

# IAEA SAFETY STANDARDS SERIES

## Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants

### SAFETY GUIDE

No. NS-G-1.9



**IAEA**  
International Atomic Energy Agency

# IAEA SAFETY RELATED PUBLICATIONS

## IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

**Safety Fundamentals** (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

**Safety Requirements** (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

**Safety Guides** (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

[www-ns.iaea.org/standards/](http://www-ns.iaea.org/standards/)

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

## OTHER SAFETY RELATED PUBLICATIONS

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

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series**, the **Radiological Assessment Reports Series**, the **INSAG Series**, the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series**, the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

**DESIGN OF THE REACTOR  
COOLANT SYSTEM AND  
ASSOCIATED SYSTEMS IN  
NUCLEAR POWER PLANTS**

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN	GUATEMALA	PERU
ALBANIA	HAITI	PHILIPPINES
ALGERIA	HOLY SEE	POLAND
ANGOLA	HONDURAS	PORTUGAL
ARGENTINA	HUNGARY	QATAR
ARMENIA	ICELAND	REPUBLIC OF MOLDOVA
AUSTRALIA	INDIA	ROMANIA
AUSTRIA	INDONESIA	RUSSIAN FEDERATION
AZERBAIJAN	IRAN, ISLAMIC REPUBLIC OF	SAUDI ARABIA
BANGLADESH	IRAQ	SENEGAL
BELARUS	IRELAND	SERBIA AND MONTENEGRO
BELGIUM	ISRAEL	SEYCHELLES
BENIN	ITALY	SIERRA LEONE
BOLIVIA	JAMAICA	SINGAPORE
BOSNIA AND HERZEGOVINA	JAPAN	SLOVAKIA
BOTSWANA	JORDAN	SLOVENIA
BRAZIL	KAZAKHSTAN	SOUTH AFRICA
BULGARIA	KENYA	SPAIN
BURKINA FASO	KOREA, REPUBLIC OF	SRI LANKA
CAMEROON	KUWAIT	SUDAN
CANADA	KYRGYZSTAN	SWEDEN
CENTRAL AFRICAN REPUBLIC	LATVIA	SWITZERLAND
CHILE	LEBANON	SYRIAN ARAB REPUBLIC
CHINA	LIBERIA	TAJKISTAN
COLOMBIA	LIBYAN ARAB JAMAHIRIYA	THAILAND
COSTA RICA	LIECHTENSTEIN	THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
CÔTE D'IVOIRE	LITHUANIA	TUNISIA
CROATIA	LUXEMBOURG	TURKEY
CUBA	MADAGASCAR	UGANDA
CYPRUS	MALAYSIA	UKRAINE
CZECH REPUBLIC	MALI	UNITED ARAB EMIRATES
DEMOCRATIC REPUBLIC OF THE CONGO	MALTA	UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
DENMARK	MARSHALL ISLANDS	UNITED REPUBLIC OF TANZANIA
DOMINICAN REPUBLIC	MAURITIUS	UNITED STATES OF AMERICA
ECUADOR	MEXICO	URUGUAY
EGYPT	MONACO	UZBEKISTAN
EL SALVADOR	MONGOLIA	VENEZUELA
ERITREA	MOROCCO	VIETNAM
ESTONIA	MYANMAR	YEMEN
ETHIOPIA	NAMIBIA	ZAMBIA
FINLAND	NETHERLANDS	ZIMBABWE
FRANCE	NEW ZEALAND	
GABON	NICARAGUA	
GEORGIA	NIGER	
GERMANY	NIGERIA	
GHANA	NORWAY	
GREECE	PAKISTAN	
	PANAMA	
	PARAGUAY	

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

© IAEA, 2004

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria  
September 2004  
STI/PUB/1187

SAFETY STANDARDS SERIES No. NS-G-1.9

DESIGN OF THE REACTOR  
COOLANT SYSTEM AND  
ASSOCIATED SYSTEMS IN  
NUCLEAR POWER PLANTS

SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY  
VIENNA, 2004

**IAEA Library Cataloguing in Publication Data**

Design of the reactor coolant system and associated systems in nuclear power plants. — Vienna : International Atomic Energy Agency, 2004. p. ; 24 cm. — (Safety standards series, ISSN 1020-525X ; no. NS-G-1.9)

STI/PUB/1187

ISBN 92-0-103404-0

Includes bibliographical references.

