



**Australian Government**

---

**Australian Radiation Protection and Nuclear Safety Agency**

# **REGULATORY ASSESSMENT PRINCIPLES FOR CONTROLLED FACILITIES**

**RB-STD-42-00 Rev 1**

**Regulatory Branch  
October 2001**

© Commonwealth of Australia 2001

**Copyright**

© Commonwealth of Australia 2001

This work is copyright in both electronic and printed form. You may download, display, print or otherwise reproduce this material, in whole or in part, in unaltered form only (retaining this notice) for your personal, educational or other non-commercial use. This is subject to the inclusion of an acknowledgment of the source and no commercial usage or sale. All other rights are reserved.

Reproduction for purposes other than those indicated above requires prior written permission from AUSINFO. Requests and enquiries concerning the content of this document should be addressed to the ARPANSA Information Officer, Lower Plenty Road, Yallambie VIC 3085.

## EXECUTIVE SUMMARY

This document describes the assessment principles to be applied by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) when assessing an application for a facility licence as well as approvals under licence for changes to facilities already the subject of a facility licence.

This document supersedes the assessment principle documents of the predecessor agencies to ARPANSA as all current regulatory guidance documents are made under the *Australian Radiation Protection and Nuclear Safety Act 1998* and the *Australian Radiation Protection and Nuclear Safety Agency Regulations 1999* currently in force. The superseded documents include the Nuclear Safety Bureau Safety Assessment Principles, the Australian Atomic Energy Commission Memorandum 100/1969, and the Regulatory Bureau Memorandum 1/82.

In preparing this document, ARPANSA drew from international publications and experience, especially from the International Nuclear Safety Advisory Group (INSAG) and the International Atomic Energy Agency (IAEA). The users of this document will be primarily the assessors within ARPANSA.

The document emphasises safety culture and 'defence in depth'. Defence in depth is a methodology that is widely accepted in the nuclear industry as part of international best practice. Defence in depth is implemented in the form of a hierarchy of diverse levels of equipment and procedures. ARPANSA strongly supports its application to controlled facilities and particularly looks for its proper implementation. When properly implemented, the principle should ensure that no single human or equipment failure would lead to injury to the public, and unlikely combinations of failures would lead to little or no injury.

This document is structured by the levels of defence in depth to underline its importance and to ensure that all safety considerations are addressed in a consistent manner. Additionally, the document may assist operating organisations in the preparation of the safety analysis report that might accompany an application for a licence or other submission. Finally, the document serves to inform the public about ARPANSA's regulatory assessment process.



## REGULATORY FRAMEWORK

The objective of the *Australian Radiation Protection and Nuclear Safety Act 1998* is to protect the health and safety of people, and to protect the environment, from the harmful effects of radiation.

So that the CEO of the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) may achieve this objective when carrying out his regulatory functions under the Act, a regulatory framework has been developed which reflects international best practice in relation to radiation protection and nuclear safety.

The requirements of the ARPANS Act and Regulations are the bases for the formation of supplementary regulatory documents. The ARPANSA document *Regulatory Assessment Principles for Controlled Facilities* is one such document. Other supplementary regulatory documents include ARPANSA's regulatory guideline documents.

The assessment criteria used by ARPANSA are identified in those supplementary ARPANSA documents. ARPANSA may also use appropriate codes of practice.

The extent to which individual criteria affect the regulatory assessment depends on their relevance. ARPANSA recognises that the relevance of each of the criteria will be different for different types of controlled facility, controlled apparatus or controlled material. The principles in the document *Regulatory Assessment Principles for Controlled Facilities* are those criteria on which ARPANSA places highest importance. At the time of the assessment, ARPANSA considers the relevance of each criterion to allow for different types of controlled facility, controlled apparatus or controlled material. ARPANSA may assess some criteria as being not relevant because they do not apply to the particular controlled facility, controlled apparatus or controlled material being assessed. Any criteria that are relevant to the particular controlled facility, controlled apparatus or controlled material and involve radiation dose limits are treated as mandatory.

The operating organisation's safety analysis for a controlled facility, controlled apparatus or controlled material can assist the regulatory judgements with respect to a criterion by clearly demonstrating that the criterion is addressed. An alternative to a criterion may be acceptable to ARPANSA if it provides a degree of safety equivalent to that of the criterion it is proposed to replace.



## FOREWORD

The ARPANSA *Regulatory Assessment Principles* are, in one sense, intended purely for internal purposes - as a guide to staff of the Agency in assessing the safety of controlled facilities proposed or operated by Commonwealth entities. They are also of professional and public interest: to the Commonwealth entities that require licences from ARPANSA to construct, operate and decommission controlled facilities and who need to know how they are to be assessed; and to the public at large who may wish to satisfy themselves that ARPANSA is applying 'international best practice' to the regulatory assessment of controlled facilities.

ARPANSA's *Regulatory Assessment Principles* have a long and distinguished pedigree. Similar documents have been in place and used by the Nuclear Safety Bureau and predecessor organisations since 1969. The most immediate relatives of the present document are the *Draft Safety Assessment Principles*.

Much of the present document owes its structure and philosophy to the work of the International Nuclear Safety Advisory Group (INSAG). This is a group of international nuclear experts that was set up to advise the Director General of the International Atomic Energy Agency in 1986. One of the remits of the INSAG is 'to formulate, where possible, commonly shared safety concepts'. This they have done in a number of publications over the years - most comprehensively in the formulation of *Basic Safety Principles for Nuclear Power Plants*, first published in 1988 and revised in 1999. Those Safety Principles and other supporting documents describe two important concepts that ARPANSA has drawn upon in the formulation of its regulatory assessment principles - safety culture and defence in depth. They are the 'Fundamental Principles' upon which the Regulatory Assessment Principles are based and they affect all the other principles.

Safety culture is the collection of characteristics and attitudes in the organisation and in the individuals working in the organisation that ensure that safety issues are treated properly with the attention required by their significance. Defence in depth is about all safety activities being subject to layers of overlapping provisions - multiple levels of protection - so that if a failure should occur it should be compensated for without causing harm to operators or the public.

While it is the case that the INSAG 'Basic Principles' were drawn up with nuclear power plants in mind, ARPANSA believes that the concepts of defence in depth and safety culture are applicable to the range of facilities likely to be considered in the Australian context: research reactors, radioisotope production facilities, fuel and waste management facilities, accelerators and major irradiators. Naturally, the principles need to be applied with sensible regard to the hazard of the particular facility under consideration.

ARPANSA's commitment is to engage with stakeholders, including the public, to inform debate and subsequent policy decision making in an open and timely way, and to publish important processes, licences, discussion documents, decisions and reasons for decisions on ARPANSA's website.

I am confident that application of these regulatory assessment principles will allow me to be assured that ARPANSA's regulatory assessments meet the objective of the ARPANS Act: 'to protect the health and safety of people, and to protect the environment, from the harmful effects of radiation.'

John Loy  
CEO of ARPANSA.

# CONTENTS

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
<b>2</b>	<b>FUNDAMENTAL PRINCIPLES .....</b>	<b>2</b>
	SAFETY CULTURE .....	2
	DEFENCE IN DEPTH .....	2
<b>3</b>	<b>SAFETY CULTURE.....</b>	<b>4</b>
	OPERATING ORGANISATION.....	5
	CONSERVATIVE PROVEN DESIGN AND ENGINEERING PRACTICE .....	6
	QUALITY ASSURANCE .....	6
	FEEDBACK OF OPERATIONAL EXPERIENCE .....	7
<b>4</b>	<b>SAFETY ANALYSIS.....</b>	<b>7</b>
	SAFETY CASE .....	7
	SAFETY ANALYSIS REPORT .....	7
	CATEGORISATION BY HAZARD AND SAFETY SIGNIFICANCE .....	8
	DESIGN-BASIS AND BEYOND-DESIGN-BASIS ACCIDENTS .....	10
	PERIODIC REVIEWS .....	13
	PLANNING FOR DECOMMISSIONING .....	14
<b>5</b>	<b>DEFENCE IN DEPTH .....</b>	<b>14</b>
	DEFENCE IN DEPTH LEVEL 1 .....	15
	HUMAN FACTORS .....	15
	SITE CHARACTERISTICS .....	16
	INHERENT SAFETY CHARACTERISTICS.....	16
	NUCLEAR FUEL INTEGRITY .....	17
	DEFENCE IN DEPTH LEVEL 2.....	17
	RADIATION PROTECTION .....	17
	OPERATIONAL LIMITS AND SAFETY SYSTEM SETTINGS .....	19
	INSPECTION, TESTING AND MAINTENANCE .....	20
	MODIFICATIONS.....	20
	NUCLEAR MATERIAL.....	20
	RADIOACTIVE WASTE .....	21
	DECOMMISSIONING AND POST-DECOMMISSIONING .....	22
	FACILITY LIFE MANAGEMENT.....	22
	AUTHORISATION OF PERSONNEL .....	23

---

DEFENCE IN DEPTH LEVEL 3 .....	23
IDENTIFICATION OF SAFETY SYSTEMS .....	23
MEASUREMENT OF PROCESS VARIABLES .....	24
REDUNDANCY, INDEPENDENCE AND DIVERSITY IN SYSTEMS IMPORTANT TO SAFETY .....	24
INDEPENDENCE OF PROCESS CONTROL SYSTEMS AND SAFETY SYSTEMS .....	25
UNPLANNED CRITICALITY .....	26
FIRE PROTECTION.....	26
PROCESS PLANT .....	27
DISABLING/BYPASSING SAFETY SYSTEMS .....	27
PERFORMANCE TESTING .....	28
CONFINEMENT AND CONTAINMENT SYSTEMS.....	28
DEFENCE IN DEPTH LEVEL 4.....	29
DEFENCE IN DEPTH LEVEL 5 .....	29
SITING ASSESSMENT .....	30
SITING PRINCIPLES.....	30
OFF-SITE EMERGENCY RESPONSE .....	31
<b>6 APPENDIX .....</b>	<b>34</b>
INTERNATIONAL CONVENTION ON NUCLEAR SAFETY .....	34
<b>7 REFERENCES .....</b>	<b>34</b>
<b>8 BIBLIOGRAPHY .....</b>	<b>35</b>
<b>9 INDEX.....</b>	<b>37</b>

# 1 INTRODUCTION

1.1 The principles in this document are those criteria on which ARPANSA places highest importance when it performs a regulatory assessment of controlled facilities.

1.2 This document applies to controlled facilities that are defined in Part 2 of the ARPANSA Act and includes nuclear installations and prescribed radiation facilities. It is written so that the assessors within ARPANSA can apply the principles to any facility thus defined. This document hereafter uses the term 'facility' in place of 'controlled facility' for convenience.

1.3 In preparing this document, ARPANSA drew from international publications and experience, especially from the International Nuclear Safety Advisory Group (INSAG) and the International Atomic Energy Agency (IAEA). The approach of ARPANSA to the regulatory assessment of facilities is strongly influenced by the INSAG publications 'Basic Safety Principles for Nuclear Power Plants' (INSAG-3, [1] and [2]), because of the emphasis on safety culture and defence in depth. While there are no existing or planned nuclear power plants in Australia, and most of the Commonwealth's facilities are not nuclear reactors, much of the emphasis in [1] and [2] is applicable to any facility where safety is important.

1.4 ARPANSA reviews its regulatory assessment principles, modifying them as required to recognise evolving international standards.

1.5 To minimise any misinterpretation due to the use of terms, reference may be made to ARPANSA's regulatory assessment glossary. [3].

1.6 The users of this document will be primarily the assessors within ARPANSA. However, the document may also assist operating organisations in the preparation of the safety analysis report that might accompany an application for a licence or other submission. Additionally, the document serves to inform the public about ARPANSA's regulatory assessment process.

1.7 This document is applicable to existing facilities as well as new facilities, including proposals for modification. Existing facilities may have been designed to different safety standards, and judgements may be necessary regarding the application of this document.

