 2005

## FOREWORD

Probabilistic Safety Assessment (PSA) has reached the point where it can, if performed to acceptable standards, strongly influence the design and operation of nuclear power plants. The methodologies in use have matured and there is a clear consensus that results from PSAs should be considered as a complement to the traditional deterministic safety analysis. In addition, the reconciliation of probabilistic and deterministic insights is a fundamental tool for optimizing safety decision making processes applied both by utilities and regulatory bodies.

Many regulatory bodies are currently revising their regulations according to the risk informed regulation concept, where risk insights are considered together with other factors to establish requirements that focus licensee and regulatory attention on design and operational issues in a way that is commensurate with their importance to public health and safety. It is believed that the use of risk insights can result in both improved safety and reduction of unnecessary regulatory burdens.

To use risk insights in the decision making processes in an adequate manner, it is very important to establish a systematic approach that integrates in a sound, transparent and justifiable manner all the elements needed. The real difficulties arise when trying to identify all the relevant safety contributors (inputs) and especially to assign the relative weight of each of them to decision making. Particular difficulties are experienced when determining the necessary quality of PSA analyses and treating inputs having large uncertainties. Many states are reluctant to consider probabilistic safety assessment reasoning and there is no international consensus on the probabilistic safety criteria to be used in judging the acceptability or not of particular safety decisions.

With this background in mind, the IAEA, in cooperation with the US Nuclear Regulatory Commission, held in Washington DC in 2001 a Technical Committee Meeting on Risk Informed Decision Making to analyse the international experience in this area and discuss the new ‘risk informed’ regulation concept, which has been for some years under consideration in a number of States. This publication addresses the main elements of the risk informed, decision making process and provides guidance on how to implement the risk informed regulation concept. The advantages and potential safety benefits that can be gained from the implementation of ‘risk informed’ regulation are underlined, as well as possible problem areas and expected difficulties. The information provided could be of equal interest to utilities and regulatory bodies in IAEA Member States.

The IAEA acknowledges the work of the participating experts and wishes to thank them for their valuable contribution to this publication. The IAEA officer responsible for the preparation of this publication was V. Ranguelova of the Division of Nuclear Installation Safety.

## *EDITORIAL NOTE*

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

*The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.*

**CONTENTS**


1. INTRODUCTION ..... 1

1.1. Background ..... 1
1.2. Scope of the report ..... 2
1.3. Structure of the report ..... 2

2. USE OF RISK IN REGULATORY DECISION MAKING ..... 3

2.1. Deterministic approach ..... 3
2.2. Probabilistic approach ..... 7
2.3. Benefits of an integrated approach ..... 13

3. INTEGRATED DECISION MAKING APPROACH ..... 15

3.1. Introduction ..... 15
3.2. Application of an integrated decision making process ..... 18
3.3. Requirements of the regulatory body ..... 25

4. INTEGRATED DECISION MAKING for PLANT SAFETY ISSUES ..... 25

4.1. Overview ..... 25
4.2. Description of the integrated decision making process as applied to plant safety issues ..... 26
4.3. Examples of decisions made using an integrated decision making process ..... 32
4.3.1. Increasing the seismic resistance capability ..... 32
4.3.2. Adding diversified safety systems ..... 33
4.3.3. Increasing the reactor power level ..... 34
4.3.4. Extending test intervals ..... 35
4.3.5. Removing one of the inputs to the reactor trip system ..... 36
4.3.6. Increasing the length of working shifts ..... 36

5. 'RISK INFORMING' REGULATORY ACTIVITIES ..... 37

5.1. Overview ..... 37
5.2. Using risk information to prioritize tasks within a regulatory activity ..... 38
5.3. 'Risk informing' the regulations ..... 39
5.3.1. Benefits of 'risk informing' ..... 39
5.3.2. General considerations ..... 40
5.3.3. Steps in 'risk informing' a set of regulations ..... 42
5.3.4. Steps for 'risk informing' an individual regulation ..... 45
5.4. 'Risk informing' other regulatory activities ..... 49
5.4.1. Issuing, amending, suspending or revoking authorizations ..... 49
5.4.2. Carrying out regulatory inspections ..... 49
5.4.3. Corrective and enforcement actions ..... 50

APPENDIX: NRC PROCESS FOR RISK INFORMING THE REGULATION FOR COMBUSTIBLE GAS CONTROL (10 CFR Part 50.44) ..... 53

REFERENCES ..... 63

CONTRIBUTORS TO DRAFTING AND REVIEW ..... 67

# 1. INTRODUCTION

## 1.1. Background

National legislation usually provides for a regulatory body to be established that is charged with the responsibility for effective control of nuclear, radiation, radioactive waste and transport safety within a country. To fulfil its statutory obligations the regulatory bodies carry out a number of activities, amongst which the following are included:

- reviewing and assessing submissions on safety and making decisions on safety issues that arise at nuclear facilities
- establishing, promoting or adopting texts of a regulatory nature such as regulations, guides, safety standards and guidance
- carrying out site inspections
- issuing, amending, suspending or revoking authorizations
- carrying out enforcement activities
- reacting to incidents that occur at nuclear sites
- carrying out research and comparable activities.

The traditional approach to regulation has been based on a deterministic approach where a set of rules and requirements has been defined that is aimed at ensuring a high level of safety.

However, over the past ten years, a Probabilistic Safety Analysis (PSA)[1] has been produced for the majority of the nuclear facilities in the Member States (as well as nuclear power plants, this also includes nuclear facilities such as fuel production and reprocessing plants, research reactors and isotope production facilities). In general, these PSAs are of a sufficiently high quality to be used routinely by both plant operators and regulatory bodies as one of the inputs into the decision making process relating to nuclear safety and regulatory issues. The probabilistic approach is being used more and more to complement the deterministic approach and to provide additional insights that would not otherwise be available.

The modern approach is to apply an integrated decision making process that combines the insights from the deterministic approach and the probabilistic analysis with other requirements (legal, regulatory, cost-benefit, etc.) in making the decision. This approach is increasingly being applied by regulatory bodies in making decisions about safety issues at nuclear facilities, and in organizing their activities so that their resources are used more efficiently and there is a reduction in the unnecessary burden on the licensees without compromising safety.

---

[1] For the purposes of this report, the terms Probabilistic Safety Analysis/Assessment (PSA) and Probabilistic Risk Analysis/Assessment (PRA) are taken to be synonymous: the term PSA is used throughout.

It should be noted that for many years, risk considerations have been used, implicitly or explicitly, in making safety decisions and determining regulatory requirements. However, the increased maturity of PSA gives a more rigorous way of providing much of the detailed risk information for use in the safety decision-making and regulatory processes. Adopting the integrated decision making process provides an efficient way of ensuring that safety decisions are taken on a sound basis.

### 1.2. Scope of the report

The report provides guidance on the use of risk information by a regulatory body as part of an integrated decision making process. This addresses the way in which risk information is being used as part of an integrated process in making decisions about safety issues at nuclear plants — sometimes referred to **risk informed decision making**, and how risk information is being used by a regulatory body as an input into the activities that it carries out — sometimes referred to as **risk informed regulation**.

The risk informed approach aims to integrate in a systematic manner quantitative and qualitative, deterministic and probabilistic safety considerations to obtain a balanced decision. In particular, there is explicit consideration of both the likelihood of events and their potential consequences together with such factors as good engineering practice and sound managerial arrangements. The basic components of risk, likelihood and consequence, are based on sound knowledge or data from experience, or derived from a formal, structured analysis such as a PSA.

This integrated approach can be applied to all types of activities and facilities including non-reactor nuclear situations. However, the examples given in this publication relate mainly to power reactors because these constitute the majority of nuclear facilities and the approach has been developed furthest in the context of these plants.

This publication describes the general concept of the use of risk information by a regulatory body and how this can be applied to making decisions on plant safety issues or regulatory activities. By following an integrated approach, this will lead to an improved decision making process that can improve safety and lead to a more efficient and cost effective use of resources. It also indicates some of the practical issues and problems that need to be addressed in adopting a risk informed approach.

It is recognized that the way in which nuclear safety regulation has developed is different in the Member States. Some of them have developed a highly prescriptive approach based on deterministic requirements that have been set by the regulatory body. Others have adopted a more goal setting, performance based approach where the plant operator and the regulatory body have much more freedom to determine the approach that can be taken to meet the goals. The application of the integrated approach to decision making in all these regulatory environments is also discussed in the report.

### 1.3. Structure of the report

Section 2 gives an overview of the way in which risk has been used in the regulatory process. This describes the traditional deterministic approach and how it has been supplemented by probabilistic analysis. The advantages and shortcomings of each of the two approaches are discussed, and how this has led to the current integrated approach. Section 3 describes the integrated approach, which is a systematic approach that combines the insights from the deterministic and the probabilistic approaches along with any other requirements in

reaching a decision. This section also gives an outline procedure for applying the integrated approach. Section 4 describes how the integrated approach can be applied by a regulatory body to making decisions about safety issues for a nuclear power plant and gives some examples that illustrate how this has been done. Section 5 describes how the integrated approach can be applied by a regulatory body to making decisions about what activities it needs to carry out. This addresses 'risk informing'[2] regulations and the prioritization of regulatory activities. The Appendix gives an example of the process that was carried out by the United States Nuclear Regulatory Commission (NRC) to 'risk inform' the regulations dealing with the standards for the combustible gas control system in light water reactors.

## 2. USE OF RISK IN REGULATORY DECISION MAKING

In the past, the regulatory bodies in most Member States have used a deterministic approach as the basis for making decisions on safety issues and organizing the activities that they carry out. This was done by applying high level criteria such as the need to provide defence in depth and adequate safety margins. These were developed into lower level requirements, which were aimed at ensuring that the risk to workers and members of the public was adequately controlled. The need to meet these deterministic requirements is the basis for most of the regulations, safety standards, guidance, etc. that are currently being used by regulatory bodies.

However, in recent years, PSAs have been developed for most of the nuclear facilities in the Member States and the information provided by these PSAs is increasingly being used to complement the deterministic approach. The move has been towards an integrated approach that combines the insights provided by the deterministic approach and those from the probabilistic approach with any other requirements in making decisions on a safety issue for a nuclear facility or in deciding on the priorities for the activities to be carried out by the regulatory body.

Sections 2.1 and 2.2 describe the main elements of the deterministic and probabilistic approaches respectively and, in each case, the advantages, disadvantages and shortcomings of the two approaches are identified. Section 2.3 gives a comparison of the two approaches and indicates the benefits of moving towards an integrated approach that combines the insights from the two approaches with any other applicable requirements in reaching a decision.

### 2.1. Deterministic approach

*Deterministic requirements*

The aim of the deterministic approach is to define and apply a set of conservative rules and requirements for the design and operation of a nuclear facility. If these rules and requirements are met, they are expected to provide a high degree of confidence that the level of risk to workers and members of the public from operation of the nuclear facility will be acceptably low. This conservative approach has provided a way of taking into account uncertainties in the performance of equipment and humans.

---

[2] For the purposes of this book, the term 'risk informing' is used to describe the move from a traditional, deterministic approach vis a vis nuclear safety regulation and decision making to one that also takes into account the risk information, that is derived from a probabilistic safety assessment, in a systematic way.

The high level deterministic principles relate to the provision of defence in depth and large safety margins and the lower level principles relate to the single failure requirement, preventing common cause failure, providing equipment qualification, limiting the claims made on the plant operating staff, etc. These requirements are described below:

**Providing for defence in depth**: the aim is to prevent deviations from normal operation from occurring and, if prevention fails, to detect and limit their consequences, and to prevent any evolution to more serious conditions. IAEA have defined five levels of defence in depth as follows — see Ref. [1]:

- **Level 1**: the aim is to prevent the occurrence of abnormal operation and failures. This is done by producing a conservative design and ensuring a high quality of construction and operation.

- **Level 2**: the aim is to control abnormal operation and detect failures if they should occur. This is done by incorporating control and surveillance systems.

- **Level 3**: the aim is to control accidents within the design basis if they should occur. This is done by incorporating engineered safety features and developing emergency operating procedures.

- **Level 4**: the aim is to control severe plant conditions if they should occur which requires the prevention of accident progression and the mitigation of the consequences of beyond design basis accidents. This is done by incorporating severe accident management measures.

- **Level 5**: the aim is to mitigate the radiological consequences of significant releases of radioactive material from the plant. This is done by developing off-site emergency response measures.

The application of the defence in depth approach to the design and operation of nuclear power plants has ensured that there are multiple means of carrying out safety functions and multiple barriers in place to prevent the release of radioactive material from the plant. The aim is to ensure that there is a reasonable balance between the prevention of core damage, the prevention of containment failure and the mitigation of off-site consequences.

**Ensuring adequate safety margins**: the aim is to design the plant and the safety systems in such a way as to provide a large margin between how the plant would behave in fault conditions and failure of any of the barriers to the release of radioactive material. These margins ought to be sufficient to take account of any uncertainties in the analysis methods and data [2]. For example, for transients and LOCAs, the operation of emergency core cooling systems needs to ensure that there is a large margin between the conditions that would be reached in the core and those that would lead to overheating of the fuel elements so that there is a high degree of confidence that fuel failures would not occur. Similarly, the operation of the containment systems needs to ensure that there is a large margin between the temperature and pressure conditions reached in the containment and those that would lead to failure so that there is a high degree of confidence that damage of the containment cannot occur.

**Applying the single failure requirement**: for safety systems provided to ensure any safety functions, the requirement is that they be designed in such a way that no single failure prevents them from carrying out their safety function. Therefore, the safety systems usually

have more than one train of equipment that is capable of carrying out the safety function. The single failure requirement is normally applied to the active components that are required to operate in order to perform the safety function. In some cases it may also be applied to passive components. The analysis that is carried out for design basis accidents assumes that the worst single failure occurs following the initiating event [3].

**Preventing common cause failure**: the reliability of the safety systems that have a number of similar/redundant trains is limited by common cause failures. When a high reliability is required, diverse means of carrying out the safety function need to be incorporated. Diversity can be provided by:

- Carrying out the safety function by using a different physical process — for example, reactor shutdown can be achieved by dropping control rods into the core or by injecting boron into the primary coolant.

- Using different equipment to carry out the safety function — for example, the use of pumps that are driven by electric motors and steam turbines in two different systems.

- Using equipment of the same type but from different manufacturers in the two different systems.

This approach reduces the likelihood that the same cause would lead to failure of both systems.

**Providing equipment qualification**: the design aim is to ensure that structures, systems and components are able to withstand the environmental conditions and loadings that they would experience following accident conditions and different initiating events. This is done by defining design basis events — for example, the Design Basis Earthquake (DBE). Analysis needs to be carried out to demonstrate that structures would not fail, and systems and components would be able to carry out their safety functions where required following the DBE. The way in which the DBE needs to be defined is often prescribed in regulatory guidance.

**Limiting the claims made on the plant operators**: the design aim is to ensure that the demands made on the plant operators in fault conditions are achievable. This is done by applying deterministic requirements, which, for example, require that no operator actions should need to be carried out in the very short term (defined as within the first 10 to 30 minutes in some Member States) in the main control room or in the short term (within the first two hours) in any plant area following any initiating event.

In some Member States, these deterministic requirements are defined in the regulations or guidance produced by the regulatory body and are strict legal requirements that need to be met by the operators of the nuclear facility. In others, a goal setting approach has been adopted that gives the regulatory body a higher degree of flexibility on the way plant operators can meet this type of requirement.

*Treatment of uncertainties in the deterministic approach*

It is recognized that there are uncertainties in many of the issues addressed by the deterministic approach. For example, there are uncertainties in:

- the analytical models, computer codes and data used to predict the behaviour of the plant in operational/accident conditions, and

- the hazard curves that are used to define different hazardous events and the capability of structures, systems and components to withstand such events.

The traditional way in which these uncertainties are treated in the deterministic approach is to make conservative assumptions and use conservative models and data. For example, for Design Basis Accidents (DBAs), the analysis assumes that: (a) the postulated initiating event has occurred, (b) the event occurs at a time when the initial conditions are at the worst end of their range, (c) no credit is taken for the operation of the control systems (unless they aggravate the situation), (d) the worst single failure occurs in the protection systems and (e) conservative damage criteria are used for the aspects of plant safety challenged by the initiating event. The aim of using these assumptions is to ensure that safety margins are available and that there is a high level of confidence that failure conditions are not reached.

The current trend is to use best estimate codes for deterministic accident analyses provided that they are either combined with a reasonably conservative selection of input data or are associated with the evaluation of the uncertainties of the results. A good level of conservatism is still expected to be built into the deterministic analysis needed to demonstrate to the regulatory body that sufficient safety margins exist.

*Strengths of the deterministic approach*

The main strength of the deterministic approach is that it is well developed and that there is a very large body of experience in the Member States in applying this approach to all types of nuclear facilities. It has been the cornerstone of demonstrating nuclear safety since the beginning of the nuclear industry and this has led to a high level of safety in Member States for all types of nuclear facilities.

*Shortcomings of the deterministic approach*

There are a number of shortcomings in the deterministic approach that need to be recognized and these include the following:

- in the past, the deterministic approach has tended to look at infrequent, bounding fault conditions (such as large LOCAs) rather than lesser faults (such as small LOCAs) that are more frequent and often give a greater contribution to the risk.

- the deterministic approach only takes initiating event frequencies and component failure probabilities into account in an approximate way so that it is not possible to show that this approach leads to a balanced design. Indeed, it has often been the case that the deterministic approach has led to a very high level of protection being provided for some initiating events but not for others.

- when a review against deterministic principles has been carried out for an existing plant and shortfalls have been identified, it is not possible to determine which of the possible plant improvements would give the greatest reduction in risk and hence which of them need to be given the highest priority for implementation.

Although the deterministic approach has been refined over the years so that it now takes probabilistic information into account, it is widely recognized that the reliance on a deterministic approach on its own is unlikely to be sufficient to demonstrate that high levels of safety have been achieved in a way that is balanced across initiating events and safety systems. This has been seen from the PSAs that have been carried out and have demonstrated that some of the contributions to the risk have not been adequately controlled by the deterministic approach.