1. Nuclear power plants — Design and construction. — 2. Nuclear reactors — Cooling. 3. Nuclear reactors — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL

04-00359

## **FOREWORD**

**by Mohamed ElBaradei  
Director General**

One of the statutory functions of the IAEA is to establish or adopt standards of safety for the protection of health, life and property in the development and application of nuclear energy for peaceful purposes, and to provide for the application of these standards to its own operations as well as to assisted operations and, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of nuclear energy.

The following bodies oversee the development of safety standards: the Commission on Safety Standards (CSS); the Nuclear Safety Standards Committee (NUSSC); the Radiation Safety Standards Committee (RASSC); the Transport Safety Standards Committee (TRANSSC); and the Waste Safety Standards Committee (WASSC). Member States are widely represented on these committees.

In order to ensure the broadest international consensus, safety standards are also submitted to all Member States for comment before approval by the IAEA Board of Governors (for Safety Fundamentals and Safety Requirements) or, on behalf of the Director General, by the Publications Committee (for Safety Guides).

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA. Any State wishing to enter into an agreement with the IAEA for its assistance in connection with the siting, design, construction, commissioning, operation or decommissioning of a nuclear facility or any other activities will be required to follow those parts of the safety standards that pertain to the activities to be covered by the agreement. However, it should be recalled that the final decisions and legal responsibilities in any licensing procedures rest with the States.

Although the safety standards establish an essential basis for safety, the incorporation of more detailed requirements, in accordance with national practice, may also be necessary. Moreover, there will generally be special aspects that need to be assessed on a case by case basis.

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA. Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

The requirements and recommendations set forth in the IAEA safety standards might not be fully satisfied by some facilities built to earlier standards. Decisions on the way in which the safety standards are applied to such facilities will be taken by individual States.

The attention of States is drawn to the fact that the safety standards of the IAEA, while not legally binding, are developed with the aim of ensuring that the peaceful uses of nuclear energy and of radioactive materials are undertaken in a manner that enables States to meet their obligations under generally accepted principles of international law and rules such as those relating to environmental protection. According to one such general principle, the territory of a State must not be used in such a way as to cause damage in another State. States thus have an obligation of diligence and standard of care.

Civil nuclear activities conducted within the jurisdiction of States are, as any other activities, subject to obligations to which States may subscribe under international conventions, in addition to generally accepted principles of international law. States are expected to adopt within their national legal systems such legislation (including regulations) and other standards and measures as may be necessary to fulfil all of their international obligations effectively.

#### *EDITORIAL NOTE*

*An appendix, when included, is considered to form an integral part of the standard and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.*

*The safety standards use the form 'shall' in making statements about requirements, responsibilities and obligations. Use of the form 'should' denotes recommendations of a desired option.*

*The English version of the text is the authoritative version.*



# CONTENTS

1.	INTRODUCTION .....	1
	Background (1.1–1.3).....	1
	Objective (1.4) .....	1
	Scope (1.5–1.6) .....	1
	Structure (1.7–1.8) .....	2
2.	EXTENT OF THE RCS AND ASSOCIATED SYSTEMS (2.1–2.3).....	2
	Reactor coolant system (2.4–2.6) .....	3
	Connected systems (2.7) .....	3
	Associated systems (2.8) .....	4
	Ultimate heat sink (2.9).....	4
3.	GENERAL CONSIDERATIONS IN DESIGN (3.1).....	5
	Objectives of the design (3.2–3.7) .....	5
	Safety systems in the RCSASs (3.8).....	6
	Safety classification (3.9–3.12) .....	7
	Design basis (3.13–3.20) .....	8
	Postulated initiating events (3.21–3.23).....	10
	Seismic considerations (3.24–3.27).....	11
	Reliability (3.28–3.35) .....	12
	Selection of materials (3.36–3.38) .....	13
	Provision for overpressure protection (3.39–3.46).....	14
	Prevention of combustible gas accumulation (3.47) .....	15
	Layout considerations (3.48–3.57) .....	15
	Interface considerations (3.58–3.65) .....	17
	Considerations of isolation (3.66–3.69) .....	19
	Instrumentation and control system (3.70–3.74) .....	20
	Provisions for in-service inspection, testing and maintenance (3.75–3.80) .....	21
	Considerations for multi-unit nuclear power plants (3.81–3.82) ....	22
	Advanced reactor designs (3.83–3.84).....	22