1.8 Where principles apply specifically to nuclear reactors, this is noted in the text.

1.9 The operating organisation's safety analysis for a facility can assist the regulatory judgements with respect to a principle by clearly demonstrating that the principle is addressed. An alternative to a principle in this document may be acceptable to ARPANSA if it provides a degree of safety equivalent to that of the principle it is proposed to replace.

1.10 The responsibility for the safety of a facility and for demonstrating that there is an adequate degree of safety rests with the operating organisation, not ARPANSA.

1.11 Economic analyses are the responsibility of the operating organisation and are not addressed in this document. This document does not address accidents of a conventional industrial nature that have no radiological impact and does not address non-radiological effects of the facility on the environment that may be subject to separate national regulatory requirements.

1.12 By using this document to assess a facility, ARPANSA is addressing the terms and obligations of the International Convention on Nuclear Safety of which Australia is a Contracting Party (see Appendix).

## 2 FUNDAMENTAL PRINCIPLES

### SAFETY CULTURE

2.1 Safety culture has been defined by the IAEA as being that assembly of characteristics in organisations and individuals which establishes that, as an overriding priority, safety issues receive the attention warranted by their significance. A poor safety culture is usually most apparent when an excessive number of incidents or accidents occur. Operating organisations and regulatory bodies strive to find indicators that which will indicate poor safety performance before incidents or accidents occur.

2.2 Safety culture is relevant to all levels of defence in depth. Organisations and individuals involved in activities that may affect any level of defence in depth need to be committed to a strong safety culture. To this end, ARPANSA encourages open communication with the operating organisations.

#### *Principle*

- (1) *The operating organisation demonstrates commitment to a strong safety culture through the articulation at the highest level, of a safety policy that stresses the importance of a commitment to safety by organisations and individuals. In particular:*
- *Open, questioning attitudes are fostered towards matters affecting safety.*
  - *A rigorous and prudent approach is fostered to tasks that are relevant to the design of facilities.*
  - *Individuals are encouraged to freely communicate with line managers and others, their concerns on design safety matters and suggestions for improvement.*

### DEFENCE IN DEPTH

2.3 A design methodology that is widely accepted in the nuclear industry as part of international best practice is defence in depth. Defence in depth is used to provide a high degree of confidence that accidents in facilities will be prevented, and to ensure that the radiological consequences of any design-basis accidents would be minor and within prescribed limits. Furthermore, defence in depth is used to ensure that the likelihood of any beyond-design-basis accident that could have serious radiological consequences is extremely small.

2.4 Defence in depth is implemented in the form of a hierarchy of diverse levels of equipment and procedures. The implementation of defence in depth in the design of a facility provides protection against a wide variety of operational occurrences and accidents, including those that might originate from equipment failures and human error and from events outside the facility. When properly implemented, defence in depth should ensure that no single human or equipment failure would lead to injury to the public, and unlikely combinations of failures would lead to little or no injury.

2.5 Table 1 shows the five levels of defence in depth that are used in this document. The levels are those of [4] (Defence in Depth in Nuclear Safety). The first four levels are oriented towards the protection of barriers and mitigation of releases; the last relates to off-site emergency response. Each level envelops the levels below. The levels are successive, that is, depending on the hazards identified in the safety analysis for the facility, the number of levels may be less than five. For example, in the case of facilities where there is no significant hazard outside the facility, the fifth level of defence in depth would not be required.

### ***Principle***

- (2) *Defence in depth is implemented at the facility to provide diverse layers of protection as successive levels, as shown in Table 1.*

**Table 1. Levels of defence in depth**

<i>Level of Defence in Depth</i>	<i>Objective</i>	<i>Essential Means</i>
1	Prevent failures, and ensure that anticipated operational occurrences/disturbances are infrequent.	Conservative, high quality, proven design and high quality in construction.
2	Maintain the intended operational states and detect failures.	Process control and limiting systems, other surveillance features and procedures.
3	Protect against design-basis accidents.	Safety systems and accident procedures.
4	Limit the progression and mitigate the consequences of beyond-design-basis accidents.	Accident management and mitigation.
5	Mitigate the radiological consequences of beyond-design-basis accidents.	Off-site emergency response.

### 3 SAFETY CULTURE

3.1 Safety culture pertains to organisational aspects of facilities and includes the responsibility of the operating organisation; conservative proven design and engineering practice; quality assurance; and feedback of operational experience.

3.2 In line with INSAG-3 ([1] and [2]), ARPANSA places much importance on the safety culture of the operating organisation.

## OPERATING ORGANISATION

3.3 In this document, the term 'operating organisation' means an organisation that applies for a licence or is a licence holder. The prime responsibility for the safety of facilities rests with the operating organisation.

### *Principles*

- (3) *The operating organisation has full responsibility for the safety of its facilities.*
- (4) *The operating organisation has detailed plans and periodic reviews with measurable outcomes that demonstrate that it has:*
  - (a) *Adequate managerial structure and resources, including financial capability;*
  - (b) *An adequate historical records system;*
  - (c) *Adequate security and safeguard programs, where appropriate;**to discharge its obligations, responsibilities and liabilities regarding the safety of its facilities.*
- (5) *The operating organisation demonstrates:*
  - (a) *Safety of a facility throughout all stages of its life.*
  - (b) *Compliance with requirements arising from any environmental assessments by Commonwealth Government environmental protection agencies.*
  - (c) *Compliance with all relevant legislation and any obligations of Australia under international treaties.*
- (6) *Positive safety attitudes are instituted and encouraged by senior management. Clear lines of authority and responsibility are established, procedures developed, sufficient resources provided, and a quality assurance system is implemented.*
- (7) *High standards of human performance and competence are expected within the operating organisation. Staff selection and training emphasise inherent abilities, qualification, personal stability, integrity, and a responsible attitude.*
- (8) *Assessment, verification and feedback activities are implemented, including independent reviews. Reviews and audits are conducted for all activities important to safety and an ongoing safety assessment program is established. Lessons are learned from operating experience and safety research, both within the organisation and internationally, and are acted on.*
- (9) *The operating organisation uses safety improvement and safety accountability indicators which take into account the extent of pending maintenance and modification tasks, radiation doses to operations staff and abnormal event reports.*

## CONSERVATIVE PROVEN DESIGN AND ENGINEERING PRACTICE

3.4 Conservative design, with conservative safety margins, applies at defence in depth levels 1 through 3. At levels 4 and 5, where highly improbable accidents and the uncertainties in the calculations of risk dominate the absolute numbers, best-estimate methodologies are more appropriate.

3.5 Whilst innovation is a prerequisite for improved designs, innovations may introduce unexpected vulnerability. The greater the innovation in the design of systems, structures and components, the greater the need for demonstration of performance and reliability.

### *Principles*

(10) *Conservative, proven design and engineering practice are used at defence in depth levels 1-3. This includes the determination of safety margins.*

(11) *Best-estimate methods and data may be used for any analyses of beyond-design-basis accidents (defence in depth levels 4-5).*

*This is in contrast to the use of conservative, deterministic methods of analysis for design-basis accidents for nuclear reactors. Calculation of the consequences of beyond-design-basis accidents and their frequency involves models of core melt progression, estimates of the source term, and models of atmospheric transport, and thus have large uncertainties.*

(12) *Technologies incorporated in the design are proven technologies, developed through: innovation, laboratory scale demonstrations, operating prototypes, and use in other facilities.*

## QUALITY ASSURANCE

3.6 Any human activity that is carried out to a specification, instruction or procedure can affect all items subject to it. Errors in design specifications, drawings, maintenance specifications and procedures could cause the failure of items subject to them. This kind of dependence represents the strongest possible coupling between redundant systems and has the potential to be a source of common cause failures. In the overall defensive strategy against common cause failures, a thorough QA program provides a major defence against dependencies.

### *Principles*

(13) *The operating organisation has a formal QA program in place that is applied at each of the stages in the life of the facility.*

(14) *The operating organisation has a recognised quality practices certification that is applied to the facility.*

- (15) *Design specifications, drawings, test, inspection and maintenance specifications and procedures are current and reflect the status of the facility at all stages in its life.*

## **FEEDBACK OF OPERATIONAL EXPERIENCE**

3.7 Decades of nuclear facility operation have led to improvements in safety culture and the implementation of defence in depth. Feedback of experience from periodic testing and maintenance and from the investigation of incidents has positively influenced design assumptions and operator task performance at defence in depth levels 1-3. At levels 4-5, feedback of operational experience has led to improved accident mitigation and emergency preparedness.

### ***Principle***

- (16) *Abnormal occurrences, the analysis of incidents and safety performance of similar facilities worldwide, the results of periodic testing, safety system performance testing, maintenance and modifications, and emergency preparedness exercises, are reviewed and fed back as appropriate into:*
- *Revised safety analyses, design modifications, revised procedures and revised quality assurance systems; and*
  - *Personnel performance assessment and counselling and retraining.*

## **4 SAFETY ANALYSIS**

### **SAFETY CASE**

4.1 For each of the principal stages in the life of a facility and as part of the licensing process, ARPANSA requires that an applicant for a licence submit an updated safety case as part of the licence application. The safety case demonstrates that throughout its life, the facility complies with the radiation dose limits specified in the 'Radiation Protection' section and Table 2 of this document, and explicitly describes how radiation exposures are kept as low as reasonably achievable (ALARA).

4.2 The safety case includes the design information for the facility, including the operational limits and conditions within which the facility must operate, and a safety analysis that is documented in a safety analysis report (SAR).

### **SAFETY ANALYSIS REPORT**

4.3 The extent and rigour of the SAR is commensurate with the hazard categorisation of the facility. A SAR is relevant to non-reactor facilities as well as reactors.

4.4 The margins between the operational limits and conditions and the relevant safety limits are included in the SAR.

4.5 To facilitate reference to two important versions of the SAR, the term 'preliminary SAR' (PSAR) is used for the version of the SAR that is first submitted to ARPANSA with an application for a licence to construct a facility. The term 'final SAR' (FSAR) is used for the updated version of the SAR that is submitted to ARPANSA with an application for a licence to operate a facility. 'PSAR' and 'FSAR' are thus progressive versions of the one SAR. The SAR is a living document that is updated as appropriate throughout the life of the facility (including the decommissioning stage) to reflect its current state.

## CATEGORISATION BY HAZARD AND SAFETY SIGNIFICANCE

4.6 An objective of this section is to ensure that the hazard associated with the facility is categorised and that there is also a categorisation by safety significance of systems, structures and components. The section aims to ensure that the extent and rigour of the safety analysis is consistent with those categorisations.