## 2.2. Probabilistic approach

*Background*

The current status is that PSAs have been developed for the majority of the nuclear facilities in the Member States. In some countries, there is a legal requirement for the plant operators to produce a PSA; in others, a PSA has been carried out by the regulatory body. In some Member States, although the plant operators have been producing PSAs for many years, the way in which these plants are regulated is still very much based on the traditional deterministic approach.

Most of the PSAs that have been carried out are for nuclear power plants and the emerging standard is to carry out a plant specific analysis that addresses:

- all internal initiating events (transients and accidents), all internal hazards (fires and floods) and all external hazards (seismic events and extreme environmental conditions);
- both the Core Damage Frequency (CDF) and the Large Early Release Frequency (LERF), taking into account the potential failure modes of the containment following core damage (that is, the analysis is a Level 2 PSA);
- all the modes of operation of the plant including full power operation, low power operation, and the various plant states that arise during shutdown and refuelling;
- all the sources of radioactive material on the nuclear site including the reactor core, irradiated fuel after it has been removed from the core and radioactive waste.

However, it is often the case that the PSAs produced are of a much more limited scope than this. This introduces limitations on the potential uses of the PSA that need to be recognized when it is used as part of the regulatory decision making process.

The PSAs produced are being maintained as Living PSAs [4] so that they can be regularly updated as changes are made to the design or operation of the plant. Where possible, plant data are used for initiating event frequencies and component failure probabilities, and simulator data are used for human error probabilities. Where this is not possible, applicable data from similar plants or generic data are used.

There is now a vast body of experience in the Member States on how PSA should be carried out for all types of nuclear facilities. In recent years, PSA standards and guidance have been developed by international organizations and in many Member States, and much of this is widely recognized and applied. This has played a significant part in ensuring that the PSAs being produced are of a high standard and are suitable for a range of applications. This has increased the level of confidence in the PSAs developed [5, 6].

In addition, the regulatory bodies in many Member States are actively encouraging the use of PSA. As an example of this, the NRC has also fully recognized that PSA has a role in the licensing and regulatory process with the issuance of its PSA Policy Statement [7], the Regulatory Guide 1.174 [8] and its associated Standard Review Plan Chapter [9], and this guidance has been adopted in many other Member States.

The NRC's Policy Statement regarding the expanded use of PSA states that:

- the use of PSA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PSA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defence in depth philosophy;

- PSA and associated analyses (for example, sensitivity studies, uncertainty analyses and importance measures) should be used in regulatory matters, where practical within the bounds of the state of the art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments and staff practices. Where appropriate, PSA should be used to support the proposal for additional regulatory requirements in accordance with the Backfit Rule — see Ref. [10]. Appropriate procedures for including PSA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised;

- PSA evaluations in support of regulatory decisions have to be as realistic as practicable and appropriate supporting data need to be publicly available for review;

- the Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

The maturity of the probabilistic approach is now at a level that allows PSAs to be used by the regulatory bodies in the Member States for a wide variety of purposes. It has been recognized that the PSA provides a good framework for addressing uncertainties and for highlighting the areas of subjectivity, and this has led to an increased acceptance of PSA as a regulatory tool.

*Probabilistic criteria*

In some Member States, probabilistic criteria have been defined. For nuclear power reactors these typically relate to CDF and LERF.

A possible framework for the definition of probabilistic criteria was given by INSAG [11]. 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 reasonable achievable measures have been taken to reduce it.

Based on current experience with nuclear power plant design and operation, numerical values were proposed that could be achieved by current and future designs. For the CDF, the

objective is $10^{-4}$ per reactor-year for existing plants and $10^{-5}$ per reactor-year for future plants. For a large release of radioactive material, the objective is $10^{-5}$ per reactor-year for existing plants and $10^{-6}$ per reactor-year for future plants.

The same framework has been used in the UK where risk criteria have been defined for doses to members of the public (five dose bands have been defined), the risk of death of workers, a large release of radioactivity from the plant, the risk of plant damage (which equates to core damage for a nuclear power plant), and an inadvertent criticality incident in stored fuel or radioactive waste. In each case, a Basic Safety Limit (BSL) and a Basic Safety Objective (BSO) have been defined [12]. Although all these criteria should ideally be addressed by the PSA, the main focus for nuclear power plants has been to address the accident sequences that lead to plant damage and to an off-site dose of >1 Sv, requiring that a full scope Level 2 PSA is carried out. If the frequency is above the BSL, operation of the plant would not be allowed. If the frequency were below the BSO, the regulatory body would not seek further improvements to be made to the plant (although the law requires that the plant operators should consider them). If the frequency is between the BSL and the BSO, the regulatory body would require improvements to be made to reduce the risk until it was satisfied that the level of risk was as low as reasonably practicable (ALARP).

In the Netherlands, the concept of environmental risk management has been developed that sets criteria and objectives that relate to individual and societal risk. The requirement is that the risk of death of an individual should be $<10^{-5}$ per year from all sources of radioactivity and $<10^{-6}$ per year from a single source. The societal risk (defined as the death of 10 people within a few weeks with no credit being taken for countermeasures) should be $<10^{-5}$ per year with more restrictive criteria being defined if greater numbers of people are affected. This requires that a Level 3 PSA be carried out as part of the licensing process for nuclear installations.

In other Member States, probabilistic safety criteria have been defined as targets, goals, objectives, guidelines or reference values for orientation.

In the USA, acceptance criteria for addressing changes in the design or operation of a plant that would lead to a change in the risk (CDF or LERF) are given in Ref. [8]. These are:

- changes that lead to a reduction in the risk (CDF and LERF) would normally be allowed;
- changes that lead to a small increase in the risk ($<10^{-6}$ per reactor year for CDF and $<10^{-7}$ per reactor year for LERF) would normally be allowed unless the overall risk is high ($>10^{-4}$ per reactor year for CDF or $>10^{-5}$ per reactor year for LERF) in which case the focus would need to be on finding ways to reduce the risk;
- changes that lead to a moderate increase in the risk (in the range $10^{-6}$ to $10^{-5}$ per reactor year for CDF or $10^{-7}$ to $10^{-6}$ per reactor year for LERF) would normally be allowed only if it can be shown that the overall risk is small (that is CDF < $10^{-4}$ per reactor year and LERF $<10^{-5}$ per reactor year);
- changes that would lead to a large increase in the risk ($>10^{-5}$ per reactor year for CDF or $>10^{-6}$ per reactor year for LERF) would not be allowed.

These guidelines are intended for comparison with the results obtained by using a full scope Level 2 PSA to determine the change in the CDF or LERF for the proposed change to the design or operation of the plant.

*PSA scope, level of detail and quality*

One overall requirements is that the scope, level of detail and quality of the PSA needs to be consistent with its intended applications and the role that the probabilistic input plays in the decision making process.

**PSA scope**: The goals and scope of the PSA, and its intended applications need to be clearly defined at the start of the analysis. The scope of the PSA needs to be wide enough to include all the relevant initiating events and address all the relevant modes of operation of the plant. The emerging standard for PSAs currently produced is to aim for completeness so that all the contributions to the risk are addressed in the analysis. This includes all internal and external initiating events and hazards and addresses all the modes of operation of the plant. However, the scope of the PSA used may sometimes be less than this and, if this is the case, the limitations in its use will need to be recognized.

**Level of detail of the PSA**: This needs to be sufficient to allow the impact of the proposed changes in the design or operation of the plant to be modelled. The emerging standard is for PSAs to be carried out to a detailed component level, which would normally allow the change in the CDF or LERF to be estimated for the majority of the proposed changes. If this is not the case, it may be necessary to amend the PSA for the proposed application.

When a PSA is carried out, it is good practice to have an appreciation of the likely uses of the PSA so that it can be done in a way that supports these applications. For some applications, the required risk information can be generated by developing a very simple probabilistic model. However, for other applications, such as configuration risk management, a very detailed PSA model is required. In general, the more detailed the PSA model produced, the wider will be the range of applications for which the PSA will be suitable.

**PSA quality**: The methods used in the analysis need to be consistent with the state of the art and current best practices as defined in national and international PSA standards and guidance. In recent years, there have been a number of activities to develop PSA standards — for example, the ASME standards [13]. The aim has been to improve the accuracy, consistency and useability of the PSAs produced.

Two additional factors that are important for the production of a high quality PSA are that the analysis has been carried out within a comprehensive quality assurance programme and subjected to an independent peer review [14].

*Strengths of the probabilistic approach*

The strengths of the probabilistic rest in that:

- the analysis starts from a comprehensive list of initiating events and sets out to identify all the fault sequences that could lead to core damage or a large early release;
- the analysis determines quantitatively the level of risk from the plant;

- modern PSA software provides calculations of a number of importance functions that can be used to determine the risk significance of all the initiating events, fault sequences and structures/systems/components included in the PSA model;

- modern PSA software allows some of the parameter uncertainties to be addressed explicitly;

- the PSA can be used to carry out a wide range of sensitivity studies;

- the analysis can be used to determine the degree to which deterministic requirements such as the provision of defence in depth and the single failure criterion have been met;

- the analysis can be used to identify where improvements to the design and operation of the plant are needed to give the greatest reduction in risk;

- the PSA provides a very good means of comparing relative risks (but perhaps not so good for predicting absolute values of the risk).

*Shortcomings of the probabilistic approach*

There are shortcomings in the probabilistic approach that arise from the scope or level of detail of the PSA. These are limitations when a particular PSA is being used for some applications. It is important to recognize this fact and to ensure that the PSA model is not used outside its range of validity. For example, if the PSA that has been carried out is a Level 1 analysis, this will only address the role of the containment in providing protection against design basis initiating events, such as steam line break and LOCA, and will not address the role that it plays in preventing a release of radioactivity following severe accidents. This shortcoming relates to the use of a particular PSA for a particular application (rather than of PSAs in general) and need to be recognized by the user of the PSA when providing an input into the risk informed process.

However, despite the long history of the development and successful use of PSAs at nuclear facilities, there is still a degree of reluctance to use them in some areas. The concerns raised by potential users of the PSA include the following:

- It is not possible to fully demonstrate that the PSA model is complete in that all the initiating events and fault sequences that could contribute to the risk have been identified.

- There are very large (orders of magnitude) uncertainties in some areas of the PSA so that the results are difficult to use in the decision making process.

- It is difficult to justify the data used to quantify the PSA, particularly when generic data have been used.

- There are modelling difficulties in some areas of the PSA — for example, modelling human errors of commission and dependency between individual human errors.

- There is a degree of subjectivity in the models developed in some areas of the PSA — for example, modelling the fault sequences that occur following core damage included in the Level 2 PSA.

Owing to the reasons mentioned, it has often been difficult to compare the PSAs that have been carried out for similar plants due to differences in methodology and data.

It should be stressed that this is a limitation for the potential application of the PSA rather than the PSAs themselves. However, this has led to reluctance by some regulatory bodies to accept the use of PSA to the extent that they are able to move towards a risk informed approach.

*Problems with the application of PSA*

It should be clear that PSA can only be a contributor to the decision making and not the sole determinant. In some people's minds, risk is inevitably linked to the use of PSA, which gives a numerical value to the likelihood of a particular consequence: indeed this combination of a consequence and its likelihood is often referred to as the "risk". However, as was pointed out earlier "risk" is a wider concept than this and risk concepts can be considered in a qualitative manner. There may be aspects of the operation of the installation where it is only possible to make a qualitative analysis or where a decision is made without recourse to a PSA.

It is good practice that the need for an analysis and the depth and quality required are always judged on the importance to the safety issue considered — this is as true of PSA as for any other method of analysis. There is a great danger in spending too much time and effort on the analysis rather than on practical measures that will affect safety. Thus the quality required cannot be set independently of the application and even a low quality PSA may provide some insights when integrated with other factors.

A danger of concentrating too much on a quantitative risk value that has been generated by a PSA is that inadequate engineering solutions or operational procedures may be apparently justified by meeting numerical criteria. Equally, a well-designed plant can be operated in a less safe manner due to poor safety management by the operator. Other considerations need to be judiciously used to provide the best solution to a safety issue. For example, when using risk analysis in design applications, it is usual to produce an outline design based on sound engineering practice and check that the design is fault tolerant by making conservative deterministic assumptions. A risk analysis, e.g. a PSA, is then carried out to ensure that the design is balanced and there are no weaknesses. It is important first of all to get the design right and then develop risk estimates. Otherwise there may be a danger of misusing PSA for justifying poor engineering and operation.

*Treatment of uncertainties in the probabilistic approach*

There are two types of uncertainties that arise — aleatory uncertainties and epistemic uncertainties — these need to be treated differently in the PSA. **Aleatory uncertainties** arise due to the random or stochastic nature of the events being modelled in the PSA and these are taken into account in the probabilistic models. **Epistemic uncertainties** arise due to limitations in the state of knowledge of the analysts carrying out the PSA.

This lack of knowledge gives rise to three types of uncertainty in the PSA — namely parameter uncertainty, model uncertainty and completeness uncertainty. They can be addressed in the PSA as follows:

**Parameter uncertainty**: this relates to the uncertainty in the parameters used in the quantification of the PSA model including initiating event frequencies, component failure

probabilities and human error probabilities. These uncertainties can be characterized in general by probability distributions. Most of the PSA software has the capability to propagate these uncertainties through the analysis and calculate the probability distribution for the PSA results.

**Model uncertainty**: this relates to the uncertainty in the assumptions made in the analysis and the models used. This includes the assumptions made, e.g. on how a reactor coolant pump would fail following loss of seal cooling and/or injection, and the way how aspects of the PSA such as common cause failure and human error are modelled. The normal approach is to address model uncertainties is to carry out studies to determine the sensitivity of the analysis on different assumptions made or models used.

**Completeness**: this relates to contributions to the risk of events that are not included in the analysis. This could include limitations in the scope of the PSA by some classes of initiating events, hazards or modes of operation not being included. In addition, it could include factors such as the effects on the risk due to ageing or organizational factors where there is no agreement on how these factors should be addressed in the PSA. Hence, there is a degree of uncertainty on what the true level of the risk would be and this needs to be recognized as a limitation of the PSA.

### 2.3. Benefits of an integrated approach

The deterministic and probabilistic approaches are both systematic approaches aimed at ensuring that the risk from the nuclear facility to workers and members of the public is adequately controlled. However, they use different assessment techniques and boundary conditions and thus have different strengths and limitations. Some of the major differences between the two approaches are shown in Table 1:

There are a number of safety issues that can be better understood and evaluated if an integrated approach to safety assessment is applied; these include the following:

- **demonstration that the design is balanced across initiating events**: with the use of PSA, it is possible to determine whether the design is balanced — that is, whether any group of initiating events makes a contribution to the risk that is much larger than the others. This is only tackled in an approximate way by the deterministic analysis. For example, usually greater levels of redundancy and diversity need to be provided for frequent initiating events than for infrequent initiating events

- **demonstration that the design is balanced across levels of defence in depth**: using the PSA, it is possible to take account of the interdependencies between the various levels of defence in depth and provide information on the relative worth of each of them and in general on how well the defence in depth concept has been implemented. This is not possible using the deterministic approach alone

- **determine the importance of structures, systems and components**: the PSA models all initiating events, hazards and structures/systems/components in a single model. Hence, it is possible to derive the relative importance of each of them explicitly. Such an explicit ranking is not possible in the deterministic approach since it treats each of the initiating events and hazards separately.

TABLE 1. COMPARISON BETWEEN DETERMINISTIC AND PROBABILISTIC APPROACHES

| **Deterministic approach** | **2.4.Probabilistic approach** |
|---|---|
| Usually uses a conservative/bounding assumptions approach to address uncertainties in the models and data | Usually uses a best estimate approach in all aspects of the modelling; sometimes conservative assumptions are used to determine the success criteria |
| Addresses a limited subset of initiating events and fault sequences that are chosen as the bounding ones | The starting point is a comprehensive set of initiating events and hazards (including those that are within and beyond the design basis) and they are all included in the analysis |
| Accident conditions are addressed separately | The PSA model integrates all initiating events and safety systems in the same model |
| Initiating event frequencies and system/ component failure probabilities are taken into account in an approximate way | Initiating event frequencies and system/ component failure probabilities are included explicitly in the PSA model |
| Uncertainties are addressed by making conservatisms assumptions, or using best estimate codes and models with associated evaluation of the uncertainties in the results | Many of the uncertainties can be addressed explicitly in the PSA models. The capabilities to address parameter uncertainties are included in modern PSA software |
| Gives a rough indication of the relative importance of systems/structures/components | Modern PSA software provides a wide range of information on ways to measure the importance of all the systems/structures/ components that are included in the analysis |

Hence, the insights provided by the probabilistic approach complement those provided by the deterministic approach. In view of this, the trend is for many regulatory bodies in the Member States to move towards a much more risk informed approach in which the insights from the risk information provided by the PSA is used formally as part of an integrated decision making process.

When this integrated process is applied to making decisions about safety issues at nuclear facilities, this is sometimes referred to as risk informed decision making. When it is applied to making decisions about the way in which a regulatory body carries out its activities, this is sometimes referred to as Risk informed Regulation.

It should be noted that, in risk informed decision making and risk informed regulation, the PSA provides only one of the inputs into the decision making process — the others being

related to factors such as the degree to which any mandatory requirements are met, the insights from the deterministic analysis, the results of any cost benefit analysis, special considerations, etc. None of the Member States is applying a risk based approach in which the input from the PSA (or other risk analysis) is the sole input into the decision making process and this practice is not advisable.

## 3. INTEGRATED DECISION MAKING APPROACH

### 3.1. Introduction

The integrated decision making process (sometimes referred to as a risk informed decision making process) is a structured process in which all the insights and requirements which relating to a safety or regulatory issue that needs to be dealt with by a regulatory body are considered in reaching a decision. It includes the recognition of any mandatory requirements, the insights from the deterministic analysis, the insights from the probabilistic analysis and any other applicable insights. In addition, once the decision has been made, there is a need to implement it and monitor in order to determine how effective it has been and whether there is a need to revise the decision. This process is shown in Fig. 1 and described in more detail below.