4.	SPECIFIC CONSIDERATIONS IN DESIGN (4.1–4.2).....	23
	Reactor coolant system (4.3–4.47) .....	23
	Chemical and inventory control systems	
	including the cleanup system for BWRs (4.48–4.61) .....	32
	Emergency boration system (4.62–4.67) .....	35
	Emergency core cooling system (4.68–4.91).....	36
	Residual heat removal system (4.92–4.104) .....	40
	Steam and main feedwater system (4.105–4.114).....	42
	Auxiliary feedwater system (4.115–4.128) .....	43
	Intermediate cooling circuits (4.129–4.137) .....	46
	The ultimate heat sink and its heat transport systems	
	(4.138–4.154).....	47
	APPENDIX: THE RCS AND ASSOCIATED SYSTEMS IN	
	PRESSURE TUBE HEAVY WATER REACTORS ....	53
	REFERENCES .....	59
	ANNEX I: MAIN COMPONENTS OF THE RCS .....	61
	ANNEX II: DIAGRAMS OF THE RCS	
	AND ASSOCIATED SYSTEMS .....	64
	ANNEX III: SAFETY CLASSIFICATION AND SAFETY CLASS	
	INTERFACE DEVICES FOR FLUID SYSTEMS .....	69
	GLOSSARY .....	73
	CONTRIBUTORS TO DRAFTING AND REVIEW .....	75
	BODIES FOR THE ENDORSEMENT OF	
	SAFETY STANDARDS .....	77

# 1. INTRODUCTION

## BACKGROUND

1.1. This Safety Guide was prepared under the IAEA programme for establishing safety standards for nuclear power plants. The basic requirements for the design of safety systems for nuclear power plants are established in the Safety Requirements publication, Safety Standards Series No. NS-R-1 on Safety of Nuclear Power Plants: Design [1], which it supplements. This Safety Guide describes how the requirements for the design of the reactor coolant system (RCS) and associated systems in nuclear power plants should be met.

1.2. This publication is a revision and combination of two previous Safety Guides, Safety Series No. 50-SG-D6 on Ultimate Heat Sink and Directly Associated Heat Transport Systems for Nuclear Power Plants (1981), and Safety Series No. 50-SG-D13 on Reactor Coolant and Associated Systems in Nuclear Power Plants (1986), which are superseded by this new Safety Guide.

1.3. The revision takes account of developments in the design of the RCS and associated systems in nuclear power plants since the earlier Safety Guides were published in 1981 and 1986, respectively. The other objectives of the revision are to ensure consistency with Ref. [1], issued in 2000, and to update the technical content. In addition, an appendix on pressurized heavy water reactors (PHWRs) has been included.

## OBJECTIVE

1.4. The purpose of this Safety Guide is to provide recommendations and guidance to regulatory bodies, nuclear power plant designers and licensees on the design of the RCS and associated systems, hereinafter referred to as RCSASs. It supplements the requirements established in Ref. [1].

## SCOPE

1.5. This Safety Guide applies primarily to land based stationary nuclear power plants with water cooled reactors designed for electricity generation or in other applications for heat production (such as district heating or desalination). It is recognized that for other reactor types, including innovative

developments in future systems, some parts of the Safety Guide may not be applicable or may need some judgement in their interpretation.

1.6. This Safety Guide covers the RCSASs, including the ultimate heat sinks as defined in Section 2. It covers design considerations for the RCSASs that are common for various reactor types, limited as mentioned in para. 1.5. Additional guidance for PHWR types is provided in the appendix. The scope does not extend to the detailed design of specific components, for example pumps or heat exchangers.

## STRUCTURE

1.7. Section 2 describes the extent of the RCSASs. Section 3 describes general concepts of and recommendations for safe design that are common to the RCSASs. Section 4 discusses specific considerations for safe design in each system introduced in Section 2.

1.8. This Safety Guide focuses on the present generation of reactors (the appendix and Annexes I–III provide additional recommendations, guidance and practical examples of present generation reactors). The applicability of the guidance presented here to a standard design that differs significantly from present water reactor designs is described under Advanced Reactor Designs in Section 3.