### *Principles*

- (17) *For each of the stages in the life of the facility and as part of the regulatory assessment process that leads to the licensing of a facility, the operating organisation submits to ARPANSA an updated safety case.*
- (18) *The safety case demonstrates that throughout its life and under conditions of normal operation and abnormal operation, the facility complies with the radiation dose limits specified in the 'Radiation Protection' section and Table 2 of this document, and that radiation exposures are as low as reasonably achievable (ALARA).*
- (19) *The safety case includes a safety analysis that is documented in a safety analysis report (SAR).*
- (20) *The safety analysis:*
  - (a) *Establishes the hazard of the facility according to the following categories:*
    - *Hazard Category F1: where there is no potential for significant consequences outside the facility.*
    - *Hazard Category F2: where there is potential for significant consequences on the site outside the facility, but not outside the site.*
    - *Hazard Category F3: where there is potential for significant consequences outside the site.*
  - (b) *Is conducted to an extent and rigour that reflects the hazard categorisation.*
  - (c) *Is conducted to an extent and rigour that reflects the categorisation by safety significance of structures, systems and components.*
  - (d) *Is conducted to an extent and rigour that reflects the margin to the relevant safety limits.*
  - (e) *Is self-standing, that is, all information necessary to support the safety analysis is available on record via a suitably referenced structure of documentation which is preserved throughout the life of the facility.*
  - (f) *Includes design-basis analyses, any beyond-design-basis analyses and, where relevant, criticality analyses.*
  - (g) *Considers transient and steady-state behaviour.*

- (h) In the case of nuclear reactors and critical assemblies, considers the effect during reactivity transients of inherent negative and positive coefficients of reactivity under conditions of normal and abnormal operation.*
  - (i) Considers internal and external hazards such as fire, flooding and earthquakes and any other initiating events that have the potential to impair several levels of defence in depth.*
  - (j) Addresses the integrity of computer-based systems and associated software that are important to safety, including details of any independent assessment of that integrity that might use diverse checking methods.*
  - (k) Confirms the effectiveness of the safety systems.*
  - (l) Includes studies such as task analyses that consider the reliability of personnel and the demands on personnel during normal and abnormal operation.*
  - (m) Addresses changes in defence in depth effectiveness during facility shutdowns, or during operations with controlled materials, including radioactive waste.*
  - (n) Is presented in a manner that facilitates verification of the safety analysis assumptions, methods, and the degree of conservatism, including human factor aspects.*
- (21) The SAR for the facility is a 'living document', that is, it is continuously developed and updated through all principal stages in the life of the facility, and reflects the appropriate depth of detail at each stage.*
- (22) The SAR includes the numerical values for the operational limits and conditions, and the proximity to the relevant safety limits, for conditions of normal and abnormal operation.*
- (23) The design bases for components, systems and structures are derived and justified in the SAR. The SAR demonstrates the adequacy of the design to meet the radiation dose limits specified in the 'Radiation Protection' section and Table 2 of this document, during normal operation, anticipated operational occurrences and design-basis accident conditions.*
- (24) The SAR addresses the use of software in computer-based systems important to safety, including in each case details of: how the software is validated and verified, taking into account software design errors that might result in common cause failures or result from specification errors; and how quality assurance and access security are applied to software development, operation and maintenance.*
- (25) For failures of non-redundant components for which defence in depth level 2 is inapplicable, the safety analysis demonstrates that such accidents do not dominate the total risk (in terms of consequences and frequency of occurrence) at the facility. That is, such accidents do not contribute to risk in a way that is excessive in comparison with other accidents. The safety analysis takes into account arrangements at defence in depth levels 1,3,4,5. Such failures might include, for example, sudden failure of a nuclear reactor vessel.*
- (26) Where a new facility is planned for a site that already has facilities, including shutdown and decommissioned facilities, its safety analysis takes into account any safety impact on existing facilities that might occur.*

## DESIGN-BASIS AND BEYOND-DESIGN-BASIS ACCIDENTS

4.7 Design-basis accidents are those accidents that are accommodated within the design of the facility. The design for such accidents addresses internal and external initiating events that may cause the facility to operate outside its limits for normal operation and anticipated operational occurrences. For additional information on external events and design-basis accidents, reference should be made to ARPANSA's siting guideline [5]. The analysis of design-basis accidents determines the safety margins and provides confidence in the robustness of the facility. ARPANSA considers that facilities should be designed so that there is no need for off-site emergency response following a design-basis accident.

4.8 Beyond-design-basis accidents are very improbable accidents that might lead to more severe consequences than design-basis accidents, including release of controlled materials to the environment. However, their lower frequency of occurrence must ensure that they do not result in intolerable risk. The analysis of beyond-design-basis accidents can give valuable insights into plant or systems areas where changes might lead to reductions in consequences or a reduction in accident likelihood. A particular beyond-design-basis accident, called the Reference Accident, is used in the initial assessment of the suitability of a proposed site for a facility with Hazard Category F2 or F3.

4.9 The classification of accidents into design-basis accidents and beyond-design-basis accidents will result from decisions taken by the designer. Those decisions will take into account the characteristics of the facility and the particular relationship between the consequences of accidents and their frequency.

4.10 Probabilistic safety analysis (PSA) methodology is a formalised, structured approach that provides the insights into potential facility weaknesses that may not be evident using deterministic methods. PSA also complements the use of deterministic methods of safety analysis at defence in depth levels 4-5 where best-estimate methods and data become increasingly important.

4.11 A level 1 PSA, which considers the frequency of release of radioactive material into the facility, may be used to confirm that a design has a balanced implementation of defence in depth. Depending on the hazard category of the facility, it may be sufficient to estimate risk from the results of a level 1 PSA, or by otherwise combining consequences that are calculated by deterministic methods, with estimates of plant damage probabilities.

4.12 Levels 2 and 3 PSA, which consider the release of radioactive material from the facility into the environment and exposure of the public, may be used to confirm that the safety limits specified in Table 2 are not exceeded. These limits set the maximum acceptable risk of accidents, grouped by individual doses at the site boundary. For each group, the risk of accidents should be as low as reasonably achievable below the safety limit. If the risk is greater than the safety objective specified for each group, it is necessary to consider whether the expenditure of further resources would be unwarranted by the reduction in the risk that would be achieved.

**Table 2. Safety limits and objectives**

<i>Maximum effective dose to most exposed individual off-site (mSv)</i>	<i>Total frequency, per facility year</i>	
	<i>Safety limit</i>	<i>Safety objective</i>
<i>0.1 - 1</i>	<i>1</i>	<i>10<sup>-2</sup></i>
<i>1 - 10</i>	<i>10<sup>-1</sup></i>	<i>10<sup>-3</sup></i>
<i>10 - 100</i>	<i>10<sup>-2</sup></i>	<i>10<sup>-4</sup></i>
<i>100 - 1000</i>	<i>10<sup>-3</sup></i>	<i>10<sup>-5</sup></i>
<i>&gt; 1000</i>	<i>10<sup>-4</sup></i>	<i>10<sup>-6</sup></i>

Notes on Table 2:

- 'Total frequency' refers to the summed frequencies of all accidents giving rise to radiation doses within each dose band.
- Consistent assumptions and levels of conservatism are used over the frequency range of each band.
- Between the safety limit and the safety objective, risks must be shown to be as low as reasonably achievable.
- Table 2 is taken from the 1992 UK NII document [8]. The risk to an individual implied by Table 2 is of the order of  $10^{-5}$  per year for a facility just meeting the safety limits, and  $10^{-7}$  per year for a facility just meeting the safety objectives. This is consistent with the objective used by the NSW Department of Urban Affairs and Planning for total non-nuclear accidents which result in public fatalities [9]. Tolerability of risk is discussed in a 1998 UK NII document [10].
- In the case of nuclear reactors the potential hazard is inherently limited by the fission product inventory, and therefore the benefits of investigating highly improbable accidents diminish as the frequency decreases. Nevertheless, depending on the hazard category of the facility, the safety objective figures suggest an investigation of individual accidents having frequencies down to  $10^{-7}$  per year can be useful, by establishing that there is no sudden increase in consequences in the vicinity of  $10^{-6}$ .

### ***Principles***

- (27) *All accidents are identified using a fault analysis, and are classified as either:*
- Design-basis accidents, or*
  - Beyond-design-basis accidents.*
- (28) *The frequency and consequences, in terms of doses to the public, of accidents are assessed and comply with the values given in Table 2.*

- (29) *If a deterministic analysis is used to establish compliance with Table 2, conservative assumptions are used. If a PSA is used to establish compliance with Table 2, best-estimate methods and data are used for determining frequencies.*
- (30) *Deterministic methods are used for the analyses of both design-basis and beyond-design-basis accidents to determine the consequences; the analyses confirm that no off-site emergency intervention would be required following any design-basis accident at the facility.*
- (31) *The frequency of accidents at the facility is as low as reasonably achievable below the relevant safety limit. If the frequency is greater than the relevant safety objective, the expenditure of further resources would be unwarranted by the reduction in the risk that would be achieved.*
- (32) *For a nuclear reactor, the safety analysis confirms that the frequency of significant damage to the nuclear core is as low as reasonably achievable<sup>1</sup>, and is less than  $10^{-4}$  per year. For a new nuclear reactor, the objective should be to demonstrate that the frequency of significant damage to the nuclear core is less than  $10^{-5}$  per year.*

*In this context, significant damage to the nuclear core means the loss of a facility's core structural integrity or melting of a significant fraction of the nuclear fuel accompanied by loss of the effectiveness of the nuclear fuel cladding barrier (for example, following the failure of heat removal or a reactivity excursion).*

*This principle is intended to ensure that the design is balanced, that is, that safety at defence in depth levels 1-3 is not relegated unduly to defence in depth levels 4-5.*

- (33) *Probabilistic methods may be used for analysing in a relative manner the balance of a design of Hazard Category F2 or F3 facilities to check that no single accident, or group of accidents, is likely to contribute to the overall risk at a facility in a way that is excessive in comparison with other accidents.*
- (34) *Probabilistic methods may be used to identify specific parts of a Hazard Category F2 or F3 facility on which safe operation depends, by performing sensitivity analyses where appropriate.*
- (35) *PSA is not used to justify a poorly engineered design which does not pass deterministic analyses.*
- (36) *Where used, PSA covers both design-basis and beyond-design-basis accidents, considers internal faults and external events, and takes into account:*
- (a) *The environmental conditions and the ageing of materials and components expected throughout the life of the facility.*
  - (b) *Uncertainties in the conditions of normal and abnormal operation.*

---

<sup>1</sup> If the safety objective is satisfied, the assessor needs only to assess the validity of the safety analysis. If the safety objective is not satisfied, the assessor needs to also consider whether the right balance has been struck by the operating organisation between the costs and the benefits, in other words, whether the risks have been made as low as reasonably achievable.

- (c) *Uncertainties in the reliability of structures, systems and components that are parts of barriers.*
  - (d) *The reliability of services such as electricity and water.*
  - (e) *Human factors.*
  - (f) *Common cause failures.*
  - (g) *Use of diversity.*
  - (h) *Changes in defence in depth effectiveness that can occur when structures, systems or components are taken out of service for maintenance during shutdowns.*
- (37) *Probabilistic methods may be used at Hazard Category F2 or F3 facilities to confirm that:*
- (a) *The design of safety systems is suitably fault tolerant and balanced (no single accident dominates the total risk) and the safety systems adequately protect against design-basis accidents.*
  - (b) *For beyond-design-basis accidents, there is no “cliff-edge” effect, that is, a sudden increase in consequences below the frequency band for design-basis accidents.*
  - (c) *The risks to the public comply with the safety limits specified in Table 2.*
- (38) *For a nuclear reactor, the safety analysis confirms that:*
- *The likelihood of failure of an emergency core cooling system to fulfil its safety function does not exceed  $10^{-2}$  per demand.*
  - *The likelihood of failure of a reactor shutdown system to fulfil its safety function does not exceed  $10^{-3}$  per demand.*

*'Failure to fulfil its safety function' includes performance failures. An example of a performance failure is where all components function, but the system does not fulfil its safety function because its action is inappropriate. Inappropriate action may result from a design oversight and inadequate performance testing.*

*This principle is intended to ensure that the design is balanced, that is, that safety at defence in depth level 3 is not relegated unduly to defence in depth levels 4-5.*

## PERIODIC REVIEWS

4.13 Periodic reviews are necessary to confirm that any changes to the design or operation of the facility do not invalidate the assumptions and conditions on which the safety analyses are based. The reviews may reveal the need for additional training of staff or updating of procedures following modifications.