**Mandatory requirements** would typically include any legal requirements, regulations and plant technical specifications. The aim would be to ensure that they were complied with unless, of course, the issues being addressed was a proposal to make amendments to regulations or to seek an exemption from the plant technical specifications. One of the overriding mandatory requirements in many Member States is that the risks be reduced to a level that is as low as reasonably achievable.

The extent to which the proposed change falls short of any of the **deterministic requirements** needs to be identified. At a high level, the deterministic requirements relate to whether the defence in depth requirement is met, e.g. by multiple barriers to the release of radioactive material from the plant, and whether adequate safety margins are being maintained. At a lower level, this relates to whether there are sufficient levels of redundancy and diversity in the safety systems that perform safety functions, that the equipment in the plant has been qualified to a sufficient level so that it can withstand the effects of initiating events and the harsh environments that would occur following initiating events, etc. The deterministic analysis provides insights on whether the deterministic requirements have been met and, if it is not the case, where the weaknesses are.

For a nuclear power plant, the **risk insights** are normally obtained from carrying out a PSA to determine the CDF or LERF. The emerging standard in the Member States is to produce full scope Level 2 PSAs that address all initiating events and hazards and all the modes of operation of the plant. The PSA provides an estimate of the level of risk from the plant and the results (cut sets, importance functions, etc.) can be used to determine where there are weaknesses in the design or operation of the plant.

In addition, there are usually **other factors** that need to be taken into account in making a decision. These could include the costs and benefits that would arise from making the proposed change, the remaining lifetime of the plant, inspection findings, operating experience, etc. Doses to workers that would arise in making changes required to the plant hardware would also be taken into account.

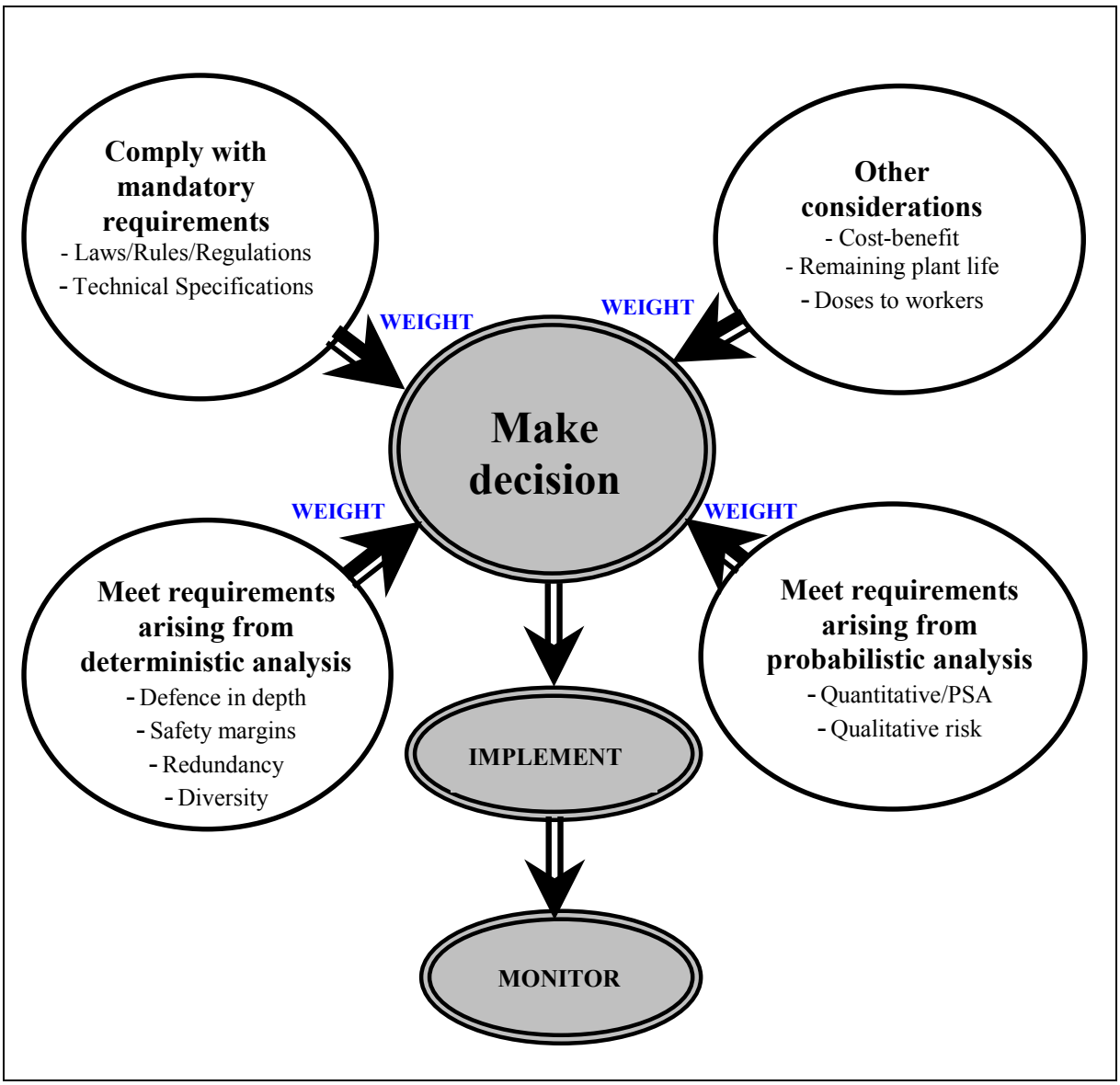



*FIG. 1. Integrated decision making process.*

The aim of a structured decision making process is to ensure that a balanced decision is made that has identified and taken into account all the factors that are relevant to the decision. In addition, this approach will make decisions easier to document, easier to verify, allow greater openness, allow better communication, etc. However, resources will need to be provided for the regulatory body to allow this process to be carried out.

The integrated decision making process may be applied to a variety of issues that need to be addressed by a regulatory body. This includes decisions on plant safety issues that need regulatory body approval and decisions on how the regulatory body operates.

Examples of plant safety issues that need authorization and could be addressed by an integrated decision making process include whether to make changes to:

- the design or operation of the plant;
- the plant technical specifications/limits and condition for normal operation;

- the frequency of in-service inspection, in-service testing, maintenance, statutory outages;

- the quality assurance arrangements — in particular, whether to introduce a graded QA system that recognizes the risk significance of items of equipment;

- the allowed combinations of safety system equipment that may be removed from service/configuration control during power operation and shutdown modes;

- the emergency operating procedures and accident management measures.

The way in which the integrated decision making process is applied to these issues is described in Section 4 which also gives some practical examples.

Where the decision being made involves changes to the plant design or operation, a decrease or increase in the risk and needs to be taken into account. If the proposed change leads to a decrease in risk, often a cost-benefit analysis is carried out to determine whether the cost of making the changes is not excessive compared to the benefits that would be obtained. If the proposed change leads to an increase in risk, this may be acceptable in some Member States if the level of risk is acceptable and the magnitude of the increase is small — for example, if it is within the limits given in Ref. [8]. However, in other Member States, changes that would lead to an increase in the risk are not formally acceptable and the risk increase would need to be shown to be negligible or compensated for by some other means.

Issues related to the way a regulatory body operates and that can be addressed by an integrated decision making process include the following:

- making changes to regulations;

- planning regulatory inspections;

- responding to incidents at a plant;

- carrying out enforcement actions;

- initiating and coordinating safety related research.

The way in which the integrated decision making process is applied to these issues is described in Section 5. An example of how this process was applied by the NRC to change one of its regulations is given in the Appendix.

In applying the integrated decision making process, care needs to be exercised if more than one issue is being considered at the same time since the cumulative effect of the decisions becomes relevant. If the issues are considered together, a relatively large increase in risk of one element could be masked by a large decrease in risk in the other. Hence, it is good practice to consider each of the issues separately to make sure that each individual decision would also be acceptable.

As noted earlier, the integrated (risk informed) decision making process described here is fundamentally different from a risk based approach, where the insights from the risk analysis would be used as the sole input to the decision making process (or this input would

be weighted very heavily). It should be noted that no regulatory bodies in any Member State applies a risk based approach.

### 3.2. Application of an integrated decision making process

In this section, a possible approach to applying the integrated decision making process as outlined in Section 3.1 and shown in Fig. 1 is described in more detail. The steps in the process are shown in Fig. 2 and described below. The aim is to describe the systematic process that is followed and identify good practice in applying an integrated decision making process.

***Step 1: Defining the issue***

The first step is to define the issue to be addressed by the integrated decision making process. This could include any of the types of issues that a regulatory body would need to address as identified in Section 3.1. Although the steps that would need to be followed in the decision making process would be broadly the same for all of them, the way in which the probabilistic, deterministic and other insights would be obtained and the weights given to these insights would be different.

***Step 2: Identifying the applicable requirements and criteria***

The next stage in the process is to identify the requirements and criteria that relate to the specific issue to be addressed. These will usually include the mandatory, deterministic, probabilistic and other requirements as follows:

*Step 2a: Identifying the mandatory requirements*

A review will need to be carried out to determine if there are any mandatory requirements that relate to the issue being addressed. This will depend on the type of issue, but could include legal requirements, governmental decrees, current regulations, plant technical specifications, etc.

These mandatory requirements will generally by very different in the Member States depending on the style of regulation that is followed. Where these are very prescriptive, there may be a number of very detailed legal requirements/regulations/guidance that would need to be identified and addressed. However, this would not be the case where the regulatory regime is non-prescriptive since it is accepted that there is likely to be more than one way to achieve the overall safety goals.

One of the mandatory requirements in many Member States is the need to ensure that the risk is reduced to a level that is as low as reasonably practicable.. In many Member States the test of reasonable practicability is to show that the costs of making the change are not excessive when compared to the benefits that would be obtained. This is often addressed formally by carrying out a cost-benefit analysis.

*Step 2b: Identifying the applicable deterministic requirements*

If the issue being addressed relates to the design and operation of a nuclear facility, the higher-level deterministic requirements will relate to addressing defence in depth and maintaining sufficient safety margins.

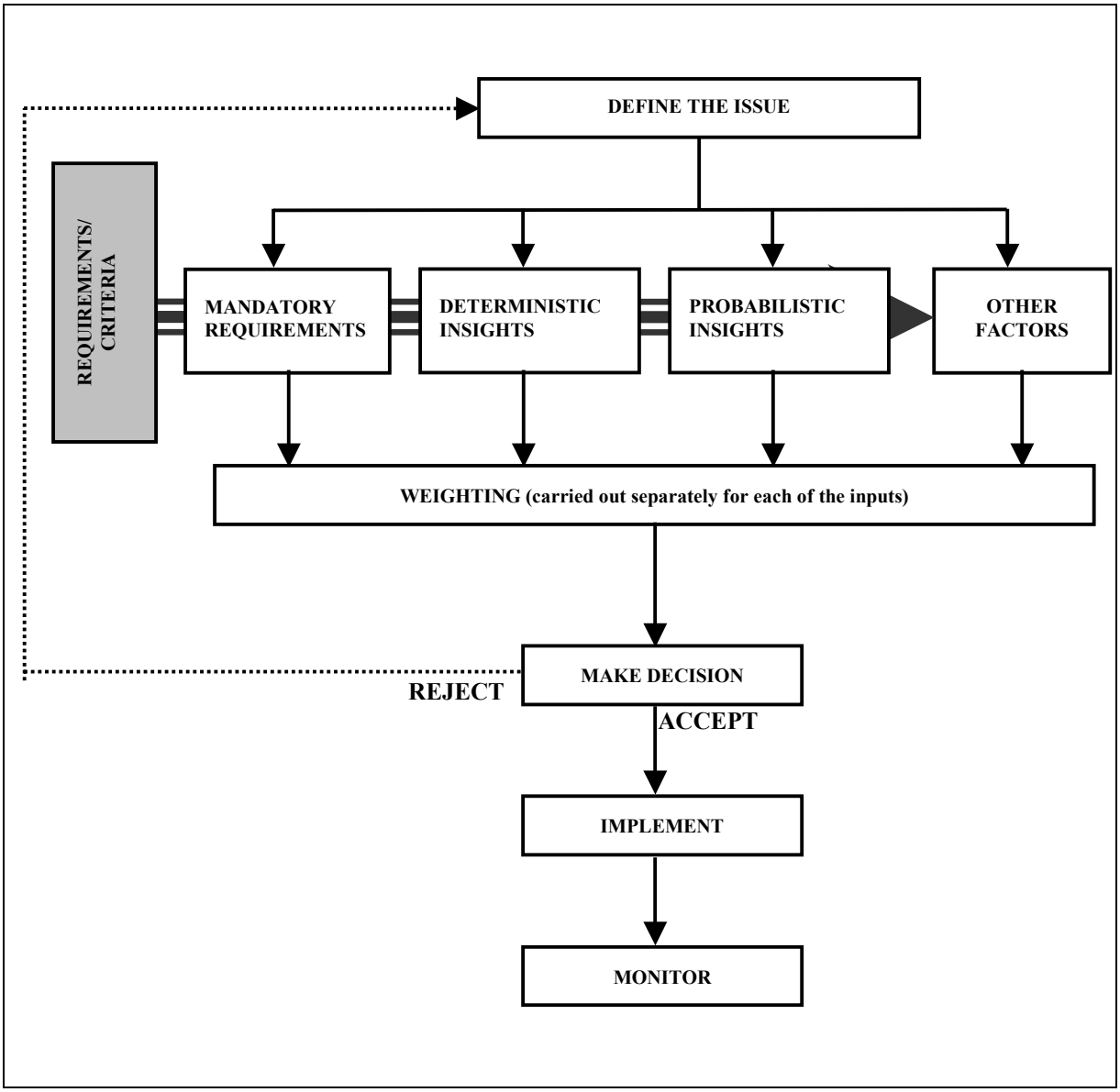



*FIG. 2. Steps in the integrated decision making process.*

The aim of addressing defence in depth is to ensure that focus is given to preventing initiating events, providing safety systems to prevent core damage, preventing containment failure and mitigating the consequences of any releases or radioactive material that could occur. This will ensure that multiple barriers are maintained intact to prevent the release of radioactive material from the plant. Maintaining sufficient safety margins means that the plant will remain within the safe limits defined in the safety analysis report/safety case so that there is a considerable margin between the conditions reached in fault conditions and an ultimate failure condition. These high level aims compensate for uncertainties in the modelling, and the lack of knowledge and understanding of the various physical phenomena that could occur in accident conditions.

At a lower level this will relate to the levels of redundancy, diversity, separation, segregation, equipment qualification, etc. required for safety systems, the restrictions on the need for operators to carry out action in a short timescale following an initiating event, etc.

If the issue relates to the way in which the regulatory body carries our its regulatory activities, the deterministic requirements will relate to the way in which the Regulations have been formulated, the existing practices and the reasons for working in that way.

*Step 2c: Identifying the applicable probabilistic requirements*

Risk criteria have been defined in some Member States. For nuclear power plants, these usually relate to the CDF and LERF. In addition, lower level requirements may have been set that relate to the reliability of the safety systems.

However, in many Member States, no such formal risk criteria have been defined. The aim has been to show that the risk from the plant is at about the same or lower as that from other similar plants worldwide where details of the PSA that has been carried out are available. The results of the PSA are used to identify weaknesses in the design or operation of the plant.

The changes that are proposed could lead to a decrease or increase in the risk (CDF and/or LERF). Where there is a reduction in the risk this would generally be acceptable to the regulatory body if it could be shown that the cost of implementing the change was not excessive. However, if there is an increase in risk, criteria will need to be developed to decide what is acceptable. If the plant marginally satisfies the safety criteria, an increase in the calculated risk is usually not acceptable, unless other non-quantitative safety considerations play an important role. If the plant satisfies the safety criteria with a considerable margin, larger increases in the estimated risk may be tolerable (unless no increase is formally acceptable, as discussed above).

An example of what is considered to be an acceptable increase in risk is given in Ref. [8], which is applied in the USA and in some of the other Member States — see Section 2.2. However, some other regulatory bodies would only allow a change to be made which would lead to an increase in the risk if this was shown to be negligibly small or could be compensated for by other changes that would be carried out at the same time and would decrease the risk.

*Step 2d: Identifying any other applicable requirements*

The aim of this step is to identify all the other factors that need to be taken into account in the decision-making process and to decide how these factors should be addressed. This would typically include economic factors important for plant operation, such as the cost of making the change (which would include the design/manufacture/installation/commissioning costs) and any benefits to the plant (which would include the increased revenue from the plant due to its higher availability or higher power level). This would also take account of the dose burden to workers in making changes to the plant, the remaining lifetime of the plant, inspection findings and operational experience.

***Step 3: Determining how the proposed change affects the mandatory requirements***

In this step, a review will be carried out to determine if there are any shortfalls in meeting any of the mandatory requirements identified in Step 2a.

***Step 4: Carrying out the assessment to get the deterministic insights***

In this step, an assessment is carried out by comparing with the applicable deterministic requirements identified in Step 2b. The aim would be to identify any areas where these requirements are not met.

For defence in depth requirements, the aim would be to determine if there were any shortfall in the provisions made for preventing initiating events from occurring, for coping with initiating events, for containment so that radioactive material is not released to the environment and for protecting the public if a release should occur. The aim would be to determine whether any of these provisions fell short of the defined standard.

For safety systems, the aim would be to determine whether sufficiently diverse equipment had been incorporated to provide protection against frequent initiating events, whether sufficient redundancy had been provided by applying the single failure criterion to safety systems, etc.

***Step 5: Carrying out the assessment to get the probabilistic insights***

The aim of this step is to carry out an assessment using the probabilistic criteria identified in Step 2c to determine the risk significance of the issue being addressed. If the issue relates to a change to the design or operation of a nuclear power plant, the risk may change — that is, it may decrease or increase. For nuclear power plants, risk insights are generally obtained by using a formal risk analysis/PSA and this would be taken forward in making the decision. For other situations, this could be a less formal input.

A fundamental requirement is that the PSA be based on an accurate model of the design and operation of the plant and is of a sufficient scope, level of detail and quality for its intended use. This could be different depending on the type of decision being made and the role that the PSA results would be expected to play in the integrated decision making process.