## **2. EXTENT OF THE RCS AND ASSOCIATED SYSTEMS**

2.1. The RCSASs consist of the RCS, the connected systems, the associated systems and the ultimate heat sink. The configurations of RCSASs for a PWR and for a BWR are shown in Figs II–2 and II–3 of Annex II.

2.2. Interfaces between the RCSASs and structures are discussed in Section 3.

2.3. A listing of RCSs and components is presented in Annex I and typical configurations for the RCSASs are illustrated in Annex II.

## REACTOR COOLANT SYSTEM

2.4. For all reactor types, the RCS includes the components necessary to ensure the proper flow of reactor coolant, but excludes fuel elements and reactivity control elements which are covered in Ref. [2].

2.5. For all water cooled reactor types, the pressure retaining boundary of the RCS extends up to and includes the first passive barrier or first active isolation device (as viewed from the core).<sup>1</sup> For indirect cycle reactors, such as pressurized water reactors (PWRs), the pressure retaining boundary of the RCS includes the primary side of the steam generators (see Annex II). For direct cycle reactors, such as boiling water reactors (BWRs), the pressure retaining boundary of the RCS also includes the primary coolant recirculation system and the steam and feedwater lines up to and including the outermost isolation valve.

2.6. Additional features of PHWRs of the pressure tube type are discussed in the appendix.

## CONNECTED SYSTEMS

2.7. ‘Connected systems’ are those systems that are connected directly to the RCS or, for some PWR designs, to the secondary side of the steam generators. Together with other systems and components, connected systems perform their functions to ensure the integrity of the RCS in normal operation or following anticipated transients or in design basis accident conditions. The systems that perform these safety functions include:

- Reactivity control fluid systems;
- Chemical and inventory control systems for the reactor coolant, including reactor coolant cleanup systems;
- The emergency boration system, if provided;
- Emergency core cooling systems;<sup>2</sup>
- Residual heat removal systems;

---

<sup>1</sup> In some States it is the practice to incorporate additional barriers or devices that are also considered part of the RCS.

<sup>2</sup> During the recirculation phase of the emergency core cooling system, part of the containment spray system can be used to recirculate sump water before injecting it into the core for long term residual heat removal. This system is described in Ref. [3].

- The main steam and feedwater systems for PWRs and PHWRs;
- The auxiliary feedwater system and emergency feedwater systems or the equivalent (if provided) for PWRs and PHWRs;
- Overpressure relief systems, including safety and/or relief valves, valve discharge lines and any associated equipment;<sup>3</sup>
- The heavy water collection system for PHWRs (see the appendix).

Other interfacing systems (e.g. sampling systems and spent fuel cooling systems) are not covered in this Safety Guide; however, their interactions with the RCS should be taken into consideration in designing the RCSAs.

## ASSOCIATED SYSTEMS

2.8. ‘Associated systems’ are systems that are essential for the RCS and connected systems, which are primarily those for transferring heat to the ultimate heat sink, such as:

- The component cooling water system;
- Intermediate cooling circuits;
- The essential service water system;
- The moderator system and its cooling system for PHWRs (see the appendix).

## ULTIMATE HEAT SINK

2.9. The ultimate heat sink is normally a body of water, the groundwater or the atmosphere, to which medium some part of or all residual heat is transferred in normal operation, anticipated operational occurrences or accident conditions. When water is the medium selected as the ultimate heat sink, the following attributes should be considered:

- The size of the water supply;
- The type of cooling water supply (e.g. ocean, lake, natural or human made reservoir or river);
- Make-up sources to the ultimate heat sink;

---

<sup>3</sup> For example, the pressurizer relief tank in a PWR and the condensation storage pool in a BWR.

- The capability of the heat sink to deliver the necessary flow of cooling water at appropriate temperatures for operational states, accident conditions or shutdown conditions of the reactor.

### **3. GENERAL CONSIDERATIONS IN DESIGN**

3.1. This section describes general concepts and recommendations for safe design that are common to the RCSASs. Specific safe design considerations for each system introduced in Section 2 are mentioned in Section 4.

#### **OBJECTIVES OF THE DESIGN**

3.2. The primary objective of the RCSASs is to ensure that an adequate flow and quality of coolant are available to remove heat from the core in all operational states and in and following design basis accident conditions. The RCSASs may also be used to mitigate the consequences of design basis accidents and beyond design basis accidents.