### *Principles*

- (39) *Periodic reviews are conducted throughout the life of the facility to confirm that:*
- (a) *The hazard categorisation of the facility has not changed.*
  - (b) *The categorisation by safety significance of structures, systems and components, including those that are affected by or are introduced by modifications to the facility or its operations, remains appropriate.*
  - (c) *The safety analysis remains valid.*

- (d) *There is compliance with the radiation dose limits specified in the 'Radiation Protection' section and Table 2 of this document.*
- (40) *Personnel are further trained or retrained as appropriate following periodic reviews.*
- (41) *Procedures, QA system, safety case, records of the facility and other relevant items are updated as necessary following periodic reviews.*

## PLANNING FOR DECOMMISSIONING

4.14 The management of decommissioning involves planning, preparatory arrangements, and safety analyses. A decommissioning plan is required which clearly describes the proposed decommissioning process and the arrangements for ensuring the safety of site personnel, the public and the environment. The plan is used to assess whether or not decommissioning can be carried out safely.

### *Principles*

- (42) *For a facility which will eventually require a decommissioning approval, a decommissioning plan is prepared by the operating organisation as part of the safety case submitted for each of the principal stages in the life of the facility. The plan shows that eventual decommissioning can be carried out safely and the volume and activity of radioactive material resulting from decommissioning will be as low as reasonably achievable.*
- (43) *An initial radiological survey of the site that includes the ambient radioactivity of the atmosphere, hydrosphere, lithosphere and biota is conducted prior to any site activities for a facility that will require a licence to decommission the facility. The survey establishes baseline radiological information for assessing the future impact of the facility and provides a reference point for monitoring during and after decommissioning.*
- (44) *Any decommissioning plan required is updated by the operating organisation throughout the life of the facility and submitted to ARPANSA:*
- (a) *As part of each safety case that is submitted for each of the principal stages in the life of the facility.*
  - (b) *As early as practicable before the anticipated final shutdown of the facility, or at least one year before the anticipated final shutdown of the facility.*

## 5 DEFENCE IN DEPTH

5.1 This document is structured by the levels of defence in depth to emphasise the importance that is placed on defence in depth in the regulatory assessment process. This approach is consistent with the common practice of associating assessment criteria with different facility states. These states are the operational states (normal operation and anticipated operational occurrences) and the accident states (design-basis accidents and beyond-design-basis accidents).

5.2 The independence and diversity of the different levels of defence in depth are important contributors to the effectiveness of defence in depth.

5.3 The use of physical barriers that confine nuclear materials at various locations can be used as part of the implementation of defence in depth. For example, in the case of nuclear reactors, barriers in the form of the fuel matrix, the fuel cladding, the primary heat transport system pressure boundary, the pool and the reactor building can be used to confine nuclear materials and limit releases to the public and the environment.

## DEFENCE IN DEPTH LEVEL 1

5.4 Defence in depth at level 1 aims to prevent failures and abnormal operation through conservative, high quality, proven design and construction. Human factors, the characteristics of the site, and the inherent safety characteristics of the facility are taken into account.

### *Principles*

- (45) *A categorisation by safety significance is carried out for systems, structures, and components (including software), ranking them in terms of safety importance.*
- (46) *Proven engineering practice and standards are used in siting, design, manufacture, construction, installation, commissioning, inspection, training, operation, testing, maintenance, modification, criticality control, life extension, and decommissioning.*
- (47) *Standards:*
  - (a) *Typically range from national or international standards through to normal industrial standards.*
  - (b) *Are applied in a way that reflects the categorisation by safety significance of the structures, systems and components.*

## HUMAN FACTORS

5.5 One of the most important lessons from analyses of abnormal occurrences at facilities, ranging from accident precursors to serious accidents, is that they have often been the result of incorrect human action. Defence in depth affords additional protection against incorrect human action.

5.6 Attention to human factors at the design stage aims to develop facilities that are tolerant to human error. ARPANSA considers that any action required ensuring safety within 30 minutes of an accident at a nuclear reactor should be automatically initiated.

### *Principles*

- (48) *Facilities are designed with systematic consideration of human factors and ergonomic principles to reduce the potential for human error, facilitate correct actions by operators, and reduce operator stress.*

- (49) *Safety systems at nuclear reactors are designed to be automatically initiated and to require no immediate operator action within thirty minutes, while permitting operator initiation or action where necessary to ensure or enhance safety.*
- (50) *Control and control room layout provides ergonomic disposition of data and controls for actions important to safety, including accident management.*
- (51) *Diagnostic aids are provided to speedily resolve questions important to safety and to monitor the status of the facility.*
- (52) *A reliable and redundant communications system is provided for all operations staff.*
- (53) *Maintenance and inspection aspects such as access are considered in the design of equipment and systems.*

## **SITE CHARACTERISTICS**

5.7 Natural characteristics of the location of a facility such as its seismology, geology, meteorology, as well as other activities such as the use of land around the site, will affect the safety of the facility. These factors may provide initiating events for accidents or may impact arrangements for waste discharges and emergency response, and must be considered in the design of the facility. The design of a safe facility for any proposed site depends also on the characteristics of the facility, including its inherent safety characteristics and the nature of its hazards. For further information, reference should be made to ARPANSA's siting guideline [5].

### ***Principle***

- (54) *The design of a facility takes into account site characteristics which may impact the safety of the facility, including:*
  - (a) *The site's seismology, geology, topography, demography (population distribution and existing population centres), ecology, hydrology, and meteorology.*
  - (b) *The effect of nearby facilities and land usage.*
  - (c) *The availability and reliability of off-site services such as electricity, water, transportation, and communication systems.*
  - (d) *The feasibility of emergency response.*

## **INHERENT SAFETY CHARACTERISTICS**

5.8 In the case of nuclear reactors, the inherent safety characteristics are inextricably linked with the design. The design of the core affects the inherent safety characteristics such as temperature and void coefficients of reactivity.

### ***Principle***

- (55) *There is consideration in the design of nuclear reactors of inherent safety*

*characteristics that reduce the likelihood or consequences of accidents. Examples of inherent safety characteristics of nuclear reactors are temperature and void coefficients of reactivity, and inherent circulation for decay heat removal.*

## **NUCLEAR FUEL INTEGRITY**

5.9 Maintaining the integrity of nuclear fuel is fundamental to the safety of nuclear reactors and spent fuel stores. Loss of that integrity has occupational exposure implications, and if it causes or is coincident with a serious impairment of a confinement system or containment system, there are public exposure implications. Note that in addition to the principles in this section, Principle 32, which relates to damage to the core of a nuclear reactor, is relevant to maintaining nuclear fuel integrity.

### ***Principle***

- (56) *Facilities incorporating nuclear fuel are designed so that nuclear fuel integrity is maintained, in preference to mitigating the consequences of fuel melting, by the use of:*
- (a) *Emergency cooling and residual heat removal.*
  - (b) *Coolant inventory make-up.*
  - (c) *Other items that are important to safety (such as sources of power and ultimate heat sinks).*
  - (d) *A combination of any of the above.*

## **DEFENCE IN DEPTH LEVEL 2**

5.10 Defence in depth at level 2 is aimed at maintaining the intended operational states. This can be achieved using process control systems and/or other limiting systems, which take automatic action or display/alarm the need for operator action before the facility transgresses its domain of operational states. An objective of this section is to ensure that the domain of operational states is identified and that the facility is designed to operate safely within that domain.

## **RADIATION PROTECTION**

5.11 The radiation protection scheme of justification, limitation and optimisation from the recommendations of the National Health and Medical Research Council (NHMRC), the International Commission on Radiological Protection (ICRP) and the IAEA, is the basis for ARPANSA's approach to radiation protection. Effective dose limits are those in the ARPANS Regulations [6].

5.12 Limits on radiation doses arising from normal operation and anticipated operational occurrences are those of Regulation 59 of the ARPANS Regulations [6]. Limits on radiation dose are specified for occupational exposure and public exposure, which are all other exposures except exposures of patients as part of a medical procedure and exposures to natural background radiation. Occupationally exposed persons who do not work directly with a source of radiation should be protected to the same extent as

members of the public.

5.13 The radiation dose limits represent doses that are just acceptable to individuals. In addition to meeting the limits, the level of radiation protection for each source of radiation must be optimised so that the magnitude of individual doses and the number of people exposed are kept as low as reasonably achievable, economic and social factors being taken into account (ALARA). Radiation protection is considered to be optimised when the level of protection needed to further decrease individual or collective doses cannot be achieved without an unreasonable social or economic cost. The process of achieving optimised protection may be aided by calculations such as cost-benefit analysis.

5.14 An upper level of dose called the dose constraint should bound the optimisation of protection for each source. The constraint is used during optimisation of protection to allow for doses that might be received by individuals from other sources, and to promote good practice. Dose constraints for each source are chosen by the operating organisation and agreed with ARPANSA, and must be no greater than the relevant dose limit.

5.15 At a low level of dose, there is no requirement to show that it is reasonably achievable to increase radiation protection, and decrease doses, any further. Where assessments show that a given level of radiation protection will result in doses less than the levels set by ARPANSA, there is no need for a demonstration that the protection is optimised. Nevertheless, the dose assessment must be verified and all assumptions in making the assessment supported.

5.16 Radiation protection for occupational exposures should be achieved through controls on the source, environmental arrangements, such as ventilation, and personal protection for workers. The design of the facility and the implementation of a radiation protection program that describes procedural controls provide these controls.

5.17 Assessments of radiation doses to the public should consider all dose pathways. The assessments should identify critical groups, which are groups of individuals of similar characteristics and who receive the highest radiation doses from a particular source or dose pathway.

5.18 Radiation protection for public exposures should be achieved through controls on the source. At facilities, public exposure will generally be due to discharges of radioactive waste. Facilities should be designed and operated so that radioactive discharges are kept as low as reasonably achievable, and less than the limits on discharge set by ARPANSA.

### ***Principles***

(57) *Throughout the life of the facility, radiation doses arising from normal operation and anticipated operational occurrences do not exceed the effective dose limits in Regulation 59 of the ARPANS Regulations [6]:*

1. *The effective dose limit for occupational exposure is 20 mSv annually, averaged over 5 consecutive calendar years.*

2. *However, the effective dose for a person subject to occupational exposure must not, in a year, be greater than 50 mSv.*
3. *The effective dose limit for public exposure is 1 mSv annually.*
4. *The effective dose limit for an unborn child is to be consistent with the effective dose limit for public exposure.*

*Note: For the obligation imposed on female employees who are pregnant, see the National Standard for Limiting Occupational Exposure to Ionizing Radiation, which is a prescribed standard for regulation 62.*

- (58) *For each radiation source, the level of radiation protection provided is optimised so that individual and collective doses are kept ALARA.*
- (59) *The optimisation of radiation protection is bounded at the upper level by a dose constraint set by the operating organisation and agreed with ARPANSA, which allows for other occupational or public exposures and takes account of good practice at the facility and other similar, well managed facilities.*
- (60) *Where it has been demonstrated to the assessor that the annual radiation dose arising from a facility would be less than 2 mSv to any occupationally exposed person and 20 microSv to any member of the public, it is not necessary to consider further optimisation of radiation protection for the facility.*
- (61) *Radiation protection for occupational exposures is considered in the design and operation of the facility, and a radiation protection plan is implemented at the facility to ensure that radiation doses to workers are ALARA, and within dose constraints.*
- (62) *Radiation protection for public exposures is achieved through the design and operation of the facility to ensure that any radioactive discharges from a facility are ALARA, and within discharge limits set by ARPANSA.*

## **OPERATIONAL LIMITS AND SAFETY SYSTEM SETTINGS**

5.19 Limits for normal operation and anticipated operational occurrences are safety limits that are necessary to protect the integrity of barriers that guard against release of radioactivity.

5.20 The process control system and other safety-related systems at level 2 are required to keep the facility within the limits for normal operation and anticipated operational occurrences. The safety margin between these limits and the safety system setting minimises spurious trips by allowing for process variable or parameter fluctuations (noise), instrumentation drift, etc.