However, it needs to be recognized that there may be limitations to the PSA, which may not be able to provide all the information that would be required. For example, the scope of the PSA might be limited in that it does not include the risk from external hazards or it may not address the contributions to the risk from low power and shutdown modes of operation. In addition, the current state of the art for PSA means that some issues such as component ageing, safety culture, etc. are not addressed. The regulatory body will then need to decide how to address those PSA limitations — that is, whether to require a PSA of higher quality to be developed or to allow use of alternative methods to account for the identified deficiencies in the PSA.

***Step 6: Carrying out the assessment to gain insights from the other relevant factors***

The aim of this step is to generate the information required to address the other relevant considerations identified in Step 2d. This could include:

- the doses to workers that would be incurred while carrying out the work to make any changes required to the design of the plant;
- the costs and timescales for carrying out the work, which would include an identification of any periods for which the plant would need to be shut down;

- any benefits that would arise — for example, an increase in the revenue from the plant;
- a cost-benefit analysis to compare the costs of making the modifications to the benefits that would be obtained from it;
- any adverse factors that could arise in making the change. for a nuclear power plant, this could include an increase in the operational complexity of the plant and any additional burden on the plant operators;
- insights from the operational experience data or inspection findings that are relevant to the issue.

***Step 7: Weighting the inputs from the assessments carried out***

The aim of this step is to determine the weight that needs to be attached to each of the inputs to the decision making process derived from Steps 3, 4, 5 and 6. From the example presented in the Appendix, it can be seen that much of this weighting is subjective and relies on engineering judgements. In fact, the judgements made by the NRC commissioners were different from those made by the NRC staff.

Where the insight relates to mandatory national legal requirements or to the need to meet established national practices, these would normally carry the highest weight and will have to be observed (unless, of course, the issue being considered relates to a change in rules or regulations or seek regulatory exemption).

This weighting process could be carried out quantitatively using a formal cost-benefit analysis or could be done qualitatively.

It is often the case that the deterministic and probabilistic insights are in agreement. For example, for a modification that improves the deterministic position — for example, it increases the level of redundancy or diversity in the safety systems, it will also lead to a reduction in the risk. In this case, the relative weighting of the deterministic and probabilistic insights may be less important and the outcome of the decision may depend on other factors such as the dose to workers or the results of the cost-benefit analysis.

If the deterministic and probabilistic insights are not in agreement, it is often the case that greater weight is given to the more conservative insight — that is, the one that indicates a need for improvement.

The weighting that would be applied to the need for a modification would be greater if the results of the probabilistic analysis showed that the overall risk from the plant was approaching a level that was not acceptable or if the change to the plant removed one of weaknesses in the design or operation of the plant that has been identified from the PSA.

There are differences in the weights that are applied in the Member States. For example, for some regulatory bodies, changes that would lead to an increase in risk would not be allowed unless it could be shown that the increase in risk was negligible or could be offset by some means.

It should be recognized that there are significant national differences in the regulatory approach and the way in which plant safety issues have been resolved. In many countries, the

regulatory approach has been based very strongly on the traditional deterministic approach, which would be difficult to change. In addition, although the worldwide view is that carrying out PSAs has reached a high level of maturity, there is still a reluctance to accept PSA as one of the major inputs into the decision making process so that PSA results and insights are sometime given a lower weighting than the scope, level of detail and quality of the PSA would warrant.

Differences in the weighting that has been applied to safety issues has led to differences in the way how safety issues have been resolved. An example of this is that filtered containment venting systems and other equipment such as hydrogen re-combiners have been incorporated to increase the level of defence in depth against severe accident scenarios in some Member States but not in others due to the greater significance that has been placed on providing protection for the containment.

***Step 8: Making the decision***

The aim of this step is to make a decision on whether the change (to the design or operation of the plant, the regulation under consideration, etc.) should be made. This requires that the individual insights and their associated weights are combined and a decision made.

As the decision making process will usually require very different inputs and factors with often very different weights to be considered and combined in reaching a decision, it is good practice that (for major decisions at least) the decisions are made by a multidisciplinary panel. It is good practice that the panel be composed of members who collectively have expertise in all the areas concerning the decision. This would usually include expertise in plant operation, maintenance, engineering, safety analysis, licensing and PSA, depending on the application at hand. The panel will need to be capable of handling inputs with different weights. In addition, due account will need to be taken of the uncertainties associated with the deterministic and probabilistic analyses, and the other factors taken into account in the decision making process.

There may be additional factors that the regulatory body may wish to take into account in making the decision. These could include the cumulative impact of previous changes that have been made, and the overall performance of the plant as reflected by inspection findings, operational data and plant performance indicators.

If an integrated approach is to be followed, this will require a degree of flexibility from the regulatory body in that it will need to move away from placing an overriding reliance on the traditional, deterministic approach and depart from requirements and practices that have been applied over many years if it can be demonstrated that this is not risk significant.

The final part of this step is to document the decision made along with the reasons for arriving at the decision. This needs to record all the inputs derived from Steps 1 to 7 and the weights assigned to these inputs. The aim is to ensure that the reasons for arriving at a particular decision are transparent and auditable.

***Step 9: Implementing the decision***

The next step in the process is the implementation of the decision. For plant safety issues, this would require the regulatory body to approve the programme of work by the plant operators to make the necessary changes to the design or operation of the plant and the

corresponding changes as required to items such as plant safety documentation, operating procedures and training.

For issues related to the work carried out by the regulatory body, the necessary changes would need to be made to the work programme. Moreover, the way in which changes towards risk informed regulations would be implemented depends on the respective national legislative system and the legal status of the regulations.

***Step 10: Monitoring the effect of a decision***

It is good practice that the consequences of any decisions made be monitored and feedback provided on their effectiveness. The aim of monitoring is to determine whether the change has been made effectively and whether there are any adverse effects. Such monitoring is usually performance based.

For changes to the design or operation of a nuclear facility, a monitoring process would usually be agreed with the plant operators and this would be included in inspection activities by the regulatory body. The monitoring programme needs to be consistent with the risk significance of the affected systems, structures and components.

For changes to the way in which the regulatory body carries out its duties, a monitoring programme needs to be set up using appropriate performance indicators to determine whether the new activities are delivering more efficient and effective regulation.

For changes to regulations, the performance of the regulatory body and the plant operators in implementing the new regulations needs to be monitored.

**USNRC Regulatory Guide 1.174**

The approach described above is consistent with the principles set out in USNRC Regulatory Guide 1.174 [8] and outlined below:

- The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change.
- The proposed change is consistent with the defence in depth philosophy.
- The proposed change maintains sufficient safety margins.
- When proposed changes result in an increase in CDF or LERF, the increases has to be small and consistent with the intent of the Commission's Safety Goal Policy Statement — see Ref. [15].
- The impact of the proposed change has to be monitored using performance measurement strategies.

Although these principles have been stated in relation to making changes to the licensing basis for a plant, they apply more generally to the risk informed decision making process.

### 3.3. Requirements of the regulatory body

For a regulatory body, implementing a risk informed approach will require a significant change in the traditional approach to regulation. In particular, it will require a higher degree of **flexibility** in the way of working which will involve the use of **multidisciplinary teams**. Furthermore, there will be a requirement for **additional resources and budget**. The integrated approach provides a framework for the **documentation** of the decisions being made, which would allow for greater **openness** in the way in which the regulatory body makes decisions. These issues are discussed below.

**Flexibility**: the application of the integrated decision making process may require a different way of thinking for a regulatory body that has followed a decision making process based mainly on deterministic insights. To be able to get the most benefit from applying a risk informed approach, the regulatory body will need to adopt a more flexible approach that is open to moving away from the traditional deterministic approach. There will be a need for an acceptance of the risk informed approach and a willingness to move away from the traditional ways of working, inspection programmes, regulations, way of dealing with plant operators/licensees, etc. There will be a need to move from a prescriptive approach to a more goal-setting approach to nuclear safety. Developing a policy for the use of PSA insights and defining appropriate probabilistic safety criteria may facilitate the transition process towards risk informed regulation.

**Use of multidisciplinary teams**: it is advisable that, in making decisions, the regulatory body use experts in relevant disciplines such as plant operations, maintenance, engineering, safety analysis, licensing and PSA. For major decision, it is suggested that an expert panel be set up that is capable of handling a diverse set of inputs with different weights.

**Additional resources/budget**: these changes will require a clear commitment on the side of all parties involved. Sufficient budget and staff need to be allocated to the various tasks, both in the industry and in the regulatory body. People need to be trained in the way they have to fulfil the new tasks. This may require that a number of staff will receive training in PSA technniques. It is important that experience be fed back into the programme, both in the use of the elements of the risk informed decision making process and in the training.

**Documentation/openness**: the integrated approach provides a framework for both making a decision and documenting how the decision has been made. It is recommended that the regulatory body document all the steps that have been taken in making a decision. This will provide a greater transparency in the way the decisions have been made by the regulatory body. However, it needs to be recognized that documenting the decision in this way will require additional resources.

## 4. INTEGRATED DECISION MAKING FOR PLANT SAFETY ISSUES

### 4.1. Overview

This section describes how the integrated decision making process is being applied by regulatory bodies in making decisions about safety issues at nuclear facilities. This could include requests by the plant operators to make changes to the design of the plant or changes to the way in which the plant is operated, that would entail making changes to:

- the limits and condition for normal operation;
- the frequency (intervals) of in-service inspection, in-service testing or maintenance;
- the way in which maintenance activities are carried out which could include carrying out more maintenance during power operation;
- the frequency of statutory outages;
- the quality assurance arrangements by introducing graded QA.

Section 4.1 describes how the integrated decision making process is applied to these issues and Section 4.2 gives a number of examples that illustrate how this process has been applied.

## 4.2. Description of the integrated decision making process as applied to plant safety issues

This section describes the steps in the integrated decision-making process as set out in Section 3.2 and shown diagrammatically in Fig. 2.

### *Step 1: Definition of the issue*

For the regulatory body the first step in the process is to define the scope of change to be made at the plant. There are a large number of changes that could be addressed using an integrated decision making process, including:

**Changes to the design of the plant**: Improvements are routinely being made to the design of nuclear facilities. The need for such changes could arise as a result of a Periodic Safety Review to determine whether the plant is adequately safe for continued operation. This usually involves a review of the level of safety of the plant using deterministic analysis and/or PSA to identify areas where improvements need to be considered.

The types of modification that have been made to improve the level of safety of nuclear facilities include major changes such as the following:

- Making improvements to structures, systems and components, increasing their capability to withstand external hazards such as seismic events.
- Increasing the level of separation and segregation of safety systems to provide protection against internal hazards such as fire and flood.
- Incorporating additional safety systems to provide a diverse means for performing some of the safety functions.

Other type of modifications include relatively minor ones where individual components are changed for ones with a greater reliability. All improvements would be expected to reduce the risk from the plant.

However, the plant operator may also wish to make modifications that would result in a small reduction in the level of safety and hence give a small increase in the risk from the plant. This could include the following:

- Changing the fuel in a nuclear power plant so that the power level of the reactor can be increased.

- Increasing the quantity of radioactive material stored at the nuclear facility. As an example of this, at a number of plants the spent fuel storage racks have been replaced with high-density racks so that the quantity of the spent fuel that can be stored can be increased to several reactor cores worth.

**Changes to the way the plant is operated**: The plant Technical Specifications give the limits and condition for normal operation and the traditional approach is that they are formulated in such a way that deterministic requirements are met. It is often the case that plant operators consider that these are too restrictive and seek relaxations of these requirements. The case presented is often based on arguments that the increase in risk from making these changes would be low or that they can be offset by other changes that would reduce the risk.

There are many examples of where plant operators have sought to change the way in which the plant is operated to gain a financial benefit. Typical changes include the following:

- Increasing the standard test intervals or allowed outage times for components.

- Carrying out testing of diesel generators less frequently to reduce the wear on them that arises from unnecessary starts.

- Varying the period at which in-service inspection is carried to reduce the burden of carrying out inspections on sections of pipe-work that have little risk significance.

- Increasing the period between statutory refuelling outages (from say 2 to 3 years).

- Increasing the length of shifts for workers from 8 to 12 hours.

- For a nuclear power plant, carrying out more maintenance while the reactor is at power and allowing more components to be removed from service at the same time, which would reduce the duration of plant shutdown.

- Introducing graded quality assurance where the level of QA required reflects the risk significance of components.

Plant operators seek to make these changes because the current requirements are seen to be over-restrictive. In addition, some of these changes would provide a financial benefit to the plant operators. However, they would also lead to an increase in the risk from the plant. For both types of changes, the regulatory body can apply an integrated process which will give a framework for considering all the relevant factors in coming to a decision on whether they should allow the change to be made.

***Steps 2a and 3: Mandatory requirements***

**Step 2a is to identify the applicable mandatory requirements**. These may be licensing requirements/regulations that are applicable to the issue being addressed and will need to be identified. The expectation is that the plant would remain inside the licensed domain after any changes have been made (unless, of course, the issue relates specifically to a change in the licensing basis for the plant).

**Step 3 is to determine how the proposed change affects the mandatory requirements**. Although some of these may be overriding requirements, the integrated decision making process would still be followed to ensure that this was done in the optimum way.

The areas where any of the applicable mandatory requirements are not met would need to be taken into account in the decision making process. This would need to be the case for all the issues addressed apart from those that related to a request for an exemption to the existing licensing requirements/regulations.

***Steps 2b and 4: Deterministic approach***

**Step 2b is to identify the applicable deterministic requirements**. There are a large number of deterministic requirements that are applied to the design and operation of nuclear facilities. The high level requirements are:

- to provide defence in depth, and
- to ensure that there are adequate safety margins.

In addition, there are lower level requirements that typically include the following:

- Structures, systems and components in the plant need to be designed so that they will withstand a defined range of initiating events and hazards.
- Redundancy and diversity need to be incorporated into the design of safety systems so that they will not be vulnerable to a single failure or a common cause failure.
- Separation/Segregation needs to be incorporated between the trains of safety systems so that they are not vulnerable to internal hazards such as fire.
- Safety system equipment needs to be qualified so that it will be able to operate in the harsh environment that would arise following design basis initiating events.

**Step 4 is to carry out the assessment to get the deterministic insights**. The change to the design or operation of the plant needs to be reviewed in order to determine how it affects the deterministic requirements. This will be relatively straightforward for improvements made to the plant to bring it up to modern standards or to remove vulnerabilities identified from a Periodic Safety Review or from the PSA since they will tend to increase the level of defence in depth, increase safety margins, improve the resilience of systems/structures/components, etc.

However, the regulatory body will also need to address changes that tend to reduce the level of safety of the plant. For such changes, the review will need to determine the extent to which deterministic requirements such as defence in depth, safety margins, etc. have been affected and to prove that adequate safety level is still ensured.

***Steps 2c and 5: Probabilistic approach***

**Step 2c is to identify the applicable probabilistic requirements**. Probabilistic criteria have been defined in many Member States. The typical approach for the government of

Member States (or the regulatory body on behalf of the government) is to define high level safety goals that relate to the level of risk that is considered to be acceptable for workers and members of the public from the operation of nuclear facilities.

In some Member States, high level goals have been defined that relate to health effects to workers and members of the public from releases of radioactive material. In others, lower level goals have been defined — for example, for nuclear power plants, these typically relate to the CDF and LERF. In addition, there is also a requirement to keep the CDF and LERF as low as reasonably practical — the ALARP requirement. In addition, if it is accepted that changes can be made that would lead to an increase in the risk, the regulatory body need to develop criteria on what would be an acceptable increase in the risk. In general, a larger increase would be allowed if the risk was low (close to the BSO) but this would reduce to zero if the risk was high (close to the BSL) unless other non-quantitative safety considerations play an important role. These are discussed in Section 2.2.

**Step 5 is to carry out the assessment to get the probabilistic insights**. For a nuclear facility, the normal approach is to carry out a PSA. The PSA can be used in two ways; firstly to provide an estimate of the risk from the plant (usually the CDF and sometimes LERF) and to use this analysis to determine whether there are weaknesses in the design or operation, and, secondly, to determine the change in the risk that would arise from proposed changes to the design or operation of the plant.

The PSA is ideally suited to provide an estimate of the change in the risk that would arise from changes to the design or operation of the safety systems. This would include changes such as the incorporation of further trains of safety equipment, addition of a diverse safety system, changing the test interval of safety system components, etc. In addition, it could be used to address the increase in risk that would arise from the removal of one of the inputs into the reactor trip system (see the example given in Section 4.3.5).

If the scope of the PSA includes internal hazards such as fire and flood, it could be used to determine the reduction in the risk that would arise from improvements to the separation and segregation of trains of safety systems. In addition, if the PSA contains a detailed human reliability assessment, it may be possible to estimate the increase in risk that would arise from increasing the duration of shifts from 8 to 12 hours. This could be done, for example, by carrying out sensitivity studies to determine whether the increases in the human error probabilities that could arise due to the longer shifts would be likely to lead to a significant increase in the risk.

In general, PSAs do not include a detailed model of pipe-work failures. Therefore, if there is a need to assess how changes in the in-service inspection intervals will influence the risk, the PSA will need to be expanded to model the pipe-work explicitly and an algorithm developed that will relate the inspection intervals to the frequencies of the pipe-work failure.

It has to be noted that the current state of the art is not developed enough to address explicitly in PSA some specific issues, such as ageing and safety culture. However, sensitivity studies could be carried out to provide an indication of whether these issues are likely to be risk significant.

*Steps 2d and 6: Other requirements/insights*

**Step 2d is to identify any other applicable requirements** and **Step 6 is to carry out the assessment to get the insights from the other relevant factors**. The aim is to ensure that any other relevant factors that have not already been addressed are included in the decision making process. These factors could include the following:

- **Costs**: the cost of making modifications to the design or operation of the plant. This would include the costs of producing the design, procuring the hardware, installation, commissioning, and any losses in revenue that would be incurred if the plant needs to be shut down to make the changes.

- **Radiation doses**: the radiation doses that would be incurred by workers in making the modifications to the design of the plant.

- **Operating experience**: this would include experience from the plant operation and the findings from regulatory inspections. Any adverse findings would need to be taken into account in the decision making process.