3.3. Other objectives of the RCSASs include reactivity control, chemical control of the reactor coolant and the removal of heat from other safety systems.

3.4. All these objectives should be met by means of appropriate design provisions. These provisions may vary with the reactor type, the operating conditions and the location of the plant (e.g. in terms of environmental conditions).

3.5. To achieve the above mentioned objectives, the design of the RCSASs should serve the following purposes:

- To provide and maintain a sufficient reactor coolant inventory for core cooling in all operational states and under design basis accident conditions, and to transfer the heat generated to the ultimate heat sink;
- To maintain a sufficient flow of coolant to ensure compliance with fuel design limits as discussed in Ref. [2];

- To prevent an uncontrolled<sup>4</sup> loss of inventory at the reactor coolant pressure boundary;
- To maintain sufficient reactivity worth and to prevent the uncontrolled insertion of reactivity so as to ensure compliance with the fuel design limits, as discussed in Ref. [2].

3.6. The safety objectives of the RCSASs as defined in paras 3.2 and 3.3 should not be compromised by the failure of the components of the RCSASs.

3.7. The design recommendations for the RCSASs should be such that no postulated internal or external initiating event could give rise to more serious plant conditions that could affect the integrity of the fuel cladding or the pressure boundary of the RCSASs.

## SAFETY SYSTEMS IN THE RCSASs

3.8. Some connected and associated systems in the RCSASs are provided to mitigate the consequences of design basis accidents and hence they are considered safety systems. Depending on the design options, there is some flexibility as to how the necessary safety functions are assigned to the various systems; for example, in some PWR designs the auxiliary feedwater system mitigates the consequences of design basis accidents and is thus a safety system, while in other designs the auxiliary feedwater system is not used to mitigate the consequences of design basis accidents. The assignment of safety functions to the connected and associated systems may vary, but every safety system in the RCSASs should have the following common attributes to provide a high level of confidence that it will adequately perform its intended safety functions:

- (1) *Sufficient capacity.* The system should have sufficient capacity to perform its intended functions and to provide a high level of confidence that the design limits for the fuel and the RCS will not be exceeded. In establishing the required capability of the system, consideration should be given to the most adverse conditions under which the system will be expected to operate.

---

<sup>4</sup> An example of an uncontrolled loss of inventory at the reactor coolant pressure boundary would be an RCS pipe rupture event or a vessel leak. Conversely, lifting of the relief valves would be a controlled loss of inventory at the reactor coolant pressure boundary.



- (2) *Single failure.* The system should be so designed that no single failure could prevent the fulfilment of its intended safety function or those of other systems.
- (3) *Electrical and emergency power supply.* The appropriate emergency power supply (AC or DC) should be provided as necessary to components that are needed for system actuation or operation.
- (4) *Protection against external events [4, 5] and internal hazards [6].* The system should be so designed and laid out that no external event or internal hazard considered in the design (such as a pipe break or a flood) has the potential to prevent it from performing its intended safety functions. In particular the capability of the system or its components should be maintained under the most severe seismic conditions considered in the design.
- (5) *Safety classification, codes and standards and assessment of mechanical design.* The system should be classified and designed for safety in accordance with internationally or nationally recognized codes and standards. It should be capable of withstanding the loads and environmental conditions resulting from all the anticipated operating conditions over the plant lifetime.
- (6) *Environmental qualification.* The system should be qualified for the most severe environmental conditions (including seismic conditions) under which it will be expected to operate.
- (7) *Monitoring of the status and behaviour of the system.* Monitoring of the status and readiness of the system in normal operation should be possible. In cases as specified in Section 4, system monitoring during an accident should be possible.
- (8) *Periodic testing, inspection and maintenance at power:* See under Provision for in-service inspection, testing and maintenance in this section, paras 3.75–3.80.
- (9) *Manual actuation.* Manual actuation of the system should be possible from the main control room and if appropriate from the supplementary control room.

## SAFETY CLASSIFICATION

3.9. It is required (Ref. [1], para. 5.1) that “All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety shall be first identified and then classified on the basis of their function and significance with regard to safety. They shall be

designed, constructed and maintained such that their quality and reliability is commensurate with this classification.”