### ***Principles***

- (63) *Limits of normal operation and anticipated operational occurrences, and safety system settings including the minimum plant configuration, are determined from safety analyses.*

(64) *The facility is constrained within the safety system settings, or else is shutdown.*

## **INSPECTION, TESTING AND MAINTENANCE**

5.21 Inspection testing and maintenance is required at a facility to: confirm and maintain availabilities and reliabilities of systems at the levels used in the safety analysis, and to avoid common cause failure. Appropriate frequencies for inspection, testing and maintenance at a facility should be established to avoid degradation of safety that might occur if the frequencies are too low.

### ***Principle***

(65) *Inspection, testing and maintenance frequencies of items important to safety take account of the categorisation by safety significance of the items.*

## **MODIFICATIONS**

5.22 Modifications to equipment, procedures, documentation or operational conditions should be categorised according to their safety significance. Arrangements for the implementation of modifications should be in place to ensure that the design, manufacture, installation and commissioning of the modifications may be safely completed. The arrangements should include provisions for the appropriate internal and regulatory approvals at various stages of the modification.

### ***Principle***

(66) *Modifications to facilities are categorised according to their safety significance, and subject to controls which ensure they are implemented safely and with any required approvals.*

## **NUCLEAR MATERIAL**

5.23 In this document, the term 'nuclear material', defined in ARPANSA's glossary [3], includes fissile material, fertile material, moderator material, fission products, radioactive isotopes, and radioactive waste. It also includes other nuclear fuel cycle materials such as nuclear fuel and neutron control absorbers which are used for (or are wholly or partly attributable to) nuclear fission and other processes wherein a substance is subjected to bombardment by neutrons or ionizing radiation. The handling and storage of nuclear material requires special safety arrangements due to characteristics such as high radiotoxicity, generation of decay heat, and criticality hazards.

### ***Principles***

(67) *Suitable provisions, procedures and facilities exist for the safe transport, handling, treatment, discharge, storage and disposal of all nuclear material arising from operations at the facility.*

- (68) *Where nuclear material is stored prior to being discharged or disposed of as radioactive waste, there are suitable provisions and procedures for its interim containment.*
- (69) *Handling facilities are sufficiently flexible to cope with faulty fuel or containers, and material of non-standard physical or chemical composition.*
- (70) *The form, locations and quantities of nuclear material are specified, monitored and recorded.*
- (71) *Where maximum inventories of fissile material exceed quantities that ensure criticality safety, the safety analysis demonstrates that, for the particular geometry and other materials present, there is criticality safety under normal and abnormal conditions.*
- (72) *The safety analysis includes consideration of nuclear material and confirms compliance with the radiation dose limits specified in the 'Radiation Protection' section and Table 2 of this document.*

## **RADIOACTIVE WASTE**

5.24 The handling, storage, transport, discharge and disposal of any radioactive waste attributable to facilities similarly require special safety arrangements.

### ***Principles***

- (73) *Suitable arrangements, including waste management facilities, exist for the safe handling, storage, transport, discharge and disposal of any radioactive waste arising from operations at the facility. The arrangements are detailed in a radioactive waste management plan.*
- (74) *Where radioactive waste is stored prior to being discharged or disposed of, there are suitable provisions for its interim containment.*
- (75) *Handling facilities for radioactive waste are sufficiently flexible to cope with faulty containers, and radioactive waste of non-standard physical or chemical composition.*
- (76) *The form, locations and quantities of any radioactive waste or discharges, are specified, monitored and recorded. The quantity and activity of radioactive wastes generated, and discharged, are ALARA.*
- (77) *Where relevant, the safety analysis includes consideration of radioactive waste and confirms compliance with the radiation dose limits specified in the 'Radiation Protection' section and Table 2 of this document.*

## DECOMMISSIONING AND POST-DECOMMISSIONING

5.25 Depending on the type of facility, the quantity of radioactive waste to be handled during the decommissioning stage may be up to a factor of five times that for other principal stages in the life of the facility.

5.26 Where required, post-decommissioning activities ensure that the facility site and any buildings left intact can be safely released for the purpose stated in the decommissioning plan.

### *Principles*

- (78) *Where required, an updated decommissioning plan is submitted to ARPANSA as part of the decommissioning safety case.*
- (79) *Consistent with the chosen decommissioning option, the quantity of radioactive waste to be generated during decommissioning is ALARA.*
- (80) *Throughout the decommissioning stage, there is compliance with the principles specified in the 'Radiation Protection' section of this document.*
- (81) *Post-decommissioning, the operating organisation submits detailed post-decommissioning radiation surveillance reports to ARPANSA which describe the facility in its decommissioned state and demonstrate that radiation exposures are ALARA and the dose limits specified in the 'Radiation Protection' section of this document are not exceeded.*

## FACILITY LIFE MANAGEMENT

5.27 Consideration may be given to the possibility of extending the life of the facility beyond its original design life. Appropriate facility conditions should be maintained and data collected during the life of the facility to allow the safety case to remain current. In the case of nuclear reactors, this may include tests on irradiated sample coupons to determine the extent of irradiation damage.

***Principle***

- (82) *The operating organisation takes into account the safety effects of ageing on its facilities, by periodically and systematically performing life extension evaluations and actioning upgrades that are needed to maintain safety.*

**AUTHORISATION OF PERSONNEL**

5.28 The number of site personnel exposed to particular risks can be controlled by authorising access of personnel to certain designated areas according to their function.

***Principles***

- (83) *Site personnel are authorised according to their function and only those who need to be there to fulfil their function are allowed access to certain designated areas.*
- (84) *The quality assurance system procedures include the authorisation of personnel.*

**DEFENCE IN DEPTH LEVEL 3**

5.29 Although arrangements are made to control radiation exposure during operational states and to minimise the likelihood of an accident resulting from loss of control during operational states, there is a low probability that an accident may occur.

5.30 Accordingly, safety systems are provided at defence in depth level 3 to protect the facility against postulated design-basis accidents. The safety systems consist of active and passive systems and are aimed particularly at preventing damage to the facility and confining nuclear materials by maintaining the effectiveness of barriers.

5.31 The postulated accidents include those originating in the facility. In the case of nuclear reactors, examples are a loss of cooling, or a failure of a process control system that leads to a reactivity excursion.

**IDENTIFICATION OF SAFETY SYSTEMS**

5.32 The highly reliable systems that comprise safety systems, and the safety-related systems which have a lower grade of categorisation by safety significance but are important to safety, need to be clearly identified. This reduces the likelihood of human action that might contribute to common cause failures.

***Principles***

- (85) *Safety systems are distinguished by clear markings (for example, colour codes or fixed notices) so that they stand out in contrast to systems that are not important to safety.*

- (86) *Safety systems are additionally distinguished from safety-related systems by clear markings to emphasise their different categorisations by safety significance.*

## **MEASUREMENT OF PROCESS VARIABLES**

5.33 The safety margins between the safety system settings and the calculation model safety limit allow for different types of uncertainties, including calculation model uncertainties, instrument inaccuracies and drift, and time delays. As a precautionary arrangement aimed at avoiding additional uncertainty, safety systems should rely on directly measured rather than calculated process variable values.

### ***Principle***

- (87) *As far as reasonably practicable, process variables that are used in safety systems are measured directly, in contrast to being calculated using assumed relationships from other measurements, so that they detect the actual conditions that require safety action.*

## **REDUNDANCY, INDEPENDENCE AND DIVERSITY IN SYSTEMS IMPORTANT TO SAFETY**

5.34 As a minimum requirement for a safety system, no single fault should lead to failure of the system (single failure criterion).

5.35 There is a limit to the benefits of identical redundancy. Redundancy can be defeated by some common cause failures. Attention to the physical and functional independence of redundant safety subsystems and the use of diversity are very effective in addressing that weakness. This is particularly important for nuclear reactors. The provision of physical and functional independence and diversity between the levels of defence in depth results in a reduction of uncertainties and the susceptibility of structures, systems and components to common cause failures.

5.36 Physical separation is typically effected by spatial separation and by the use of barriers, and may be between redundant subsystems or between those and sources of potential environmental influences. Functional separation includes, for example, avoiding the sharing of process variable sensors across redundant subsystems.

5.37 Operational experience indicates that complete independence of redundant subsystems is practically unattainable. Residual dependence of identical redundant subsystems exists to some extent because of their physical form and because of the wide variety of external influences to which they are subjected during their lifetime. Whilst application of the principle of defence in depth may make up for that limitation in the implementation of independence, there is a need for the highest degree of physical and functional independence in redundant systems for which the grade of categorisation by safety significance is highest.

### ***Principles***

- (88) *Independence and diversity are provided between levels of defence in depth.*
- (89) *Safety systems have sufficient redundancy so that no single fault can lead to failure of the system, including during testing and maintenance and during shutdowns, when safety systems may be degraded.*
- (90) *The design of systems important to safety is subject to safety analyses to determine the required extent of redundancy.*

*The highest level of physical and functional independence and diversity is used in redundant systems where the safety significance is highest.*

- (91) *The highest degree of physical and functional independence is used in redundant systems where the safety significance is highest.*
- (92) *Redundant subsystems in safety systems are kept functionally and physically separate, from measurement of the process variable (avoiding common sensors) through to shutdown actuation.*
- (93) *Independence of redundant subsystems in safety systems is sufficiently effective under fire conditions.*
- (94) *Diversity is used in redundant safety systems, from measurement of the process variable through to shutdown actuation.*
- (95) *Electrical power supply systems and emergency power systems (for example, those that supply compressed air, steam or water), are among the systems to which the principles of redundancy, independence and diversity are applied.*
- (96) *Nuclear reactors have two diverse and independent shutdown systems.*

## **INDEPENDENCE OF PROCESS CONTROL SYSTEMS AND SAFETY SYSTEMS**

5.38 At nuclear reactors, independence between process control systems and safety systems is an important principle that has been emphasised since the early days of nuclear reactors. It is a major contributor to defence in depth, because of its effect on the reduction of common cause failures.

### ***Principles***

- (97) *Process control systems of nuclear reactors are kept functionally and physically separate from safety systems, from measurement of the process variable (avoiding common sensors) through to shutdown actuation, so that a system is not relied upon to perform both control and safety functions.*

- (98) *Independence of process control systems and safety systems is sufficiently effective in the event of fires.*

## UNPLANNED CRITICALITY

5.39 Criticality safety is a central safety issue wherever fissile material is present. With insufficient attention to criticality safety, a criticality accident might occur in the form of an unplanned reactivity excursion. Although that accident would manifest itself principally as heat in the fissile material, the associated ionizing radiation may be lethal to nearby personnel. Such personnel may not be aware that an accident has occurred. There may be no apparent damage; the only indication might be the sounding of radiation alarms.

### *Principles*

- (99) *For nuclear reactors, the safety analysis demonstrates that the reactor has sufficient shutdown reactivity margin under conditions of normal operation, anticipated operational occurrences and accident conditions to effect and maintain a shutdown state.*
- (100) *In the case of an arrangement of fissile material, there is a criticality analysis as part of the safety analysis, which demonstrates that sub-criticality is maintained by a suitable margin under conditions of normal operation and anticipated operational occurrences and accident conditions.*
- (101) *If required by the safety analysis, an effective detection and alarm of any reactivity event is used in the safety system to protect personnel against unplanned criticality.*

## FIRE PROTECTION

5.40 Fire events of internal and external origin have the potential to impair several levels of defence in depth at a facility.

### *Principles*

- (102) *The safety analysis includes a fire hazard assessment.*
- (103) *The following arrangements are implemented to an extent that is commensurate with the safety analysis:*
- (a) *Fire prevention arrangements in the design and operation of the facility.*
  - (b) *Early detection systems.*
  - (c) *Timely extinguishment arrangements which would not jeopardise safety by leakage or inadvertent operation.*
  - (d) *Fire protection barriers or other physical separation arrangements, and arrangements for manual fire fighting.*

*Safety systems that prevent fires, detect fires, or limit the consequences of fires (for example, by use of fire zones or fire barriers or fire suppression systems), are designed with sufficient capacity; their rupture or inadvertent operation does not jeopardise the operation of components, systems and structures important to safety.*

## **PROCESS PLANT**

5.41 Some items of process plant such as pumps, water supplies, and power sources that are not part of the safety system may be safety-related during accident conditions, and thus warrant special consideration.