- **Economic benefits**: many of the modification that are proposed by plant operators would lead to a benefit — that is, a higher rate of income from the plant or lower maintenance costs. For example, if the issue relates to increasing the power level for a nuclear power plant or increasing the throughput of a fuel reprocessing plant, this would result in an increase in the revenue for the plant. This needs to be recognized in the decision making process although, economic benefits would not usually influence much the decision, as illustrated in the examples included at the end of this chapter.

- **Remaining lifetime**: it is often the case that the need to make modifications is identified as part of a Periodic Safety Review that has been carried out for an older nuclear facility and the remaining lifetime of the plant needs to be taken into account in the decision making process. If the remaining lifetime is short, it may not be reasonably practicable to make a change and consideration needs to be given to whether it would be acceptable for the plant to continue operation without improvements being made.

- **Cost-benefit ratio**: it is often the case that the costs and benefits of making a plant modification are compared by carrying out a formal cost-benefit analysis.

*Step 7: Weighting the inputs from the assessments carried out*

The manner in which the mandatory requirements and the deterministic, probabilistic and other insights are weighted depends on the particular issue being addressed and on the practice in the Member States. Therefore it is not possible to give definitive guidance on how this should be done.

If there are political or governmental requirements, this will usually be given the highest weight and this would often be the overriding factor in making the decision.

The relative weights given to the deterministic and probabilistic insights vary among the Member States as well as the confidence that the regulatory body has in the PSA. Although a higher weight has traditionally been given to deterministic analysis, the current trend is for

high quality PSAs to be produced and for PSA insights to be used effectively in the regulatory decision making process.

The weight given to the probabilistic analysis will take account of the type of probabilistic input that was provided — that is, whether it is based on a full PSA analysis or whether only less formal risk insights are available. If a full scope PSA has been used, the weight of the PSA insights will further depend on the quality of the analysis carried out. This will also take account of the results of sensitivity studies and uncertainty analysis where these have been carried out.

The weighting would also be expected to take account of the outcome of any cost-benefit analysis that had been carried out. If this has shown that the costs of making the changes are excessive when compared to the benefits that would be obtained, this would lead to a low weighting for the change to be made.

It is clear that the regulatory regimes have developed very differently in the Member States in that some are very prescriptive and others are much more goal setting. In addition, there are significant differences in the way in which safety issues have been resolved. Hence, it is clear that it would not be possible to provide detailed guidance on the weighting factors that are ultimately applicable to all safety issues.

***Step 8: Making the decision***

In making the decision, the regulatory body will need to take account of all the requirements and insights identified from the preceding steps, combine them taking account of the different weights assigned to them and reach a decision on whether the proposed change should be accepted or rejected. However, there is a fundamental difficulty in doing this because the requirements and insights obtained from the preceding steps are not expressed in the same units.

It is good practice for the regulatory body to involve multidisciplinary teams in the decision making process where the members of the team are able to deal with the diverse inputs with different weights. The team normally includes members who can cover all the disciplines involved (that is, transient analysis, radiological analysis, human factors task analysis, severe accident analysis, PSA, etc. as required for the issue being addressed) and are familiar with the plant (which would include the design, operation, operational experience, etc.). The aim of putting together the team is to ensure that all the information relevant to the issue has been generated, made available to all the members of the team, and that its significance and origin are understood.

The inputs provided by the experts in each of the areas would include:

- The methods and data used, and the assumptions made, in carrying out the analysis, identifying also limitations that might impact the use of the results.
- The conclusions drawn from the analysis carried out.
- An understanding of any uncertainties in the analysis and the results of any sensitivity studies that have been carried out.

- The relationship between the input that they are providing and that are being provided by the other experts.

The members of the multidisciplinary team would be expected to have a high level of expertise in at least one of the areas that provide a significant input into the decision making process. They would need to be able to explain their input also to non-specialists. They would also need to have a broad perspective on nuclear safety issues so that they would be able to understand and take account of the inputs being provided by the other experts.

The level of expertise of the members of the multidisciplinary team would need to be consistent with the importance of the decision being made. In the example given in the Appendix, which relates to the issue of whether to make changes to the regulations on combustible gas control for light water reactors, the decision was made by the NRC commissioners. In this case the weightings given by the specialists in individual areas were reconsidered by the multidisciplinary team of senior experts.

If more than one issue arises at the same time, it is recommended that the regulatory body consider them individually and a separate decision made on each of them. If two or more issues are considered together, it is possible that one of the issues may lead to a relatively large increase in the risk, which would be masked by a relatively large decrease in the risk from the others. This needs to be avoided and each of the issues has to be considered on its own. However, if a number of proposals arise within a short period of time to make changes that would lead to the risk being increased, it is advisable that the regulatory body take account of the combined effect of these changes to make sure that this is also acceptable.

***Step 9: Implementation of the change***

After the decision has been taken, the regulatory body will need to agree a programme of work with the plant operators for the implementation of the change to the design or operation of the plant.

***Step 10: Monitoring the change***

After the change in the design or operation of the plant has been made, it is good practice for the regulatory body to monitor the effect of the change. Monitoring needs to be based on measurable parameters with objective criteria defined for the performance required. If these criteria are not met, the cause needs to be determined and corrective actions taken.

## 4.3. Examples of decisions made using an integrated decision making process

### *4.3.1. Increasing the seismic resistance capability*

*Issue:* Many of the older nuclear facilities were built at a time when there was no requirement for the structures, systems and components to be seismically qualified. Hence these older plants have a very limited capability to withstand seismic events and there is a need for improvements. The issue that needed to be addressed by a number of regulatory bodies was to determine which improvements would be reasonably practicable for the plant operators to make.

*Mandatory requirements:* The need to make such changes has arisen in many Member States due to pressure from the government, from international community or from the

regulatory body. The issue has also been identified as a weakness in the Periodic Safety Reviews that have been carried out for the older nuclear facilities.

*Deterministic insights:* The deterministic requirements is that the structures, systems and components that are important to safety should be seismically qualified so that they do not fail following the DBE. The modern standard is that the DBE is an event that has a frequency of exceedance of $10^{-4}$ per year and the magnitude of the event needs to be chosen in a conservative way to take account of the uncertainties. The design requirement is that one line of protection should be available following the DBE to provide the necessary safety functions. In some Member States there is also a requirement that a second line of protection should be available following the Operating Basis Earthquake (OBE), which has a frequency of exceedance of $10^{-2}$ per year.

However, most of the older nuclear power plants fall well short of this requirement and the aim of the seismic analysis was to determine which level of seismic event the plant would be able to withstand and what improvements would be reasonably practicable.

*Probabilistic insights:* The probabilistic requirement is that the contribution to the risk from seismic events should be low (and meet any quantitative risk criteria, if these have been defined). In the absence of seismic PSAs for the majority of the older nuclear power plants, the risk insights have been derived from the seismic analysis using judgements on the potential failure modes, the margins to failure and the likely consequences of failures. Single failures that would lead to core damage/large early release and failures of the reactor shutdown/post trip cooling systems are of particular concern.

*Other factors:* These include the following:

- The **cost** of making the improvements, including the cost of modification itself and the lost revenue during the period when the reactor needed to be shut down.
- The **radiation dose uptake** by the workers in making the improvements.
- The **remaining lifetime** of the plant. Although this was not defined exactly it was likely to be short for some of the older plants.

*Decision made:* In many Member States, the overriding requirement was the political or regulatory pressure to improve the seismic resilience capability of the older plants. The insights from the deterministic, probabilistic and other requirements were used to determine the level of seismic resilience that it would be reasonably practicable to achieve. The way in which this has been done is very specific to individual power plants. However, some of the older plants have been shut down since it was not considered reasonably practicable to make the required improvements.

### *4.3.2. Adding diversified safety systems*

*Issue:* The modern standard is to provide diversity in the safety systems required to perform the safety functions for frequent initiating events. However, for some of the older plants, the level of diversity provided may be lower. Hence, the issue to be addressed by the regulatory body is whether to backfit additional safety systems to the older reactors.

*Mandatory requirements:* The need to make such changes has arisen in many Member States due to pressure from the government, from international pressure or from the regulatory body. The issue has also been identified as a weakness in the Periodic Safety Reviews that have been carried out for the older nuclear facilities.

*Deterministic insights:* The deterministic requirement is that diverse systems should be provided to carry out the safety functions for all frequent initiating events. In one Member State this was specified as initiating events with a frequency greater than $10^{-3}$ per year. A deterministic review was then carried out to identify the initiating events and safety functions where the diversity requirement was not met.

*Probabilistic insights:* From a risk point of view, the PSA has been used as follows:

- To indicate the overall level of risk from the plant. In this case, the CDF was high/near to the maximum acceptable level, which indicated that a high priority needs to be given to reducing risk.

- To determine where the weaknesses were in the design and operation of the plant. High importance values for common cause failure of any of the safety systems pointed out areas where consideration needed to be given to the incorporation of additional diverse systems.

- After a decision that additional diverse systems were needed, the PSA was used to compare the reduction in the risk which the various options for these systems would give.

*Other factors:* As for the example given in Section 4.2.1, the other issues to be addressed in the decision making process were the cost of the improvements, the radiation dose uptake by the workers and the remaining lifetime of the plant.

*Decision made:* In many Member States, the factor that was given the highest weight by the regulatory body was to meet the deterministic requirement. This resulted in a number of diverse systems being added that included reactor shutdown and steam generator feedwater systems. It was deterministically required that these systems needed to be seismically qualified. Updated PSA showed that these improvements led to a large reduction in the risk from the plant.

### *4.3.3. Increasing the reactor power level*

*Issue:* The issue that needed to be addressed was whether the regulatory body would allow the power rating of a nuclear power plant to be increased by 5%.

*Mandatory requirements:* The mandatory requirement is that the plant remains within its licensing basis.

*Deterministic insights:* The deterministic requirement is that adequate safety margins are maintained. The transient analysis demonstrated that, although the safety margins were reduced, there were still acceptable margins available.

*Probabilistic insights:* It was intuitively expected that increasing the reactor power level would increase the CDF and LERF. However, the Level 1 PSA was reviewed and the

conclusion drawn that there were margins in the safety system success criteria used so that they were still valid at the increased power level.

*Other factors:* The other issue was that the increase in the power level of 5% would significantly increase the revenue from the plant. However, this was not taken into account by the regulatory body — that is, it was given a zero weighting in the decision making process.

*Decision made:* The regulatory body agreed that the power level of the reactor could be increased by 5%.

### *4.3.4. Extending test intervals*

*Issue:* The issue to be addressed was whether the regulatory body would allow increasing of the test intervals provided in the plant technical specifications.

*Mandatory requirements:* The mandatory requirement is that the plant Technical Specifications have to be observed.

*Deterministic insights:* From a deterministic point of view, although the technical specifications were considered to reflect the manufacturer's requirements and current best practice, there was no firm justification for the test intervals defined.

*Probabilistic insights:* The existing PSA had been quantified using the test intervals given in the Technical Specifications and the CDF calculated for the plant was acceptably low. The importance functions were used to determine the risk significance of individual components. Sensitivity studies were carried out to determine the change in risk that would arise from reducing the test interval of the components with the greatest risk significance and increasing the test interval of those with the lowest risk significance [16].

In the PSA, the failure probabilities for standby components were calculated using the formula ½•λ•T where λ is the failure rate per unit time and T is the test interval. However, in carrying out the sensitivity studies, it was recognized that this approximation is unlikely to be valid for test intervals that are very much shorter than those given in the technical specifications. Hence, the change in the test interval was restricted to no more than a factor of 2 of the value given in the technical specifications.

*Other factors:* It was recognized that there was a possible economic benefit to the plant operators if fewer tests needed to be carried out. However, this was not taken into account by the regulatory body in reaching its decision.

*Decision made:* As a result of the analysis, the regulatory body agreed that changes could be made to the test intervals. The set of changes made to the technical specifications was risk neutral in that increases in the test intervals for components with a low risk significance were offset by reductions in the risk by shortening the test interval for components with a high risk significance and the changes were restricted such that the new test intervals were increased or decreased by no more than a factor of 2 compared to the original values.

### *4.3.5. Removing one of the inputs to the reactor trip system*

*Issue:* One of the inputs to the reactor trip system was provided by instruments that were located at the top of the reactor core. However, those instruments were very unreliable so that their availability was low. In addition, since they were located in an area where the radiation level was high, there was a large radiation dose burden to workers associated with their repair or replacement. The issue that the regulatory body needed to address was whether this set of instrumentation could be removed.

*Mandatory requirements:* The mandatory requirement is that the plant should remain within its licensing basis.

*Deterministic insights:* From a deterministic point of view, this means removing one of the diverse inputs into the reactor trip system for a group of initiating events. However, the plant operator carried out a transient analysis to demonstrate that there was an alternative parameter already available that would initiate a reactor trip. Although this trip parameter would have led to the reactor being tripped later than for the original one, it could be demonstrated that safety margins would not be significantly reduced.

*Probabilistic insights:* From a PSA point of view, the only change was to the parameter that was claimed to initiate a reactor trip. Although this parameter already provided an input into the reactor trip system, no credit was taken for it in the existing PSA. When the PSA was changed to replace the old unreliable parameter with the alternative, more reliable one, the risk was slightly reduced. However, this is an incorrect insight due to the conservative assumption made in the original PSA, which did not take credit for the second available reactor trip signal. It could be deduced that the removal of one of the redundant reactor trip signals would only lead to a small increase in the risk.

*Other factors:* These include the following:

- The **radiation dose uptake** by the workers would be reduced since there would no longer be a need to carry out work to repair or replace the unreliable instruments in an area with a high level of radiation.

- There will be cost savings since there would be no requirement to carry out the work to maintain these instruments and the cost of amending the safety case documentation.

*Decision made:* As a result of this, the regulatory body agreed that the instruments could be removed.

### *4.3.6. Increasing the length of working shifts*

*Issue:* A request was made to the regulatory body by the operators of a nuclear facility in one Member States for the length of the working shifts to be increased from 8 hours to 12 hours. The view that was taken by the plant operators was that this would give a significant saving in the running costs without reducing the level of safety of the plant.

*Mandatory requirements:* The mandatory requirement was that, as part of the licensing basis for the facility, the operating organization needed to employ a sufficient number of suitably qualified and experienced personnel to ensure safe plant operation and any changes in staffing levels needed to be agreed by the regulatory body.

*Deterministic insights:* There were no other deterministic requirements.

*Probabilistic insights:* Intuitively it would be expected that increasing the length of the working shifts could increase the potential for human errors to occur due to performance shaping factors arising from increased levels of fatigue and this could lead to an increase in the risk. However, since the length of the shifts is not included explicitly in the PSA this issue could not be addressed directly. The approach that was adopted was to carry out sensitivity studies. It was judged that human error probability and some of the initiating event frequencies would be increased by a factor of no more than 2 or 3. Sensitivity studies were carried out, which demonstrated that for this particular plant the increase in the CDF would be relatively small. The reason for this is that a high level of automation is provided that restricts the potential for human errors.

*Other factors:* The other relevant factor was that the change would lead to a significant cost saving to the plant operators However, this factor as not taken into account by the regulatory body in reaching its decision — that is, it was given zero weighting.

*Decision made:* The regulatory body agreed that the change could be made. A programme of regulatory inspections was put in place to monitor the operation of the facility to verify that there was no reduction in the level of safety of the plant.

## 5. 'RISK INFORMING' REGULATORY ACTIVITIES

### 5.1. Overview

This section describes how the integrated decision making process is being applied by regulatory bodies in making decisions on the way in which they carry out their activities. The relevant activities include:

- developing, adopting and updating regulations and guides
- issuing, amending, suspending or revoking authorizations
- carrying out regulatory inspections
- ensuring that corrective actions are taken
- taking enforcement actions when necessary.

All these activities involve judgments by the regulatory body that can benefit from applying an integrated decision making process that explicitly takes any relevant risk information into account.

Risk information can be used to **prioritize** the tasks within an activity, and to **optimize** and enhance tasks themselves.

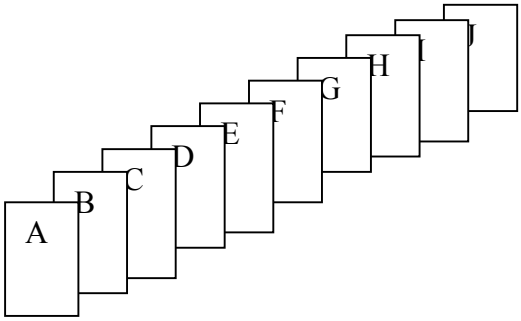
For example, if the activity is updating regulations, risk insights can be used as one of the inputs to **prioritize** the order in which regulations are updated and to **optimize** the way in which this activity is carried out by identifying which aspects of a particular regulation need to be updated. Prioritizing tasks within an activity is briefly discussed in Section 5.2, while the rest of the section deals with applying risk insights to the individual tasks within an activity.

However, it should be noted that it is not practicable to use risk insights to decide which of the activities need to be carried out first, or to rank the activities. For example, it would not be possible to use risk information to determine whether it would be better to revise regulations or to carry out regulatory inspections. However, it would be possible to use risk information as one of the inputs into deciding which regulations should be revised first and how they should be revised, or to determine the priority that should be given to carrying out various regulatory inspections.

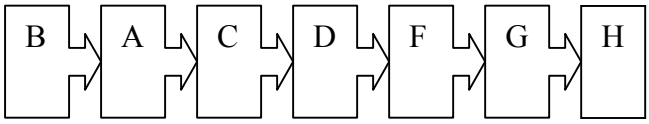
### 5.2. Using risk information to prioritize tasks within a regulatory activity

Risk information can be an essential input to prioritizing the regulatory tasks attached to an activity. The risk significance of a task is an important consideration in assigning its priority. The resources of a regulatory body are always limited and the inclusion of risk information will help to optimize how those resources are spent to maximize the benefit to safety.