3.10. It is required (Ref. [1], para. 5.2) that “The method for classifying the safety significance of a structure, system or component shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:

- (1) the safety function(s) to be performed by the item;
- (2) the consequences of failure to perform its function;
- (3) the probability that the item will be called upon to perform a safety function;
- (4) the time following a [postulated initiating event] (PIE) at which, or the period throughout which, it will be called upon to operate.”

3.11. The functions and safety significance of at least those structures, systems and components (SSCs) in the RCSAs performing the following safety functions should be classified:

- Providing the pressure retaining parts of the RCS whose failure could cause a loss of coolant accident in excess of the normal make-up capability for the reactor coolant;
- Providing fission product barriers;
- Providing heat removal from the core;
- Ensuring emergency core cooling (with the coolant supplied directly to the core);
- Introducing negative reactivity to render the reactor subcritical or to maintain it in a subcritical condition.

3.12. Recommendations on principles for the classification are provided in Ref. [7]. An example of principles for safety classification is given in Annex III.

## DESIGN BASIS

3.13. To establish the design basis (acceptance criteria) for the RCSAs, an analysis of the PIEs (see under Postulated initiating events in this section, paras 3.21–3.23) should be carried out.

3.14. Structures, systems and components of the RCSASs should be designed, fabricated, erected, constructed, tested and inspected in accordance with appropriate and well established codes and standards, commensurate with the importance of the safety function to be performed.

3.15. The design of components of the RCSASs such as pressure vessels, piping, pumps and valves should comply with the appropriate national engineering codes and standards or practices (see Ref. [1], para. 3.6) or those codes and standards or practices in use internationally.

3.16. In the design of SSCs of the RCSASs important to safety, account should be taken of all external hazards such as seismic hazards (for further information see under Seismic considerations in this section, paras 3.24–3.27), tornadoes, missiles, floods and hurricanes that may possibly be encountered in all operational states and in design basis accident conditions.

3.17. The design basis (the set of design conditions and requirements) for the RCSASs and their components should specify the following:

- The extent to which plant instrumentation and control systems are assumed to function under normal operating conditions;
- The credit taken for the functioning of plant systems that are normally operating;
- The extent to which operator actions are necessary and the credit taken for them;
- The extent to which plant protection systems and reactor protection systems are required to function;
- The extent to which safety systems are required to operate;
- Appropriate margins for malfunctions.

3.18. The most widely used method for the design of the RCSASs is deterministic, whereby SSCs are designed to comply with guiding rules. This approach is generally complemented with a probabilistic risk assessment whose objective is to verify that the plant as designed does not have any unacceptable vulnerabilities.

3.19. In order to achieve a well balanced design, appropriate consideration should be given to the redundancy and diversity of systems and components. For safety systems, this consideration should be based on a deterministic

approach such as the application of the single failure criterion, supplemented by a risk informed approach.<sup>5</sup>

3.20. Equipment outages should be taken into account in the design (see Ref. [1], para. 5.42).

## POSTULATED INITIATING EVENTS

3.21. A list of PIEs should be established for use in the safety analysis of the RCSASs. The likelihood of occurrence of the events and their potential consequences should be taken into account. For plants at which preventive maintenance at power is intended, the need for considering a PIE that is coincident with the maintenance of one safety system train should be evaluated.

3.22. In establishing the list of PIEs, combinations of events relevant to the design of the RCSASs should also be considered, in accordance with Ref. [1].

3.23. Examples of PIEs that could significantly influence the design of the RCSASs include:

- Primary and secondary side pipe breaks;
- Turbine trip, loss of condenser vacuum, closure of the main steam isolation valves (in BWRs) and failure of the steam pressure regulator;
- Loss of reactor coolant flow (e.g. due to pump failure);
- Inadvertent opening of the pressure relief valve;
- Rod drop (in BWRs), rod ejection (in PWRs) or boron dilution accidents (in PWRs);
- Loss of off-site power;

---

<sup>5</sup> Risk informed consideration is an approach for using probabilistic risk assessment in decisions on plant specific changes to the licensing basis. When the design of the RCSASs is formulated using risk informed regulatory principles, other design aspects relating to defence in depth, safety margins, core damage frequency, prescribed limits on releases of radioactive material and performance monitoring should be re-evaluated. Thus a risk informed approach may be used for ensuring the adequacy of the design with respect to the safety requirements. If the risk study indicates the need for additional requirements, these should be established to ensure the adequacy of the design and consistency with risk targets.