### ***Principle***

- (104) *Whenever the categorisation by safety significance designates items of process plant as safety-related:*
- (a) *The principles of redundancy, independence, and diversity, including consideration of common cause failures, are applied to those items to the extent that is appropriate to their categorisation by safety significance.*
  - (b) *Safety analyses confirm that those items do not cause a design imbalance, that is, failures of the items do not contribute to risk disproportionately in comparison with other accidents.*

## **DISABLING/BYPASSING SAFETY SYSTEMS**

5.42 In the course of maintenance, testing or calibration activities, an operator may inadvertently (for example, by incorrectly calibrating a sensor or failing to restore a valve or piece of equipment to its functional state) or intentionally disable or bypass a safety system. This is a particularly important consideration during shutdowns. Provisions must be made to ensure that these acts do not adversely affect the safety of the facility.

### ***Principles***

- (105) *Temporarily disabling or bypassing part of a safety system is potentially unsafe and is avoided unless a special safety case is made. The design minimises the need for disabling or bypassing part or all of a safety system.*
- (106) *Special cases where disabling or bypassing part of a safety system has to be carried out temporarily require that:*
- (a) *The disabling or bypassing is addressed in the safety analysis.*
  - (b) *Testing confirms proper operation after removal of the disabling or bypassing.*
- (107) *As far as practicable, disabling or bypassing of redundant safety systems is carried out one at a time, so that the remaining redundant systems are capable of fulfilling their safety function.*

## PERFORMANCE TESTING

5.43 A performance failure of a safety system can result from a design oversight that testing repeatedly fails to detect because that system's performance may never have been tested under the accident conditions for which it was intended to function.

### *Principles*

(108) *To demonstrate satisfactory safety system performance, testing of safety systems emphasises performance failure aspects by simulating as faithfully as reasonably practicable the actual initiating event and conditions.*

(109) *Testing of safety systems, from measurement of the process variable through to shutdown actuation, is facilitated by:*

- (a) *The use of coincidence or equivalent technology.*
- (b) *The physical layout of the facility.*

## CONFINEMENT AND CONTAINMENT SYSTEMS

5.44 High hazard facilities such as nuclear reactors may have confinement systems or be housed in sturdy, reliable, long-term effective containment system buildings/structures.

5.45 A reliable, leak-tight, long-term effective containment system can be an important contributor to safety. In the case of nuclear reactors, the bulk of the fission products which may escape from a damaged core in the event of an accident may reach the inside of the containment building, but an effective containment system will limit the release of nuclear material to the environment.

5.46 This section addresses the highly reliable containment and confinement systems that may be required under design-basis accident conditions to prevent or mitigate the release of nuclear material.

### *Principles*

(110) *Where provided, the confinement system or the containment system prevents or mitigates the release of nuclear material under accident conditions.*

(111) *The design of a confinement system or a containment system addresses heat removal and leak tightness under transient conditions, and takes into account sealing and closure times of penetrations and ventilation systems.*

(112) *The degree of leak tightness of the containment or confinement is determined from the safety analysis, which takes into account the inventory of volatile radionuclides and related effects such as the temperature and pressure which may exist under design-basis accident conditions.*

## DEFENCE IN DEPTH LEVEL 4

5.47 The purpose of defence in depth at level 4 is to invoke accident management arrangements to limit the progression of a beyond-design-basis accident and to mitigate its consequences. To an extent that depends on the conditions and with assistance from equipment, it is possible for operators to diagnose the status of the facility and to take action management arrangements. Accident management arrangements may include maintaining or restoring at least one barrier for the confinement of radioactive material.

### *Principles*

- (113) *Where required, accident management arrangements are based on the outcomes of the safety analysis.*
- (114) *Accident management is not relied upon at the expense of good design at defence in depth levels 1-3.*
- (115) *Accident management arrangements at a nuclear reactor attempt to restore heat removal from the core of the facility and effect long-term core cooling to maintain the integrity of the confinement system or containment system by preventing loads on the systems in excess of those permitted.*
- (116) *Instrumentation important for monitoring the status of the facility and to undertake effective accident management arrangements is regularly inspected, tested and maintained.*

## DEFENCE IN DEPTH LEVEL 5

5.48 Defence in depth at level 5 addresses mitigation of the off-site radiological consequences that might result from the highly improbable failure of defence in depth at levels 1-4. The siting of facilities contributes to defence in depth level 5 to protect the public and the environment from such accidents. In addition, off-site emergency response arrangements enhance the effectiveness of the resources available by the involvement of off-site groups. By definition, provisions for siting and off-site emergency response do not apply to Hazard Category F1 facilities.

5.49 The design of the facility must take in account the characteristics of the site. Principles related to the impact of the site on the design of the facility are included in the section Defence in Depth Level 1.

5.50 Siting should be considered early in the planning process of the facility, perhaps well before the detailed design is known. In this case, the initial siting assessment can only be based on a design concept, or reference design, for the facility. Where the siting is based on a reference design, the validity of the initial siting assessment must be checked against the detailed design when it is finalised, using the PSAR.

## SITING ASSESSMENT

5.51 Since the facility is designed so that the off-site health consequences of design-basis accidents are minor, a severe accident, called the Reference Accident, is postulated. This accident is established for the reference design of the facility, assuming some degraded performance of the safety systems. The development of a Reference Accident is described in more detail in ARPANSA's siting guideline [5].

5.52 For the purposes of the siting assessment, the consequences of the Reference Accident must be determined using more conservative assumptions than would be used for the analysis of beyond-design-basis accidents. This provides a high degree of confidence that the consequences of the Reference Accident would be unlikely to be exceeded by those of any actual accident at the facility. For the site to be approved by ARPANSA, the calculated consequences must be no greater than the criteria included in the siting principles below.

5.53 The characteristics of the site for a facility such as its seismology, geology, meteorology, and other characteristics such as the use of land around the site, may impact the safety of the facility. These factors could give rise to events that lead to accidents or could impact arrangements for waste discharge and emergency response.

## SITING PRINCIPLES

5.54 The intention of this section is to ensure that, following the Reference Accident:

- The imposition of emergency interventions would be feasible.
- The collective effective dose to the most exposed population would be less than the specified limit.
- The contamination of the environment would not be so extensive as to restrict the long-term use of land around the site.

5.55 In calculating the collective effective dose to a population arising from the Reference Accident, no allowance should be made for the aversion of individual doses by short-term countermeasures such as sheltering, administration of stable iodine and evacuation. Individual doses that could be readily averted by medium and long-term countermeasures such as restrictions on food supplies and decontamination should not be included in the calculation.

5.56 The population considered when determining the collective effective dose must represent the worst case in terms of location, but should also exclude individuals whose dose is small compared to those close to the site. While recognising that all radiation dose is assumed to carry some risk of harmful effects, it is considered that a collective dose due to many persons each receiving a very small dose, should be treated differently to the same collective dose due to a few persons who each receive a much higher dose.

5.57 To ensure that the collective effective dose is a relevant representation of societal risk, individual doses below some cut-off value should be excluded from the calculation

of collective dose. This cut-off may be determined by the population distribution of the area around the site, topographical or geographical features, or based on a level of dose that is considered to represent an acceptable level of risk in the circumstances. Collective dose should be calculated and documented within bands of individual dose (such as between 10 and 100 mSv, etc) and a rationale provided for the choice of such bands and the minimum cut-off.

### ***Principles***

- (117) *Where required, the siting assessment is performed early in the planning stages of a proposed facility, to determine whether the selected site provides adequate protection of individuals, society and the environment against hazards arising from potential accidents at the facility.*
- (118) *Where a detailed design is not yet established, the siting assessment is based on a reference design for the facility. The assessment determines the consequences of a postulated accident called the Reference Accident, which involves some degradation of the safety systems of the reference design for the proposed facility, and includes conservative assumptions on the release of radioactive materials.*
- (119) *The consequences of the Reference Accident are determined for meteorological conditions which result in the maximum consequences of the accident, but which occur no less than 10% of the time, and the effect of rain is considered. For these consequences, it is determined that:*
- (a) *Emergency intervention would be feasible at any location around the site, at the intervention levels agreed with ARPANSA.*
  - (b) *The maximum collective effective dose would be less than 200 person.Sv.*
  - (c) *The long-term use of any land surrounding the site would not be disrupted due to radioactive contamination.*
- (120) *In calculating collective effective doses, no allowance is made for the imposition of short-term emergency interventions. A calculation cut-off is set so those individual doses representing very low levels of risk are not included in the collective dose.*
- (121) *Where the siting assessment has been based on a reference design of a proposed facility, the Reference Accident is compared to the analyses of the final design in the PSAR, to check the validity of the siting assessment.*

## **OFF-SITE EMERGENCY RESPONSE**

5.58 Depending on the type of facility, off-site emergency response arrangements may be important in the event that the facility experiences beyond-design-basis accident conditions. The operating organisation has the responsibility for ensuring the availability and effectiveness of any off-site emergency response arrangements.

5.59 It is important that the public is aware of any off-site emergency arrangements. The arrangements should be documented in an emergency plan for the facility that is

periodically exercised, reviewed and updated. Consistent with its role as a regulatory body, ARPANSA does not have any responsibility for implementing or executing any off-site emergency response arrangements in the event of an accident.

5.60 For details of off-site services such as transportation and communication services and the availability of skilled labour, that may be relevant to off-site emergency response, reference should be made to ARPANSA's siting guideline [5].

### *Principle*

(122) *Where off-site emergency response may be required, the operating organisation prepares and periodically updates an emergency plan which:*

- (a) *Is prepared in consultation with public authorities that act on the advice of the operating organisation and ARPANSA.*
- (b) *Is based on the consequences of accidents considered in the safety analysis report of the facility, which may be complemented by a probabilistic safety analysis.*
- (c) *Considers a range of intervention arrangements.*
- (d) *Complies with relevant legislation and national and international agreements.*

5.61 For emergency planning purposes, the generic intervention levels for urgent protective arrangements recommended by the IAEA [7] should be used.

**Table 3. IAEA recommended generic intervention levels for urgent protective arrangements**

Protective action	Generic intervention level (dose avertable by the protective action) <sup>a,b</sup>
Sheltering	10 mSv <sup>c</sup>
Evacuation	50 mSv <sup>d</sup>
Iodine prophylaxis	100 mGy <sup>e</sup>

<sup>a</sup> These levels are of avertable dose, that is, the action should be taken if the dose that can be averted by the action, taking into account the loss of effectiveness due to any delays or for other practical reasons, is greater than the figure given.

<sup>b</sup> The levels in all cases refer to the average over suitably chosen samples of the population, not to the most exposed individuals. However, projected doses to groups of individuals with higher exposures should be kept below the thresholds for deterministic effects.

<sup>c</sup> Sheltering is not recommended for longer than 2 days. Authorities may wish to recommend sheltering at lower intervention levels for shorter periods or so as to facilitate further countermeasures, for example, evacuation.

<sup>d</sup> Evacuation is not recommended for a period of longer than 1 week. Authorities

may wish to initiate evacuation at lower intervention levels, for shorter periods and also where evacuation can be carried out quickly and easily, for example, for small groups of people. Higher intervention levels may be appropriate in situations in which evacuation would be difficult, for example, for large population groups or with inadequate transport.

- <sup>e</sup> Avertable dose to the thyroid. For practical reasons, one intervention level is recommended for all age groups.