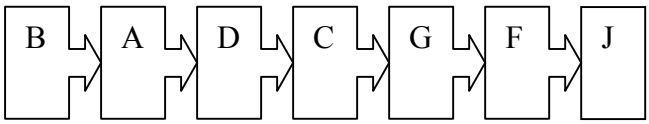
Consider a regulatory activity for which a series of tasks that could potentially be carried out, designated tasks A to J, have been identified:




A prioritization of these tasks based on traditional criteria, such as deterministic safety considerations, resource needs, cost-benefit, and other factors, may result in a priority order as follows:




In this example tasks E, I, and J have been dropped because of their low priority based on the factors considered. Of the tasks remaining, B is of highest priority while H is of lowest priority. When risk insights are added to the factors used for prioritizing the result may change somewhat to the following:




In the most likely case the strictly deterministic prioritization will agree with the risk informed one for the highest priority tasks, as shown in this example. However, the order of carrying out less important but still vital tasks may likely be affected by the risk information as indicated. As also indicated, including the risk information may alter the group of those tasks that are dropped because of resource or time limitations. In the example shown, task H

was of such low risk significance that it was dropped, and the now available time and resources are used for task J instead.

To make this example of prioritizing tasks within an activity less theoretical, consider an activity like updating the regulations. When updating a set of regulations, by 'risk informing' them for instance, establishing the optimum order in which individual regulations are changed calls for a prioritization involving risk insights. Similarly, for the activity of carrying out inspections, when deciding what types of inspections to carry out, and in what order, prioritizing is necessary and risk insights would be an essential part of the prioritization criteria.

### 5.3. 'Risk informing' the regulations

One of the most important responsibilities of a regulatory body is the establishment and updating of regulations and guides that form the basic structure for the regulatory process. Including risk information in the establishment and/or updating of the regulations can be of benefit to both the regulatory body and the plant operators.

If risk information is available and considered at the creation of the set of regulations it would be straightforward to establish a regulatory structure that includes risk considerations in a consistent and coherent way. While such a possibility of a 'clean sheet approach' may exist for establishing a new set of regulations for a new generation of advanced reactors, this is not practical for the operating reactors. The national regulations for nuclear power plants in operation have evolved over the last five decades. While this evolution implicitly took some account of intuitive risk consideration in promulgating deterministic requirements, the bulk of the evolution occurred without the benefit of the insights from the PSA and severe accident research. Therefore, in most Member States the existing regulations governing the design and operation of the current fleet of plants are mainly deterministic in nature, but may contain a few specific regulations that explicitly address concerns identified from risk analyses. The 'risk informing' of the body of such regulations involves very different considerations from those of the 'clean sheet' approach. The discussion that follows focuses on 'risk informing' a set of existing, mainly deterministic, regulations.

#### *5.3.1. Benefits of 'risk informing'*

The first question is: what is the rationale for 'risk informing' the regulations — that is, what benefit can result from such an effort? In the broadest terms, 'risk informing' the regulations is expected to: (1) improve the effectiveness, efficiency and realism in the regulatory body's decision, practices, and processes, (2) increase public confidence, and (3) reduce the unnecessary burden on operators without compromising safety. More specifically, some of the benefits that can be identified are:

- Enhancing safety by focusing the work and the resources of the regulatory body and the operator in areas commensurate with their importance to health and safety.

- Addressing more explicitly the broader set of challenges, as well as their associated uncertainties, identified from risk information.

- Providing the regulatory body with a consistent structure for considering risk information when taking action in regulatory matters.

- In some Member States, providing a consistent way to use risk information as a means to allowing flexibility in the design and operation of the plant that can result in a reduction in the burden without compromising safety.

As an example of the third item above, one can consider the repeated application of the risk informed decision process for dealing with safety issues. Chapter 4 discusses the risked informed process and consideration by the regulatory body of changes to the licensing basis of a specific plant. These changes are considered at the request of the operator or regulator and are likely to involve exemption from a regulation, in whole or in part, or one or more of its associated requirements, based at least to some extent on risk considerations. If such an exemption is more broadly applicable than to a single plant, i.e. if a plant specific issue becomes a generic issue, it may be more effective and efficient for the regulatory body to deal with the issue by modifying, i.e. 'risk informing', the relevant regulation or requirement, rather than dealing with the issue on a plant specific basis.

The approach to 'risk informing' the regulations can take a number of forms, but is generally expected to involve one or more of the following:

- Adding further risk informed requirements to existing regulations.

- Revising part or all of an existing regulation and its associated requirements to reflect risk information, and

- Deleting unnecessary or ineffective parts of regulations or entire regulations.

### *5.3.2. General considerations*

The nature of the 'risk informing' depends on the safety philosophy in a particular Member State. In some Member States, there is a safety policy that allows different approaches to deal with changes in risk depending on the absolute value of the risk (including due considerations of uncertainties). Such a policy is founded on the principle that 'undue' increases in risk are not allowed, but 'insignificant' increases can be tolerated in some cases. If the risk is found to be above a certain upper limit, usually associated with acceptable safety, the risk must be reduced regardless of cost. If the risk is below this limit, however, the safety policy may link risk reduction to cost-benefit considerations. If the risk is substantially below the upper risk limit, then the safety policy may allow slight increases in risk because of economic or other justification. This is the case in the USA, for example, where the guidance in Ref. [3] espouses this philosophy. On the other hand, in some member states the safety policy may not allow any increase in risk, no matter how small. These two differing philosophies will result in very different approaches to 'risk informing' the regulations.

The type and amount of 'risk informing' also depends on the nature of the existing regulations — in particular, whether they are prescriptive or performance based in nature. Performance based regulatory actions aim to accomplish certain objectives by focusing on indicators that show that the desired results have been achieved. Prescriptive regulatory actions provide detailed directions on how the results are to be attained. A hypothetical regulation whose objective is to ensure that a certain diesel generator reliability can provide an illustrative example of the differences in prescriptive and performance based approaches. A prescriptive approach would direct the plant operator to conduct detailed maintenance operations, testing procedures and inspections, carried out at specific time intervals. A

performance based regulation would set a desired objective, such as a diesel reliability of 95 percent, and leave it up to the operator as to how this objective is achieved. The operator would furnish certain performance indicators, i.e. the appropriate testing records, to the regulatory body to confirm the desired reliability has been achieved and is being maintained. Most likely, the operator would also be subject to independent inspections by the regulator. Another example of a performance based principle, which allows the operator flexibility in achieving the objective, is the ALARA/ALARP provision, discussed below. In practice regulations often consist of a combination of prescriptive and performance based elements. This may be due to the lack of practical performance indicators for some objectives, and/or may reflect the regulator's desire to achieve its aims in a more prescriptive manner. By setting the performance goal at the highest level practical, i.e. the most aggregated level of safety significant systems, structures and components that is possible, maximum flexibility is achieved.

Since performance indicators are often risk related metrics, performance based regulations are likely to incorporate some risk elements already. In comparing performance based and prescriptive regulations, prescriptive regulations are likely to be more deterministic, while performance based regulations are likely to be more risk informed. Risk informed and performance based approaches to regulation often complement one another. In the USA, for example, the NRC staff has stated that activities to risk inform the regulations should also, to the extent appropriate, incorporate the performance based approach to regulation, and that performance based regulations should be risk informed whenever possible. In summary, the extent of 'risk informing' that is warranted for a regulation may depend on where the regulation falls in the prescriptive to performance based spectrum. If a whole body of regulations has already incorporated performance based elements to the extent practical, comparatively little 'risk informing' may be called for.

Whatever the approach, it is prudent that any process that is put in place to risk inform a set of existing regulations consider a number of factors to assure adequate protection of public health and safety in the transition from the current regulations to the risk informed regulations.

It is assumed that the existing body of regulations in a Member State provide adequate protection of the public health and safety in that Member State. It is important that risk informed changes to the requirements be carried out in such a way that there is reasonable assurance that an adequate protection is maintained. Therefore the process of 'risk informing' the regulations needs to preserve essential factors included in the deterministic formulation of the regulations. These factors include the fundamental safety principles of defence in depth, safety margins, the ALARA or ALARP principles for radiation protection, and adherence to any safety goals that exist in the Member State. In complementing the risk information, these principles are particularly important to account for the uncertainties that are associated with such direct challenges to plant safety as equipment unreliability, human error and severe accident phenomena, as well as the uncertainties attached to more indirect factors such as the management style and safety culture at the plant. This is really a restatement of the principles that apply to any integrated decision making process, as discussed in Section 3 above.

*Defence in depth*

Defence in depth as defined in Section 2.1 and Ref. [1] is brought into play to ensure public safety given the uncertainty in safety assessments, both deterministic and probabilistic. Defence in depth requires successive compensatory measures to prevent radiation exposure

and to prevent accidents, or to mitigate damage during an accident resulting from equipment failure, human error, or a natural event such as an earthquake. For mechanical systems defence in depth is achieved by redundancy and diversity, as well as separation of preventive and mitigating systems. Similarly, exposure to radiation is limited by shielding, distance and time. When 'risk informing' a regulation or requirement, it is necessary to ensure that:

- the number and nature of physical and functional barriers for ensuring defence in depth are commensurate with the potential risk and the associated uncertainty;
- there is a reasonable balance between accident prevention, accident mitigation, and prevention of exposure to radiation;
- defences against potential common cause failures are preserved and the potential for new common cause failures is assessed;
- the independence of barriers is preserved to the extent possible;
- defences against human errors are preserved;
- other regulations that are interrelated with the regulation being 'risk informed' are not adversely impacted by the potential change.

*Safety margins*

Safety margins are one of the means of achieving defence in depth. Safety margins compensate for uncertainty in analysis and data, and in some cases ensure that adequate time is available to prevent unacceptable consequences. When 'risk informing' a regulation or requirement, it is necessary to ensure that:

- safety margins are still acceptable, given the risk significance of the challenge the regulation/requirement is meant to address, including associated uncertainties; and
- there is a method available for assessing that safety margins are still adequate.

*The ALARA/ALARP principle for radiation protection*

By applying the 'as low as reasonably achievable' or 'as low as reasonably practical' principle to radiation protection, i.e. by using the conservatism of a linear, no-threshold model for radiation damage, the uncertainty of what dose level represents the level at which no adverse health effects occur, is compensated for. When 'risk informing' a regulation or requirement, it is necessary to ensure that either the risk informed change is consistent with the ALARA/ALARP principle, or radiation limits are set in some other acceptable manner.

*Safety goals*

If explicit safety goals exist, conflict between the risk informed regulation/requirement and the safety goal needs to be avoided.

### *5.3.3. Steps in 'risk informing' a set of regulations*

The steps in the process are outlined in Fig. 3.

**Step 1. — Identifying candidates for 'risk informing'**: The objective is to identify which parts of the aggregate set of regulations are candidates for risk informed changes. Such changes may involve modification of individual requirements, or sets of requirements. The identification of those portions of the regulations, that are candidates to be risk informed are likely to be determined based on a number of screening factors, a general understanding of the basis for the current requirements, and criteria for improving the current requirements. Some of the more obvious criteria are (1) the potential for improving safety, (2) the potential for reducing burdens for the operator and/or regulator, and (3) the extent to which risk information can be incorporated in the requirement. The outcome of this step will be a set of regulations that at least have the potential to be risk informed.

**Step 2. — Prioritizing**: In this step, the candidate regulations and the identified requirements from the previous step are prioritized according to a number of factors and associated criteria which will most likely include risk information. Some of the same factors used to identify and screen candidate regulations in the previous step are likely to be used here; however, the criteria for applying the factors will likely differ. For example, in identifying a potential candidate, a criterion would likely be whether improvements were even possible. The prioritization criterion would consider how much improvement might potentially occur. Some of the factors that may be used in the prioritization process are:

- potential for improving safety
- potential for reducing burdens on operator and/or regulator
- the anticipated complexity of changes
- resources needed (by the regulatory body and the plant operators) for putting changes in place
- time needed for full implementation
- application to current and/or future plants
- the scope of the risk assessment that is required
- the extent to which risk information can be incorporated into the requirement
- whether 'risk informing' a candidate requirement would require 'risk informing' other related requirements.

The regulatory body will weight the factors and make a judgment on priorities. Determining how far down the prioritization list candidate changes should be pursued, i.e. whether medium or low prioritized candidates need to be pursued, is important for the efficient use of a regulator's resources.

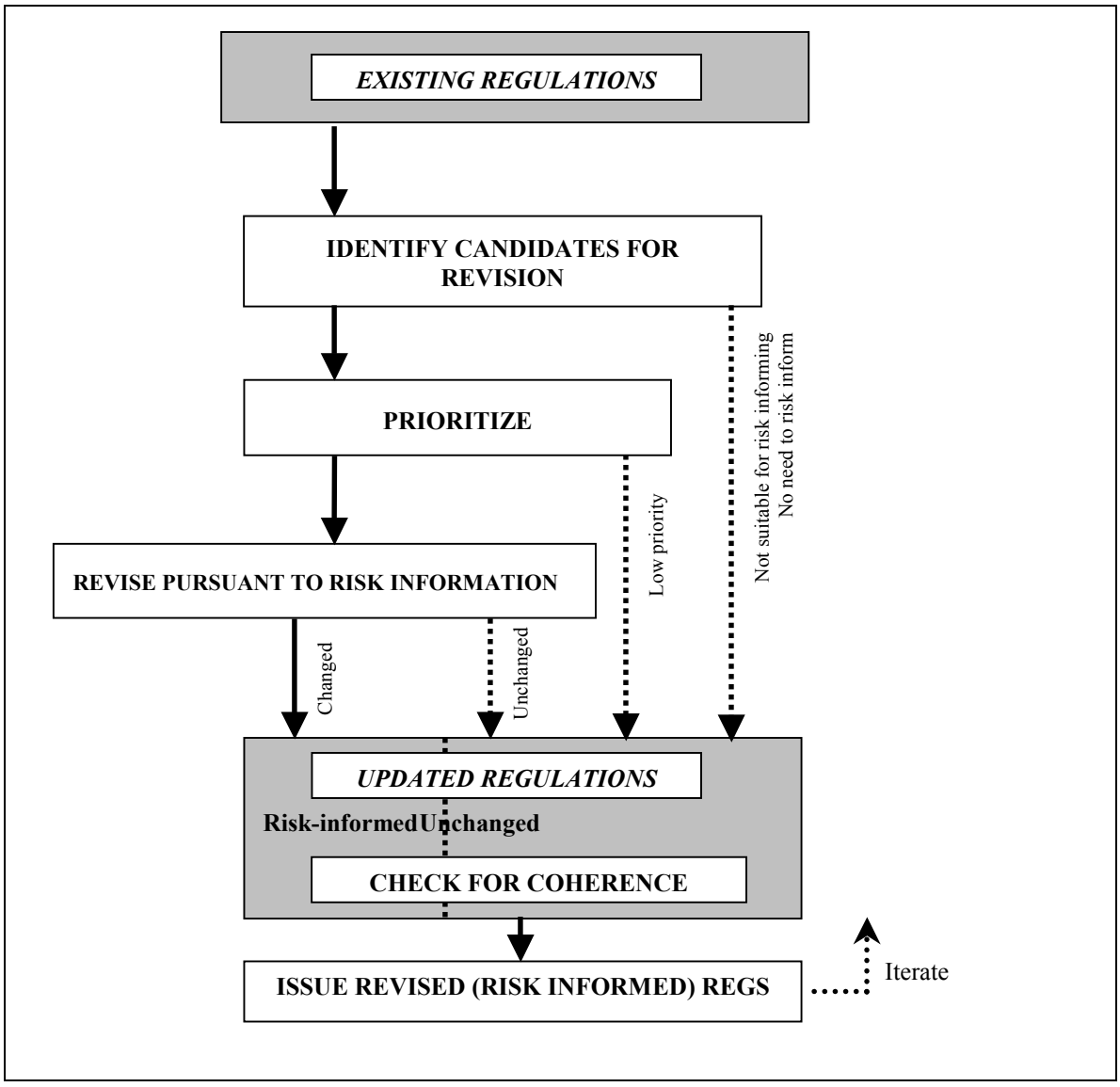



*FIG. 3. Process of 'risk informing' the regulations.*

This second step can be thought of as an example of the process described in Section 5.2 above, with tasks A through J in 5.2 representing ten tasks associated with 'risk informing' ten individual regulations.

**Step 3. — 'Risk inform'**: The aim is to carry out risk informed changes to individual (or a group of related) regulations. This step broadly incorporates within it the steps of the integrated decision making process discussed in Section 3 and which are shown in Fig. 1. The application of the process to a regulation is discussed in some detail in Section 5.3.4 below, but here it is important to note that, as part of the process, options to change each of the candidate requirements will likely be identified and evaluated for those regulations and requirements that have been identified as high priority in the previous step. Specific options with respect to possible changes are likely to include one or more of the following:

- changes in the design basis accident description (i.e. a risk informed design basis);
- changes in the acceptance criteria (peak clad temperature, oxidation limits, etc.) based on new engineering information;
- changes in the method and assumptions for demonstrating compliance with the acceptance criteria;
- changes in systems, structures and components subject to technical requirements, as well as changes to the technical requirements themselves.

If more than one option is identified for 'risk informing' an individual requirement the decision makers in the regulatory body will then select the option best suited to their aims and policies.

**Step 4. — Checking for coherence**: The final step when undertaking the 'risk informing' of the set of existing regulations is to check whether the resulting body of regulations is coherent and consistent. As Fig. 3 indicates, there are a number of reasons why many regulations will not be changed in the process. Therefore the final result can be expected to be a mixture of regulations consisting of:

- those that are unchanged because they do not lend themselves to 'risk informing';
- those that are unchanged because, while they could be risk informed in principle, are too low in priority (i.e. if benefit to safety, or unnecessary burden reduction are not significant) to justify 'risk informing';
- those that have been changed by the 'risk informing' process.

It is recommended that such a mixture be checked for discrepancies, inconsistencies, variations and irregularities and that any problems identified be corrected.

The overall process is likely to be highly iterative. An initial group of requirements that are obvious candidates for 'risk informing' are identified first, then after additional evaluation of the candidate group of requirements, the list is modified.

The approach described above is similar to that proposed in the USA for 'risk informing' Part 50 of Title 10 of the US Code of Federal Regulations, the part of the code that governs the licensing and operation of commercial nuclear power plants [9].