### ***Principle***

(123) *Emergency response exercises together with other test and review activities are conducted selectively to:*

- (a) *Test emergency equipment.*
- (b) *Assess the adequacy of site personnel resources.*
- (c) *Test communications.*
- (d) *Confirm the definition of emergency planning zones and the arrangements that apply to each zone.*
- (e) *Confirm the viability of intervention arrangements to protect the public.*
- (f) *Confirm the availability of suitable emergency public information systems.*
- (g) *Confirm the availability of required external aid groups and facilities, including those for provision of medical aid to treat injured contaminated persons.*
- (h) *Confirm the adequacy of the interface with government, local authority and off-site agencies.*
- (i) *Monitor and improve, as appropriate, public awareness that there are a number of off-site arrangements which can be invoked in the event that a facility experiences beyond-design-basis accident conditions.*

## 6 APPENDIX

### INTERNATIONAL CONVENTION ON NUCLEAR SAFETY

6.1 Australia signed the International Convention on Nuclear Safety<sup>2</sup>, becoming a Contracting Party, in December 1996. The Convention applies to land-based nuclear power plants. ARPANSA has been designated by the Commonwealth Government to take primary responsibility for Australia's obligations under the Convention, working in consultation with other Australian agencies. A Contracting Party's compliance with the Convention's terms and obligations is reported internationally, Convention article-by-Convention article, in accordance with agreed reporting guidelines.

6.2 Although Australia does not have any nuclear power plants, and none are planned, ARPANSA views the preparation of Convention compliance reports as an opportunity for Australia to:

- Assess the regulatory framework and safety standards of Australia's research reactors from the point of view of the sound safety practices promoted by the Convention.
- Promote and contribute to a similarity of approach to nuclear safety worldwide.
- Promote transparency of nuclear operations within Australia and other countries.
- Better understand the Convention obligations voluntarily accepted by Contracting Parties, thereby facilitating Australia's review of the National Reports of other countries, including neighbouring countries.

## 7 REFERENCES

- [1] International Atomic Energy Agency. *Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1*, International Safety Advisory Group Report INSAG-12. Vienna, 1999.
- [2] International Atomic Energy Agency. *Basic Safety Principles for Nuclear Power Plants*, International Nuclear Safety Advisory Group Report Safety Series No. 75-INSAG-3. Vienna, 1988.
- [3] Australian Radiation Protection and Nuclear Safety Agency. *Glossary of Terms Used for Regulatory Assessment*. RB-STD-61-01 Rev 0. Sydney, October 2001.
- [4] International Atomic Energy Agency. *Defence in Depth in Nuclear Safety*, International Safety Advisory Group Report INSAG-10. Vienna, 1996.

---

<sup>2</sup> The "Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management" was signed by Australia in November 1998, however the steps towards ratification are currently in progress.

- [5] Australian Radiation Protection and Nuclear Safety Agency. *Criteria for the Siting of Controlled Facilities*, Regulatory Guideline RG-4. Sydney, April 1999.
- [6] Australian Radiation Protection and Nuclear Safety Regulations 1999, Statutory Rules 1999 No. 37 made under the Australian Radiation Protection and Nuclear Safety Act 1998.
- [7] International Atomic Energy Agency. *Intervention Criteria in a Nuclear or Radiation Emergency*. Safety Series No.109. Vienna, 1994.
- [8] Nuclear Installations Inspectorate, Health and Safety Executive. *Safety Assessment Principles for Nuclear Plants*. United Kingdom, 1992.
- [9] Department of Urban Affairs and Planning. *Multi-level Risk Assessment*. Sydney, 1997.
- [10] Nuclear Installations Inspectorate, Health and Safety Executive. *Tolerability of Risk from Nuclear Power Stations*. United Kingdom, 1988.

## 8 BIBLIOGRAPHY

Australian Radiation Protection and Nuclear Safety Agency. *Expectations Guideline*, RG-13. December 2000.

Australian Radiation Protection and Nuclear Safety Regulations 1999 Statutory Rules No. 37, 1999.

Australian Radiation Protection and Nuclear Safety Act 1998 No. 133, 1998.

Cassidy K. *Developments in HSE Risk Criteria*, Major Hazards Assessment Unit, HSE. United Kingdom, 1997.

International Atomic Energy Agency. *Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Facilities*, Safety Series No. 50-C/SG-Q. Vienna, 1996.

International Atomic Energy Agency. *Operational Limits and Conditions of Research Reactors*, Safety Series No.35-G6. Vienna, 1995.

Atomic Energy Control Board, Advisory Committee on Nuclear Safety. *Proposed Quantitative Approach to Safety for Nuclear Power Plants in Canada*. INFO-0568(E), ACNS-20. Canada, 1995.

National Health and Medical Research Council (NHMRC). *Recommendations for Limiting Exposure to Ionizing Radiation*. NOHSC:3022 (1995) and *National Standard for Limiting Occupational Exposure to Ionizing Radiation*. NOHSC:1013 (1995), Radiation Health Series No.

39. Australia, 1995.

International Atomic Energy Agency. *International Basic Safety Standards for Protection Against Ionizing Radiation and for the Safety of Radiation Sources*. Vienna, 1994.

International Atomic Energy Agency. *Safety in the Utilization and Modification of Research Reactors*. Safety Series No.35-G2. Vienna, 1994.

International Atomic Energy Agency. *Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report*. Safety Series No.35-G1. Vienna, 1994.

International Atomic Energy Agency. *Code on the Safety of Nuclear Research Reactors: Operation*. Safety Series No. 35-S2. Vienna, 1992.

International Atomic Energy Agency. *Code on the Safety of Nuclear Research Reactors: Design*. Safety Series No.35-S1. Vienna, 1992.

International Atomic Energy Agency. *The Safety of Nuclear Power*. Safety Series No. 75-INSAG-5. Vienna, 1992.

Department of Energy. *Hazard Categorisation and Accident Analysis Techniques for Compliance with DOE Order 5480.23*. Nuclear Safety Analysis Reports, DOE-STD-1027-92. Washington DC, 1992.

International Atomic Energy Agency. *Safety Culture*. Safety Series No 75-INSAG-4. Vienna, 1991.

Ernst PC, French PM, Axford DJ, Snell VG. *Development of Small Reactor Safety Criteria in Canada*. Paper IAEA-SM-310/93 presented at International Symposium on Research Reactor Safety, Operations and Modifications. Chalk River, Ontario, 1989.

International Commission on Radiological Protection. *Recommendations of the ICRP*. Publication No. 60, Pergamon Press. Oxford, 1960.

National Health and Medical Research Council (NHMRC). *Intervention in Emergency Situations Involving Radiation Exposure*. Radiation Health Series No. 32. Australia, 1990. Under Revision.

## 9 INDEX

abnormal occurrence, 15  
Abnormal occurrence, 7  
abnormal operation, 8, 9, 13, 15  
access, 9, 16, 23  
accident conditions, 9, 26, 27, 28, 31, 33  
accident management, 16, 29  
Accident management, 4, 29  
accident precursor, 15  
accountability, 5  
activity, 6, 14, 22  
actuation, 25, 28  
age, 33  
ageing, 13, 23  
ALARA, 7, 8, 18, 19, 22  
alarm, 17, 26  
anticipated operational occurrence, 4, 9, 10, 15, 18, 19, 20, 26  
applicant, 7  
application, i, vi, 1, 7, 8, 24  
approval, 14  
ARPANS Act, iii, vi, 1  
arrangement of fissile material, 26  
as low as reasonably achievable, 7, 8, 10, 11, 12, 14, 18, 19  
assessor, 19  
atmosphere, 14  
atmospheric, 6  
authorisation, 23  
authorisation of personnel, 23  
automatic, 17  
availability, 16, 31, 32, 33  
avertable dose, 32  
Avertable dose, 33  
background radiation, 18  
barrier, 12, 29  
best-estimate, 6, 10, 12  
Best-estimate, 6  
beyond-design-basis accident, 2, 4, 6, 10, 12, 13, 15, 29, 30, 31, 33  
Beyond-design-basis accident, 10, 11  
boundary, 10, 15  
building, 15, 28  
bypass, 27  
bypassing, 27  
calculation model, 24  
calculation model safety limit, 24

calibration, 27  
categorisation by safety significance, 8, 14, 15, 20, 23, 24, 27  
certification, 6  
chemical, 21, 22  
cladding, 12, 15  
classification, 10  
cliff-edge, 13  
codes, iii, 23  
codes of practice, iii  
coincidence, 28  
collective dose, 18, 19, 30, 31  
Collective dose, 31  
collective effective dose, 30, 31  
combinations of failures, i, 3  
commissioning, 15, 20  
common cause, 6, 9, 20, 23, 24, 25, 27  
Common cause, 13  
common cause failure, 6, 9, 20, 23, 24, 25, 27  
Common cause failure, 13  
communication, 2, 16, 32  
communication system, 16  
compressed air, 25  
computer-based, 9  
confine, 15  
confinement system, 17, 28, 29  
conservatism, 9, 11  
conservative, 4, 6, 12, 15, 30, 31  
Conservative, 4, 6  
construction, 4, 15  
containment system, 17, 28, 29  
contaminated, 33  
contamination, 30, 31  
control absorber, 21  
control room, 16  
control system, 17, 20, 23, 25, 26  
controlled apparatus, iii  
controlled facility, iii, 1, 8  
controlled material, iii, 9, 10  
Coolant, 17  
cooling, 13, 17, 23, 29  
core, 6, 12, 13, 17, 28, 29  
Council, 18, 35, 36  
critical, 9, 18  
critical group, 18  
criticality, 9, 15, 21, 26  
Criticality, 26  
criticality accident, 26  
criticality analysis, 26

criticality control, 15  
criticality safety, 21, 26  
Criticality safety, 26  
damage to the core, 17  
decay, 17, 21  
decay heat, 17, 21  
decommissioning, 8, 14, 15, 22  
decommissioning plan, 14, 22  
decontamination, 30  
defence in depth, i, v, 1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 15, 17, 23, 24, 25, 26, 29  
Defence in depth, i, v, 2, 3, 15, 17, 23, 29  
degradation, 20, 31  
demography, 16  
design, 2, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, 22, 25, 26, 27, 28, 29, 30, 31  
design bases, 9  
design modification, 7  
design specifications, 6  
Design specifications, 7  
design-basis, 2, 4, 6, 8, 9, 10, 12, 13, 15, 23, 28, 30  
Design-basis, 10, 11  
design-basis accident, 2, 4, 6, 9, 10, 12, 13, 15, 23, 28, 30  
Design-basis accident, 10, 11  
design-basis accident conditions, 9, 28  
detect, 4, 24, 27, 28  
deterministic, 6, 10, 12, 32  
Deterministic, 12  
deterministic analysis, 12  
disable, 27  
disabling, 27  
discharge, 5, 19, 21, 30  
display, 2, 17  
disposal, 21  
diverse, i, 3, 9, 25  
diversity, 13, 15, 24, 25, 27  
Diversity, 25  
domain of operational states, 17  
dose, iii, 7, 8, 9, 11, 14, 18, 19, 21, 22, 30, 31, 32  
Dose, 18  
dose assessment, 18  
dose constraint, 18, 19  
Dose constraint, 18  
dose limit, iii, 7, 8, 9, 14, 18, 19, 21, 22  
Economic analyses, 2  
economic and social factors, 18  
effective dose, 11, 19, 30, 31, 32  
Effective dose, 18  
Electrical power supply system, 25  
emergency core cooling, 13

emergency core cooling system, 13  
emergency equipment, 33  
emergency plan, 32, 33  
emergency planning zones, 33  
emergency power system, 25  
emergency preparedness, 7  
emergency public information system, 33  
emergency response, 3, 4, 10, 16, 17, 29, 30, 31, 32  
Emergency response, 33  
Energy, i, v, 1, 34, 35, 36  
environment, iii, vi, 2, 10, 14, 15, 28, 29, 30, 31  
environmental, 5, 13, 18, 24  
environmental conditions, 13  
equipment, i, 3, 7, 16, 20, 27, 29, 33  
ergonomic, 16  
evacuation, 30, 33  
Evacuation, 32, 33  
event, 5, 26, 28, 31, 32, 33  
experience, i, 4, 5, 7, 24  
exposure, 10, 18, 19, 23  
Exposure, 19, 35, 36  
external, 9, 10, 13, 24, 26, 33  
external event, 10, 13  
external hazard, 9  
facility licence, i  
failure, 23  
fault, 11, 13, 24, 25  
fault analysis, 11  
fault tolerant, 13  
feedback, 4, 5, 7  
Feedback, 7  
Feedback of experience, 7  
feedback of operational experience, 4, 7  
Feedback of operational experience, 7  
fertile material, 20  
financial, 5  
fire, 9, 25, 26, 27  
Fire, 26  
Fire protection, 26  
fire suppression, 27  
fire zone, 27  
fissile material, 20, 21, 26  
fission product, 11, 20, 28  
flooding, 9  
food, 30  
frequency, 6, 9, 10, 11, 12, 13  
FSAR, 8  
fuel, v, 12, 15, 17, 21