### *5.3.4. Steps for 'risk informing' an individual regulation*

The impetus to change a regulation may come form the regulatory body or from the plant operator. The desire to change regulations due to safety concerns based on new risk information are likely to come from the regulator, but could also be prompted by concerns first identified by the operator. The desire to change a regulation, because risk insights indicate it is too restrictive without substantially adding to safety, is likely to come from the operator. In either case, the steps to be followed by the regulator in the process of 'risk informing' an individual regulation are analogous to those shown in Fig. 2 for the integrated decision making process. These steps are the following:

***Step1: What is the safety concern and how well is it addressed by the regulation?***

In Fig. 2, the first step is defining the issue. Here, with a regulation that has been selected for 'risk informing', the issue is how well does the regulation meet the safety challenges it is meant to address and how can it be improved. This involves clearly defining the safety concern and determining its significance. Some of this information will likely have been identified already during the screening/prioritization process described earlier.

***Step 2: Identifying the applicable high level requirements and criteria***

Since here the process involves changes to the regulations themselves, this step is somewhat different from that in Fig. 2. The need is to identify the high level requirements and criteria, such as safety goals or other overarching principles that continue to form the foundation of the nuclear safety policy of a Member State. These high level requirements can include mandatory, deterministic, probabilistic and other requirements and factors, and will generally be different in the Member States, depending on the style of regulation that is followed.

*Step 2a: Identifying the high level mandatory requirements*

As noted in Chapter 3, there may be a number of very detailed legal requirements/regulations/guidance that would need to be identified and addressed. However, this would probably not be the case where the regulatory regime is non-prescriptive and there are several ways to achieve the overall safety goals. An example is the ALARA/ALARP requirement used in many Member States to ensure that the risk is reduced to a level that is as low as reasonably practicable. In many Member States the test of "reasonable practicability" is to show that the costs of making the change are not excessive when compared to the benefits that would be obtained. This is often addressed formally by carrying out a cost-benefit analysis.

*Step 2b: Identifying the applicable high level deterministic requirements*

The higher level requirements of the defence in depth, the multi-barrier concept and sufficient safety margins are likely to be part of high level deterministic requirements. This may include general requirements related to the levels of redundancy, diversity, separation, segregation, equipment qualification, etc. required for safety systems, and other operational restrictions.

*Step 2c: Identifying the applicable high level probabilistic requirements*

High level risk criteria, in terms of qualitative and/or quantitative safety goals for instance, have been defined in some Member States. In some cases these high level requirements are developed further for nuclear power plants, in the form of surrogate metrics, usually related to CDF and LERF. However, in many Member States, no such formal risk criteria have been defined. In addition, high level criteria may exist that would define whether risk increases are allowed, and if so, the magnitude of the allowable increase.

*Step 2d: Identifying any other applicable requirements or factors*

Other factors such as costs to licensees, burden on regulators, worker dose, public perception, utility pressure and international standards would be relevant here.

***Step 3: Determining the technical basis of the current regulation and its requirements***

Again, because the process involves changes to the regulations themselves, this step is somewhat different from that illustrated in Fig. 2. The step involves a review of the technical bases for the current requirements of the regulation and their related material, and how these requirements relate to the technical concern the regulation is meant to address. The review also considers the interrelationships and linkages among the requirements contained in the regulation, how defence in depth and safety margins are applied across requirements, and such factors as the balance between accident prevention and mitigation. Factors the review will likely consider are:

- the safety function intended to be addressed by the requirement;
- the analysis methods, assumptions and acceptance criteria used, including their degree of conservatism;
- the technical bases for each requirement;
- the reasons why the requirement is or is not effective in addressing the safety concern.

The review here will be closely linked to Step 1 which identified the safety concern being addressed and how well it is being addressed. This is also the step where the impact of mandatory requirements identified in Step 2a is assessed.

***Step 4: Identifying and assessing the deterministic insights***

In this step, deterministic insights related to the concern are assembled. This includes insights, which may have formed the technical bases for the regulation, already identified in Step 3, as well as requirements identified in 2b, and any new deterministic insights acquired since the formulation of the current regulation.

***Step 5: Identifying and assessing the probabilistic insights***

In this step the probabilistic requirements from Step 2c are considered, and other probabilistic insights related to the concern are gathered and reviewed. Often these can be obtained from a formal risk analysis/PSA and this would be the most desirable source. But less formal probabilistic input, including qualitative information can be also helpful. The uncertainty associated with the probabilistic information needs to be recognized. Ideally, an uncertainty analysis would be included with the PSA information, but if this is not the case some consideration of uncertainty have to be included. The caveats regarding PSA, pointed out in Chapter 3, apply here as well, i.e. there may be limitations to the PSA, so that not all required information can be obtained, because of limits in the scope of the PSA or the inability to address some issues such as component ageing and safety culture.

***Step 6: Identifying and assessing the insights from the other relevant factors***

Information and insights from Step 2d are assessed in this step. This would include, for example, economic burdens imposed by the existing regulations, as well as the costs, efforts and delays resulting from changing the current regulation. It could also include more intangible factors, such as the impact on the public perception of safety a change in the regulation may have.

***Step 7: Weighting the inputs from the insights obtained***

In this step, a weight is attached to each of the inputs gathered from the insights of Steps 3 to 6. This weighting process could be carried out quantitatively or could be done qualitatively. As in Chapter 3, if the deterministic and probabilistic insights are in agreement, the relative weighting of the deterministic and probabilistic insights is not important. If the deterministic and probabilistic insights are not in agreement, it is often the case that the greater weight is given to the one that indicates that there is a need to make an improvement. Again it is important to point out that there are likely to be differences in the weights that are applied in the Member States. For example, for some regulatory bodies, those insights that would indicate an increase in risk would not be allowed.

***Step 8: Formulating candidate changes to the regulation and submitting them to decision makers for acceptance or rejection***

The initial identification of candidate changes to the regulations will likely be based on the risk considerations of the challenge which the regulation is meant to address. Included are judgments regarding the potential safety benefit, and in some cases the excessive conservatism of the existing regulation. Such considerations could include the frequency and risk significance of the initiating event, the event scenario, and an evaluation of the extent of conservatism in the requirements. Proposed changes aimed at incorporating risk information need to address not only risk. but also defence in depth, safety margins and, in some cases, cost-benefit considerations.

Next, the candidate changes along with their rationale, including the reason for the weights attached to the various insights from Steps 3 to 6, will likely be presented to the decision makers for acceptance or rejection of the proposed change. The decision makers are expected to be a different group from the formulators of the candidate changes, although some overlap may occur. The decision makers may want to revisit Step 7 and assign their own weighting factors before combining the weights and reaching a decision. As noted in Section 3 for the standard integrated decision making, here also it is desirable that the multidisciplinary team that makes the decision includes experts with experience in a range of disciplines such as operations, maintenance, engineering, safety analysis, licensing and PSA, to ensure that sound decisions are made. It is also desirable that the team include individuals with a background in the safety philosophy followed in the Member State.

As shown in Fig. 2, Steps 1 through 8 are likely to be part of an iterative loop where some of the candidate changes are rejected, and the steps revisited to produce modified candidates until a candidate change is found acceptable or until reasonable options have been exhausted.

***Step 9: Implementing the change***

Once the decision makers have made a choice and accepted a risk informed change to the current regulation, the implementation phase can begin, starting with the formal writing of the revised regulation. Some of the considerations during the implementation phase are:

- whether the risk informed regulation replaces the old regulations or represents a voluntary alternative;

- if a voluntary alternative has been chosen, whether selective implementation of changed requirements should be allowed;

- what the resource implications for implementation are.

***Step 10: Monitoring the change***

The consequences of any risk informed changes may need to be monitored, and feedback provided on their effectiveness. Such monitoring could be performance based. Monitoring can also be used to check on the coherence of the revised regulation with the rest of the regulations.

An example of the process described in Steps 1 through 10 above is provided in the Appendix, where the NRC experience in 'risk informing' the regulation addressing combustible gas control in the containment (10 CFR 50.44) is described.

## 5.4. 'Risk informing' other regulatory activities

### *5.4.1. Issuing, amending, suspending or revoking authorizations*

Risk information, often in the form of a PSA, provides useful insights into the safety significance of items requiring authorizations for a nuclear power plant. It is a useful contributor to the prioritization, urgency, frequency of renewal, amending, suspending or revoking such authorizations. Risk information can provide valuable arguments for justification of continued plant operation, which may influence authorization matters.

The types and number of authorizations issued for a particular facility vary among Member States. Some states may issue only one authorization followed by various amendments, additions and modifications, while others issue individual authorizations at a number of points during the life of the plant, such as site approval, construction, commissioning, and operation of the plant, including return to operation after an outage. In a number of Member States a PSA is now required for licensing the plant, thus incorporating risk information into the authorization process. If an unscheduled plant shutdown occurred as a result of a safety concern, it is very likely that a risk assessment would be required prior to restart authorization. Operator requests for changes in technical specifications based on risk considerations, such as increased allowed outage times for certain safety related equipment, are another example of where risk information can play a role in amending an authorization.

### *5.4.2. Carrying out regulatory inspections*

Risk information is an obvious input to focus the emphasis of regulatory inspections on the most safety significant aspects of a plant, thereby optimizing the resources needed for the inspections. By using a risk informed approach in selecting areas for inspection, the potential risk posed by the targeted area is included as one of the inspection criteria, along with the usual criteria based on regulatory requirements and operational experience. By including risk significance as a criterion, the inspection will be focused on activities and systems, structures, and components (SSCs) that are 'risk significant' — that is, that have the potential to initiate an accident, as well as the potential to mitigate or increase the effects and consequences of an accident. This includes inspections carried out by the regulatory body itself, as well as inspections carried out by the plant operator to satisfy regulatory requirements.

If performance based regulations have been established then regulatory inspection programmes are also used to verify the accuracy of an operator's reports on performance indicators. Since performance indicators often incorporate risk information already, these inspections implicitly have a risk informed component.

Besides aiding in the selection of inspection targets, risk information can also be an important input for determining the significance of a particular inspection finding. Time and resources spent by a regulator on violation findings that are determined to be of low risk significance may detract from the review of issues of potentially higher risk. Processing a large number of findings with low safety significance may impose an unnecessary burden on the regulator as well as the plant operator.

The NRC's reactor oversight process is an example where risk informed inspection, along with risk informed performance monitoring and assessment, is used to track the safety performance of nuclear power plants. Operators provide performance indicator reports that are reviewed by NRC inspectors who assess violations. The NRC also carries out independent inspections, sometimes resulting in violation reports. Violations are colour-coded based on indicators of risk. 'Green' is least risk significant while 'Red' is the most risk significant, and "…indicates a significant reduction in safety margin in the area measured by that performance indicator". Plant events or conditions categorized as Green are estimated to represent increases in CDF less than or equal to $1 \times 10^{-6}$ per year and are thus considered to be of very low safety significance. A relatively large number of Green findings are regularly reported and a small number of regulations, related to quality assurance (QA) and procedural issues, account for the majority of the violations. At least on the surface, it appears that the regulations in question do not have great risk significance, and may be candidates for 'risk informing'. However, other potential implications must also be considered. For example, a safety conscious culture at a power plant is crucial, and it may very well be that QA and procedural issues, while not directly important from the point of view of contribution to risk measures, may have a cross-cutting importance from the point of view of creating the desired safety culture at the plant that provides a benefit to all plant activities.

### *5.4.3. Corrective and enforcement actions*

Risk information can be a useful input for a regulatory body to determine whether corrective and enforcement actions that are proposed or implemented need to be taken and are adequate to address the concern identified.

Risk information can help the regulatory body determine the significance of specific violations and therefore provide a means of prioritizing enforcement actions, as well as a means of making the actions, including penalties imposed, commensurate with the seriousness of the violation. A measure of the risk significance of a violation can assist a regulator in determining the urgency for corrective action, the appropriate level of the corrective action, and the need to disseminate information of the violation, and corrective action taken, to a wider audience, including the general public. For example, a violation with low safety significance may initially be only discussed in an inspection report, without any formal enforcement action taken, while a violation with higher safety significance may result in a formal notice of violation to the operator.

Information on the risk significance of the violations observed may in some instances also lead to additional actions by the regulator. For instance, if repeated violations of the same

requirement are found to have high safety significance, the regulator's attention will be more swiftly focussed on trying to find the root cause of the violations and on providing guidance for avoiding future violations. On the other hand, if repeated violations of the same requirement are found to have low safety significance, the regulator may wish to examine the requirement in question further to determine the role it plays in enhancing the safety of the plant, and whether it should be modified or dropped.

A regulatory body may also use risk information to choose not to enforce certain operational limits and conditions or other licensing conditions. This could be the case where strict compliance with the technical specifications may call for a test or for system alignments inappropriate with current plant conditions. Under such circumstances the plant operator may requests a temporary exemption from the usual limiting conditions for operation. Such a request is likely to include risk information as part of the justification.

# APPENDIX

## NRC PROCESS FOR RISK INFORMING THE REGULATION FOR COMBUSTIBLE GAS CONTROL (10 CFR PART 50.44)

This appendix presents an example of the considerations and steps that need to be taken for applying 'risk informing' to a regulation. It is based on the work carried out by the NRC on the regulation given in 10 CFR 50.44 which relates to the standards for the combustible gas control system in light water cooled power reactors [17].

Section I.1 describes the regulation. Section I.2 explains why the regulation was considered to be a candidate for applying the risk informed approach. Section I.3 then describes the tasks and steps carried out. An example of the process is described in Sections 3 and 5.

### I.1. THE REGULATION

The standards for combustible gas control system in light water cooled reactors (LWR) given in Part 50.44 were produced in 1978 to provide a means for the control of hydrogen gas that could be evolved following a design basis loss of coolant accident (LOCA) and reduce the risk of hydrogen combustion that could threaten the integrity of the containment. Further requirements were added following the Three Mile Island Unit 2 (TMI-2) accident to reduce the risk of hydrogen combustion from degraded core accidents in the smaller volume containments. One amendment was incorporated into the rule in 1981 and the other in 1985.

The original 1978 rule requires each LWR fuelled with oxide pellets encased within zircaloy cladding to have a means for controlling hydrogen gas generated following a postulated LOCA. The hydrogen gas could be generated by: (1) metal-water reaction between the zirconium cladding and the reactor coolant, (2) radiolytic decomposition of the coolant, and (3) corrosion of metals.

In controlling the generated gas, each boiling or pressurized LWR is required to have a capability for:

- Measuring the concentration of hydrogen in the containment.
- Ensuring a mixed atmosphere in the containment.
- Controlling combustible gas concentrations in containment following a postulated LOCA.

In addition, for each boiling water reactor (BWR) or pressurized water reactor (PWR), it must be shown, during the time period following a postulated LOCA but prior to effective operation of the combustible gas control system, that either:

- an uncontrolled hydrogen-oxygen recombination would not occur within the containment; or
- the plant could withstand the consequences of an uncontrolled recombination without loss of safety function.

If these two conditions cannot be fulfilled then the containment shall be provided with an inerted (oxygen deficient) atmosphere to provide protection against hydrogen burning and explosion during the time period specified above.

To meet this requirement, operators in the USA used hydrogen re-combiners and/or vent-purge systems in their plants.

After an initial study of the TMI-2 accident, the NRC added the following requirements to the rule in 1981:

- An inerted atmosphere for Mark I and Mark II containments.
- Installation of recombiners for LWRs that rely on a purge or repressurization system as a primary means of controlling combustible gases following a LOCA.
- Installation of high point vents.

After further study and analysis in 1985, the NRC added another amendment that required a hydrogen control system for BWRs with Mark III containments and PWRs with ice condenser containments, justified by a suitable programme of experiments and analysis:

- Mark III and ice condenser plants that do not rely on inerting must have systems and components to establish and maintain safe shutdown and containment integrity and these systems must be able to function in an environment after burning and, possibly, detonation of hydrogen unless it is shown that such events are unlikely to occur.
- The amount of hydrogen to be considered is that generated from an equivalent 75% metal-water reaction.

## I.2. IDENTIFYING THE 10 CFR 50.44 AS A CANDIDATE FOR 'RISK INFORMING'

This regulation was selected as a test case for 'risk informing' by the NRC for a number of reasons. This was prompted in part by the fact that a number of licensees of commercial nuclear power plants in the USA have identified this as a regulation which includes requirements that may not be risk significant, and whose implementation therefore places unnecessary burden on the licensees. A public workshop held in 1999 that was sponsored by the NRC focused on the identification of candidate requirements and design basis accidents to be revised, particularly on the selection of top candidate(s) for risk informing. Several participants expressed views that this regulation should be such a candidate for 'risk informing' as some of the requirements of the current regulation do not contribute to risk reduction and cause unnecessary burden.

This regulation was also the subject of an exemption request from a US licensee, Southern California Edison that operates the San Onofre Nuclear Generating Station (SONGS), which has a PWR with a large dry containment. Specifically, SONGS requested an exemption from this regulation to remove requirements for hydrogen control systems in accordance with the pilot programme for risk informed, performance based regulation. The petition was granted by the NRC, and the NRC staff recognized that the basis for the exemption was not SONGS specific, but was applicable on a wider, generic basis. In accordance with NRC guidance, rulemaking should be used to avoid numerous exemption requests.

This regulation also becomes a viable candidate for 'risk informing' when the selection applicable to screening candidate regulations are applied — see Step 1 in Section 5.3.3:

1. Does the regulation affect accident prevention and mitigation?

2. Does the regulation address the safety issue of concern most efficiently or effectively, or are there:

   a. Risk significant accidents that are not addressed? and/or

   b. Excessive unnecessary burdens imposed?

3. Is the regulation directly linked with other regulations?

With regard to Item 1, the ability to control combustible gases is directly tied to the defence in depth concept of accident prevention and mitigation. Specifically, hydrogen combustion is a direct threat to the containment integrity (that is, its ability to mitigate an accident), but could also be minimized by preventive strategies.

With respect to Item 2, this regulation warrants 'risk informing' since, when examining current requirements, certain parts of it appear to be designed to mitigate accidents that are not risk significant, and consequently, appear to impose unnecessary burden. For instance, it is likely that the removal of some aspects of the hydrogen control systems for LOCA, or a reduction of their surveillance and maintenance requirements would be cost beneficial. In addition, there appear to be risk significant accidents that the current requirements do not address. As a matter of fact, risk studies indicated that station blackout accidents could be significant contributors to risk in most nuclear power plants, including PWR plants with ice condenser containments and BWR plants with Mark III containments. The hydrogen control systems in these two containment types are not operational under station blackout conditions and concerns had been raised that the parts of the regulation dealing with these containment types should be revisited.