Fuel, 34  
fuel cladding, 12, 15  
fuel integrity, 17  
fuel melt, 17  
functional independence, 24, 25  
Functional separation, 24  
geology, 16, 30  
glossary, 1, 20  
Glossary, 34  
harm, v  
harmful effects of radiation, iii, vi  
hazard, v, 3, 7, 8, 10, 11, 14, 26, 28  
Hazard, 8, 10, 12, 13, 29, 36  
hazard categorisation, 7, 8, 14  
heat removal, 12, 17, 28, 29  
hierarchy, i, 3  
highly reliable system, 23  
historical records, 5  
historical records system, 5  
human, i, 3, 5, 6, 9, 15, 16, 23  
Human, 13, 15  
human activity, 6  
human factor, 9, 16  
Human factor, 13, 15  
human performance, 5  
hydrology, 16  
IAEA, i, 2, 18, 32  
ICRP, 18, 36  
implementation, i, 3, 7, 10, 15, 18, 20, 24  
importance, i, iii, 1, 2, 4, 15  
important to safety, 5, 9, 16, 17, 23, 25, 27  
improbable, 6, 10, 11, 29  
inadvertent operation, 26, 27  
independence, 15, 24, 25, 27  
Independence, 25, 26  
independent assessment, 9  
independent review, 5  
individuals, v, 2, 18, 30, 31, 32  
Individuals, 2  
inherent, 5, 9, 15, 16, 17  
inherent circulation, 17  
inherent safety characteristic, 15, 16, 17  
inherent safety characteristics, 15, 16, 17  
initiating event, 9, 10, 16, 28  
initiation, 16  
injury, i, 3  
inspection, 7, 15, 16, 20  
Inspection, 20

instrumentation, 20  
Instrumentation, 29  
integrity, 5, 9, 12, 17, 19, 29  
interface, 33  
interim, 21  
internal, v, 9, 10, 13, 20, 26  
internal fault, 13  
international best practice, i, iii, v, 2  
International Convention on Nuclear Safety, 2, 34  
international standards, 1, 15  
intervention, 12, 31, 32, 33  
Intervention, 35, 36  
intervention level, 31, 32, 33  
inventories, 21  
inventory, 11, 17, 28  
inventory make-up, 17  
iodine, 30  
Iodine, 32  
ionizing radiation, 21, 26  
irradiated, 22  
items important to safety, 20  
layout, 16, 28  
leak tightness, 28  
leakage, 26  
licence, i, 5, 7, 8, 14  
life extension, 15, 23  
limiting system, 4, 17  
long-term, 28, 29, 30, 31  
maintenance, 5, 6, 7, 9, 13, 15, 20, 25, 27  
Maintenance, 16  
margin, 8, 20, 26  
markings, 23, 24  
medical, 18, 33  
Medical, 18, 35, 36  
members of the public, 18  
meteorological, 31  
meteorology, 16, 30  
microSv, 19  
minimum plant configuration, 20  
mitigate, 4, 28, 29  
Mitigate, 4  
mitigation, 3, 4, 7, 29  
moderator, 20  
modification, 1, 5, 15, 20  
Modification, 36  
monitoring, 14, 29  
mSv, 11, 19, 31  
natural, 18

Natural, 16  
NHMRC, 18, 35, 36  
normal operation, 8, 9, 10, 15, 18, 19, 20, 26  
nuclear facility, 7  
nuclear fuel, 12, 17, 20  
nuclear fuel cycle, 20  
nuclear installation, 1  
nuclear material, 15, 20, 21, 23, 28  
nuclear power, v, 1, 34  
nuclear power plant, v, 1, 34  
nuclear reactor, 1, 6, 9, 11, 12, 13, 15, 16, 17, 22, 23, 24, 25, 26, 28, 29  
Nuclear reactor, 25  
nuclear safety, iii, 34  
occupational exposure, 17, 18, 19  
Occupationally exposed persons, 18  
off-site, 3, 10, 11, 12, 16, 29, 30, 31, 32, 33  
Off-site, 4  
off-site emergency response, 3, 10, 29, 31, 32  
Off-site emergency response, 4  
operating organisation, i, iii, 1, 2, 4, 5, 6, 7, 8, 12, 14, 18, 19, 22, 23, 31, 32  
Operating organisation, 2, 5  
operation, 7, 8, 9, 10, 12, 13, 15, 18, 19, 20, 26, 27  
Operation, 36  
operational limits, 7, 9  
operational limits and conditions, 7, 9  
operational states, 4, 15, 17, 23  
operator, 7, 16, 17, 27  
operator action, 16, 17  
passive system, 23  
performance failure, 13, 28  
performance testing, 7, 13  
periodic review, 5, 14  
Periodic review, 13, 14  
periodic testing, 7  
physical separation, 26  
Physical separation, 24  
pool, 15  
post-decommissioning, 22  
Post-decommissioning, 22  
power supply, 25  
power supply system, 25  
prescribed limit, 2  
pressure, 15, 28  
priority, 2  
probabilistic, 32  
Probabilistic, 10, 12, 13  
probabilistic safety analysis, 32  
Probabilistic safety analysis, 10

probability, 23  
procedure, 6, 18  
process control, 17, 20, 23, 25, 26  
Process control, 4, 25  
process control system, 17, 20, 23, 25, 26  
Process control system, 25  
process plant, 27  
process variables, 24  
progression, 4, 6, 29  
proven design, 4, 6, 15  
PSA, 8, 10, 12, 13, 29, 31  
PSAR, 8, 29, 31  
public, i, v, vi, 1, 3, 10, 11, 12, 13, 14, 15, 17, 18, 19, 29, 31, 32, 33  
public exposure, 17, 18, 19  
QA, 6, 14  
QA program, 6  
qualification, 5  
quality assurance, 4, 5, 7, 9, 23  
Quality assurance, 6  
radiation, iii, vi, 1, 5, 7, 8, 9, 11, 14, 17, 18, 19, 21, 22, 23, 26, 30  
Radiation, 1, iii, 7, 8, 9, 14, 18, 19, 21, 22, 34, 35, 36  
radiation alarm, 26  
radiation exposure, 7, 8, 22, 23  
radiation protection, iii, 17, 18, 19  
Radiation protection, 18, 19  
radiation protection plan, 19  
radiation source, 19  
radioactive, 9, 10, 14, 18, 19, 20, 21, 22, 29, 31  
Radioactive, 34  
radioactive material, 10, 14, 29, 31  
radioactive waste, 9, 19, 20, 21, 22  
radioactive waste management, 21  
radioactive waste management plan, 21  
radioactivity, 14, 19  
radioisotope production, v  
radiological, 2, 4, 14, 29  
Radiological, 18, 36  
radiological consequences, 2, 4, 29  
rain, 31  
reactivity, 9, 12, 17, 23, 26  
reactivity excursion, 12, 23, 26  
reactivity transient, 9  
records, 5, 14  
redundancy, 24, 25, 27  
Redundancy, 24  
redundant, 6, 16, 24, 25, 27  
Redundant, 25  
Reference Accident, 10, 30, 31

regulatory assessment, i, iii, v, vi, 1, 7, 8, 15  
regulatory assessment process, 7, 8, 15  
regulatory body, 32  
regulatory document, iii  
regulatory framework, iii, 34  
release, 10, 19, 28, 31  
reliability, 6, 9, 13, 16  
removal, 12, 17, 27, 28, 29  
reporting, 34  
research reactor, v, 34  
residual heat, 17  
residual heat removal, 17  
resources, 5, 10, 12, 29, 33  
responsibility, 1, 2, 4, 5, 31, 32, 34  
risk, 6, 9, 10, 11, 12, 13, 27, 30, 31  
Risk, 35  
safety analysis, i, iii, 1, 3, 7, 8, 9, 10, 12, 13, 14, 20, 21, 22, 26, 27, 28, 29, 32  
Safety analysis, 7  
safety analysis report, i, 7, 8, 32  
Safety analysis report, 7  
safety case, 7, 8, 14, 22, 27  
Safety case, 7  
safety culture, i, v, 1, 2, 4, 7  
Safety culture, v, 2, 4  
safety function, 13, 26, 27  
safety issues, v, 2  
safety limit, 7, 8, 9, 10, 11, 12, 13, 19, 24  
Safety limit, 11  
safety margin, 6, 10, 20, 24  
safety objective, 10, 11, 12  
Safety objective, 11  
safety research, 5  
safety significance, 8, 14, 15, 20, 23, 24, 25, 27  
safety system, 7, 9, 10, 13, 20, 23, 24, 25, 26, 27, 28, 30, 31  
Safety system, 4, 16, 23, 24, 25, 27  
safety system performance, 7, 28  
safety system setting, 20, 24  
safety system settings, 20, 24  
safety-related, 20, 23, 24, 27  
security, 5, 9  
seismology, 16, 30  
sensitivity, 12  
sensor, 27  
separation, 24, 26  
serious accident, 15  
services, 13, 16, 32  
severe, 10, 30  
severe accident, 30

sharing, 24  
sheltering, 30, 32  
Sheltering, 32  
shutdown, 10, 13, 14, 20, 25, 26, 28  
shutdown reactivity margin, 26  
shutdown system, 13, 25  
significant consequence, 8  
single failure, 24  
single failure criterion, 24  
site, 8, 10, 14, 15, 16, 22, 23, 29, 30, 31, 33  
Site, 23  
site characteristics, 16  
site personnel, 14, 23, 33  
Site personnel, 23  
siting, 3, 10, 15, 16, 29, 30, 31, 32  
Siting, 29, 35  
societal risk, 30  
software, 9, 15  
source of radiation, 18  
source term, 6  
spent fuel, 17  
spent fuel store, 17  
spurious, 20  
stage, 8, 9, 16, 22  
stages in the life of the facility, 6, 8, 9, 14, 22  
standards, 1, 5, 15, 34  
Standards, 15, 36  
steam, 25  
storage, 21  
stress, 16  
structural, 12  
structure, v, 8  
sub-criticality, 26  
sudden failure, 9  
surveillance, 4, 22  
survey, 14  
systematic, 16  
task, 7, 9  
temperature, 17, 28  
tested, 28, 29  
testing, 7, 15, 20, 25, 27, 28  
Testing, 27, 28  
thyroid, 33  
trained, 14  
training, 5, 13, 15  
transient, 9, 28  
transport, 6, 15, 21, 33  
transportation, 16, 32

ultimate heat sink, 17  
uncertainties, 6, 24  
Uncertainties, 13  
uncertainty, 24  
unplanned criticality, 26  
valve, 27  
ventilation, 18, 28  
ventilation system, 28  
verification, 5, 9  
void coefficient, 17  
vulnerability, 6  
waste, v, 9, 16, 19, 20, 21, 22, 30  
Waste, 34  
waste management, v, 21  
water supplies, 27  
website, vi