## I.3. STEPS FOR 'RISK INFORMING' THE REGULATION

***Step1: What is the safety concern and how well is it addressed by the regulation?***

The safety concern addressed by the regulation is the potential for loss of containment integrity posed by hydrogen combustion. Originally the concern was with the small amounts of hydrogen evolved during a LOCA, but after the TMI-2 accident the concern shifted to the larger amounts of hydrogen that could be generated during a core damage accident. The current existing regulation addressed these concerns via the following requirements:

- Providing monitors to measure hydrogen concentrations in all containment types.
- Ensuring a mixed containment atmosphere in all containment types.
- Controlling post design basis LOCA combustible gases in all containment types.
- Installing high elevation vents in the reactor coolant system (RCS) of all reactors.

- Inerting the containment atmospheres of BWR Mark I and BWR Mark II containments; and

- Providing a hydrogen control system for BWR Mark III and PWR ice condenser containments capable of mitigating the hydrogen generated from a 75% metal-water reaction.

Risk studies indicated that it would be reasonable to revisit the basis for the third and sixth requirement above, as discussed in more detail in Steps 4 and 5 below.

***Step 2: Identifying the applicable high level requirements and criteria***

To ensure that high level safety goals and criteria are considered when conducting the risk informing process, the NRC established a risk informed framework, or regulatory structure, that provides both qualitative and quantitative criteria that need to be adhered to when carrying out the process.

The structure and elements of the framework are consistent with NRC's established regulatory philosophy and have as a high level goal the protection of the public health and safety. A balanced high level defence in depth approach (based on prevention and mitigation) is included in the framework to help achieve this goal. Defence in depth considerations are included in the framework by applying the following strategies:

- limiting the frequency of accident initiating events (initiators);

- limiting the probability of core damage given accident initiation;

- limiting radio-nuclide releases during core damage accidents;

- limiting public health effects due to core damage accident.

The strategies are applied in a risk informed manner so that:

- Reasonable balance is provided among the strategies.

- Over-reliance on administrative measures to compensate for weaknesses in plant design is avoided.

- Safety function success probabilities commensurate with accident frequencies, consequences, and uncertainties are achieved via appropriate:

  – redundancy, independence, and diversity;

  – defences against common cause failure mechanisms;

  – defences against human errors;

  – safety margins.

- The intent of the General Design Criteria (GDCs) is maintained — see Ref. [18].

***Step 3: Determining the technical basis of the current regulation and its requirements***

The technical basis for the existing rule is given in Section I.1. Following the TMI-2 accident, the NRC re-evaluated the adequacy of the regulations related to combustible gas control. Significant quantities of hydrogen from the metal-water reaction, estimated at approximately 400 kg, were generated during the core melt accident at TMI-2 on March 28, 1979, and combustion of the hydrogen released to containment generated a pressure spike of about 3 atmospheres. The accident pressure spike did not pose a threat to the TMI-2 containment. However, the occurrence of the extensive metal-water reaction and subsequent hydrogen burn in the TMI-2 accident gave impetus to the imposition of additional hydrogen control requirements that included additional hardware backfits to the small volume pressure suppression containments, such as the BWRs and the PWRs with ice condensers. New requirements were also imposed as part of 10 CFR 50.44 that required installation of high point vents in the reactor coolant system (RCS) of all plants to allow venting of non-condensable gases. This led to two amendments being made to the regulation also described in Section I.1.

A feasibility study was conducted to determine the technical basis of the requirements and their risk significance. The observations that were derived are listed under Steps 4 and 5 below.

***Step 4: Identifying and assessing the deterministic insights***

Regarding hydrogen monitors to measure the concentration of hydrogen in the containment, the feasibility study found that they are needed for a beyond design basis accident to assess the degree of core damage and confirm that random or deliberate ignition has taken place and that containment integrity is not threatened by an explosive mixture. If an explosive mixture that could threaten containment integrity exists during a beyond design basis accident, then other severe accident management strategies, such as purging and/or venting, would need to be considered. The hydrogen monitors are needed to implement these severe accident management strategies. For BWR Mark I, II and III containments, the monitoring of hydrogen is used extensively in the emergency procedure guidelines/severe accident guidelines. Therefore hydrogen monitoring of the containment atmosphere is needed in all plants for beyond design basis combustible gas control and severe accident management. However, the hydrogen monitors need not be classified as safety related components since (see below) they are no longer needed for the design basis LOCA hydrogen release, but rather to diagnose the course of beyond design basis accidents.

A mixed containment atmosphere was also found to be important, because this requirement is considered a significant defence in depth element, in line with meeting the intent of one of the important GDC — see Ref. [18]. A mixed atmosphere will prevent local accumulation of combustible or detonable gases that could threaten containment integrity or equipment operating in a local compartment. This requirement ensures that features that promote atmospheric mixing, either active systems and/or containment internal structures, that have design features that promote the free circulation of the containment atmosphere, are provided. Risk studies performed as part of the NRC's Individual Plant Examination programme show that a well-mixed atmosphere is highly likely due to the availability of active mixing systems, such as containment sprays and fan coolers.

The feasibility study also found that the design basis LOCA hydrogen release did not contribute to the likelihood of a large release (within approximately 24 hours after the onset of core damage). The re-combiners and/or vent and purge systems required by the original Part 50.44 were intended to address the limited quantity and rate of hydrogen generation that was postulated from a design basis LOCA. This hydrogen release was found to be not risk significant. In addition, these installed systems were found to be ineffective at mitigating hydrogen releases from those risk significant accident sequences that could threaten containment integrity. For BWR Mark I and Mark II containments, the feasibility study also noted that the possibility exists for oxygen generation, and therefore, a combustion challenge to containment integrity in the long term (that is, after several days) needed to be considered during implementation of accident management strategies.

The feasibility study examined the requirement to install high point vents, imposed to permit venting of non-condensable gases from the RCS that may interfere with the natural circulation pattern. This is regarded as an important safety feature in accident sequences that credit natural circulation of the reactor coolant system. In other sequences, the pockets of non-condensable gases may interfere with pump operation. The high point vents could be instrumental for terminating a core damage accident if emergency core cooling system (ECCS) operation is restored. Under these circumstances, venting non-condensable gases from the vessel allows emergency core cooling flow to reach the damaged reactor core and thus prevent further accident progression. However, since these issues are not directly related to containment performance but rather to ECCS performance, this requirement might be relocated to another regulation.

***Step 5: Identifying and assessing the probabilistic insights***

The feasibility study found the requirement to inert BWR Mark I and II type of containments to be risk significant. Removal of this requirement would result in the integrity of these containments being highly vulnerable to hydrogen combustion and, therefore, the existing requirement is risk significant to public health and safety. Given the potentially large concentration of hydrogen that a severe core damage accident could cause in these types of containments, due to their relatively small volume and large zirconium inventory, the likelihood of containment failure from hydrogen combustion would be very high if the containment were not inerted.

Finally, the hydrogen control system required in BWRs with Mark III containments and PWRs with ice condenser containments was also found to be risk significant to public health and safety in the feasibility study. This is because a beyond design basis accident generating significant amounts of hydrogen (on the order of the TMI-2 accident) would pose a severe threat to the integrity of these containment types in the absence of the installed igniters. When igniter systems are available and operable, the feasibility study found that hydrogen combustion is not risk significant. When igniters were inoperable, as during station blackout (SBO) sequences, the calculated mean risk based on an aggregate of existing was within acceptable levels. However, the existing studies also indicated a wide range of uncertainty in the risk under these circumstances, including one study where the $95^{th}$ percentile of the uncertainty distribution estimated the probability of containment failure to be close to unity without igniters. Based on the uncertainty involved, the feasibility study found that the need for combustible gas control during station blackout sequences in these two containment types, when the igniter systems are not operable, should be investigated further.

***Step 6: Identifying and assessing the insights from the other relevant factors***

A number of licensees of commercial nuclear power plants in the USA identified this as a regulation, which includes requirements that may not be risk significant, and whose implementation therefore places unnecessary burden on the licensees.

Factors attached to changes in the regulation such as cost and effort and time constraints on the regulators and licensees were also included here.

***Step 7: Weighting the inputs from the insights obtained***

In the process of 'risk informing' the regulation, no formal weighting factors were used. The insights were not presented to the NRC with weighting factors attached, but in reaching their decision on rejecting and accepting different proposed options (see Step 8 below) the commissioners likely weighed certain factors more heavily than others.

***Step 8: Formulate candidate changes to the regulation and submit to decision makers for acceptance or rejection***

NRC's process for applying risk information to a regulation recommends that two approaches be followed for developing risk informed options. Both approaches begin with an examination of the concerns that necessitated the regulation, and both approaches have the same overall objective, which is to develop risk informed options for dealing with the identified concern. However, one approach starts from the current set of requirements that address the concern and attempts to develop risk informed options by analysing these requirements. The second approach considers the development of alternative risk informed options for addressing the concern by applying the high level defence in depth strategies (as incorporated in the framework discussed above); in effect, ignoring the existing body of regulations.

There are two principal reasons for following two approaches to developing risk informed options to a regulation. The first reason is for completeness. Following both of the above approaches gives greater confidence that all reasonable risk informed options have been identified. The second reason is to identify a risk informed alternative that is the most optimal by looking at the concern from an alternative perspective — that is, without being constrained, or unduly influenced, by the existing requirements.

Application of the first method led to the following suggested changes to the existing requirements:

- Given the need for the capability of establishing hydrogen concentration levels under degraded core conditions, for long term accident management, revising hydrogen measurement related regulations to remove continuous measuring and safety grade requirements, and instead call for an increased measurement range.

- Making no change to the requirement for ensuring a mixed containment atmosphere.

- Eliminating the requirements for combustible gas control systems following a postulated LOCA from the regulations.

- Making no change to the existing requirement of the high point vents and to the related regulations. (This requirement could be moved elsewhere in the regulations).

- Retaining an inerted containment for BWR Mark I and Mark II plants; or

- Retaining the existing combustible gas control requirements for BWR Mark III and PWR ice condenser containments, and perhaps modify them to ensure combustible gas control during all risk significant accidents (for example, for station blackout sequences).

A second method was derived from the defence in depth strategies contained in the framework document for 'risk informing' the regulation. The proposed change would be to replace the current regulation with a regulation that provides for specific mitigative and preventive goals based on the defence in depth strategies that, if met, would address the combustible gas concern. Licensees would be asked to demonstrate that:

- any risk significant core damage accident does not result in an unacceptable conditional large early release probability and conditional large late release probability as a result of combustible gases, if this cannot be shown, then demonstrate that;

- any risk significant core damage accident does not result in an unacceptable large early release frequency and large late release frequency from combustible gases, if this cannot be shown, then demonstrate that

- adequate emergency preparedness is in place for each core damage accident class for which the above criteria are not met;

- the specific means of demonstrating that the goals are met would be outlined in a Regulatory Guide and would be consistent with the framework guidelines.

After evaluating these alternatives, and after the NRC directed the NRC staff to proceed expeditiously with rulemaking, the NRC staff recommended a revised approach to the rulemaking effort. The rulemaking approach recommended involved a rebaselining revision of the existing regulations rather than development of a voluntary alternative approach to rulemaking. The NRC Commission directed the NRC staff to proceed with the rebaselining revision to the regulation.

The rebaselining revision would retain the current requirements for ensuring a mixed atmosphere, inerting BWR Mark I and II containments, and providing hydrogen control systems capable of accommodating an amount of hydrogen generated from a metal-water reaction involving 75% of the fuel cladding surrounding the active fuel region in BWR, Mark III and PWR ice condenser containments.

The revision would eliminate the design basis LOCA hydrogen release from the regulation, and would consolidate the requirements for hydrogen and oxygen monitoring to the regulation, while relaxing safety classifications and licensee commitments to certain design and qualification criteria.

The proposed revision would relocate, without change, the high point vent requirements from 10 CFR 50.44 to 10 CFR 50.46. In addition, the hydrogen control requirements in 10 CFR 50.34(f), applicable for future license applicants, would be relocated to 10 CFR 50.44.

The NRC staff also informed the Commission that a Generic Issue had been established to assess the costs and benefits of possible additional hydrogen control requirements for BWR Mark III and PWR ice condenser containment designs during all risk significant accidents such as SBO — see Ref. [19]. This Generic Issue will be resolved independently of the rulemaking effort.

***Step 9: Implementing the change***

Rulemaking on the proposed changes commenced, and SECY-03-0127 [20], a written issues paper by the NRC staff dated July 24, 2003, deal with the final rulemaking on the risk informed 10 CFR 50.44. Among its attachments the SECY includes the US Federal Register Notice with the final rule, the Regulatory Analysis, and the needed revisions to Regulatory Guide 1.70 [21] and the Standard Review Plan.

***Step 10: Monitoring the change***

Monitoring of the revised regulations will be carried out.

## REFERENCES


[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, IAEA; INSAG-10, IAEA, Vienna (1996).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Margins of Operating Reactors, IAEA-TECDOC-1332, Vienna (2003).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion; Safety Series No. 50-P-1, IAEA, Vienna (1990).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (LPSA), IAEA-TECDOC-1106, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Probabilistic Safety Assessments by Regulatory Bodies, Safety Reports Series No. 25, IAEA, Vienna (2002).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, Vienna (2001).

[7] US NUCLEAR REGULATORY COMMISSION, Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement, 10 CFR 42622, Federal Register Vol. 60, US Government Printing Office, Washington, DC (1995) 42622.

[8] US NUCLEAR REGULATORY COMMISSION, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Regulatory Guide 1.174, USNRC, Rockville, MD (1998).

[9] US NUCLEAR REGULATORY COMMISSION, Proposed Staff Plan for Risk-Informing Technical Requirements in 10 CF Part 50, SECY-99-264, USNRC, Rockville, MD (2000).

[10] UNITED STATES CODE OF FEDERAL REGULATIONS, Back-fitting, 10 CFR 50.109, US Government Printing Office, Washington, DC (1989).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Basis Safety Principles for Nuclear Power Plants, IAEA; 75-INSAG-3 Rev. 1; INSAG-12, IAEA, Vienna (1999).

[12] HEALTH AND SAFETY EXECUTIVE, Safety Assessment Principles for Nuclear Plants, HMSO, London (1992).

[13] THE AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, RA-S-2002, ASME, New York (2003).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, IAEA-TECDOC-1101, Vienna (1999).

[15] US NUCLEAR REGULATORY COMMISSION, Safety Goals for the Operations of Nuclear Power Plants: Policy Statement, 51 FR 30028, Federal Register Vol. 51, US Government Printing Office, Washington, DC (1986) 30028.

[16] US NUCLEAR REGULATORY COMMISSION, Framework for Risk-Informed Changes to the Technical Requirements of 10 CFR 50, Attachment 1 to SECY-00-198, USNRC, Rockville, MD (2000).

[17] UNITED STATES CODE OF FEDERAL REGULATIONS, Standards for combustible gas control system in light-water-cooled power reactors; 10 CFR 50.44, US Government Printing Office, Washington, DC, Revised as of January 1, 2002.

[18] UNITED STATES CODE OF FEDERAL REGULATIONS, Appendix A to Part 50 General Design Criteria, 10CFR50, US Government Printing Office, Washington, DC, Revised as of January 1, 2002.

[19] US NUCLEAR REGULATORY COMMISSION, Generic Issue Station Black Out, (GI-189) USNRC, Rockville, MD (1998).

[20] US NUCLEAR REGULATORY COMMISSION, Combustible Gas Control in Containment, Final Rulemaking—Risk-Informed 10 CFR 50.44, SECY-03-0127 (2003).
[21] US NUCLEAR REGULATORY COMMISSION, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, Regulatory Guide 1.70, Rev. 3, USNRC, Rockville, MD (1978).

## ABBREVIATIONS

| | |
|---|---|
| ALARA | as low as reasonably achievable |
| ALARP | as low as reasonably practicable |
| ASME | American Society of Mechanical Engineers |
| BSL | basic safety limit |
| BSO | basic safety objective |
| BWR | boiling water reactor |
| CDF | core damage frequency |
| CFR | Code of Federal Regulations of the USA |
| DBA | design basis accident |
| DBE | design basis earthquake |
| ECCS | emergency core cooling system |
| GDC | general design criteria |
| INSAG | International Nuclear Safety Advisory Group |
| LERF | large early release frequency |
| LOCA | loss of coolant accident |
| LWR | light water cooled reactor |
| NPP | nuclear power plant |
| PRA | probabilistic risk analysis/assessment |
| PSA | probabilistic safety analysis/assessment |
| PWR | pressurized water reactor |
| QA | quality assurance |
| RCS | reactor coolant system |
| SBO | station blackout |
| SONGS | San Onofre Nuclear Generating Station |
| SSC | systems, structures and components |
| TMI-2 | Unit 2 of the Three Mile Island plant |

## CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|---|---|
| Drouin, M. | Nuclear Regulatory Commission, United States of America |
| Grantom, R. | NPP South Texas, United States of America |
| Hill, T. | National Nuclear Regulator, South Africa |
| Lehner, J. | Brookhaven National Laboratory, United States of America |
| Lyubarskiy, A. | Federal Nuclear and Radiation Safety Authority of the Russian Federation, Russian Federation |
| Misak, J. | International Atomic Energy Agency |
| Parry, G. | Nuclear Regulatory Commission, United States of America |
| Ranguelova, V. | International Atomic Energy Agency |
| Shepherd, C. | Health and Safety Executive, United Kingdom |
| Vaughan, G. | Health and Safety Executive, United Kingdom |
| Vayssier, G. | Nuclear Safety Consultancy, Netherlands |
| Vojnovic, D. | Slovenian Nuclear Safety Administration, Slovenia |

### Consultants Meetings

15–18 October 2002, 20–24 October 2003

### Technical Committee Meeting

Washington, DC, United States of America: 5–9 November 2001