- Failure of a heat exchanger tube in PWRs (e.g. rupture of a steam generator tube);
- Internal missiles;
- Internal flooding;
- Fires;
- Earthquakes;
- External missiles;
- Floods and other natural phenomena;
- Results or consequences of human activities (excluding sabotage).

## SEISMIC CONSIDERATIONS

3.24. Structures, systems and components of the RCSASs should be classified and assigned to the appropriate seismic categories in accordance with the recommendations and guidance given in Ref. [4]. The SSCs of the RCSASs, irrespective of the safety class to which they are assigned, should be considered seismic category I if they are necessary to effect any of the following:

- Maintaining the integrity of the RCS pressure boundary,
- Achieving and maintaining residual heat removal,
- Achieving and maintaining shutdown of the reactor,
- Mitigating the consequences of a seismic event.

3.25. Structures, systems and components of the RCSASs should be designed on the basis of seismic ground motions appropriate to the site and the seismic category to which they are assigned as established in accordance with the procedures given in Ref. [8]. Appropriate restraints, supports and snubbers should be provided so that the relevant limitations on stress and displacement and the no-loss-of-function criteria are met.

3.26. The dynamic effect of flow instabilities and the dynamic loads (e.g. water hammer) induced by earthquakes should be taken into account in the design in accordance with the safety analysis. Some combinations of an earthquake and other PIEs likely to occur independently of an earthquake should be taken into account by the use of methods as stated in Ref. [1], paras I.14–I.18, and appropriate provisions should be made for these combinations.

3.27. It should be ensured in the design that the failure of SSCs of the RCSASs or other systems not designed in accordance with seismic category I would not cause failure of those systems that are designed in accordance with seismic category I.

## RELIABILITY

3.28. Systems that are relied upon to fulfil a safety function should have adequate reliability commensurate with the safety function that they perform. In assessing system reliability, appropriate consideration should be given to both redundancy and diversity.

3.29. Redundancy alone may be insufficient to provide adequate reliability owing to common cause failures; diversity could have the potential to compensate for this. In assessing the potential benefit of diversity the following should be considered:

- The consequence of different operating conditions;
- The effects of different manufacturing processes on the reliability of components;
- The consequences for the reliability of components of different work processes based on different physical methods;
- The potential benefit or detriment resulting from the increased complexity of maintenance and/or the increased burden on operators in the event of an accident.

3.30. Since redundant or diverse systems are also potentially vulnerable to events (e.g. fires, floods) resulting in common cause failures, appropriate physical barriers or physical separation or a combination of both should be used as far as is practicable.

3.31. Methods of probabilistic analysis can be used to demonstrate that the reliability of the systems is adequate.

3.32. When deterministic methods are used, it may not be necessary to specify numerical values to be achieved for the reliability of systems and components. However, the reliability of systems and components should be commensurate with their importance to safety.

3.33. Any computer codes used in the safety analysis should be verified and validated. The calculation methods used in the computer code should be appropriate for the purpose.

3.34. Operator errors can have a major influence on the reliability of the systems and components necessary to fulfil safety functions, and therefore in

the design of the RCSASs adequate consideration should be given to minimizing the potential for human errors.

3.35. If credit is claimed for operator action in the initial phase of a transient, an assessment should be made of the consequences of delay and/or error on the part of the operator with respect to predetermined acceptable limits.

## SELECTION OF MATERIALS

3.36. The materials used for the pressure retaining boundary of the RCSASs should be compatible with the coolant that they contain, with joining materials (e.g. welding materials), and with adjoining components or materials such as sliding surfaces, spindles and stuffing boxes (packing boxes), overlay or radiolytic products. Materials specified for the RCSASs should comply with the applicable provisions of the code used, including but not limited to the following properties and characteristics:

- Resistance to heat loads;
- Strength, creep and fatigue properties;
- Corrosion and erosion related properties;
- Resistance to stress corrosion cracking;
- Resistance to effects of irradiation;
- Resistance to temper embrittlement;
- Ductility characteristics (including crack growth rate);
- Fracture toughness (brittle failure) characteristics;
- Ease of fabrication (including weldability);
- Resistance to metal–water reactions.

3.37. Materials should be selected to be suitable for the service conditions expected in all operational states and under design basis accident conditions.

3.38. If the materials selected do not meet the specifications, they should be qualified by means of analysis, testing, the feedback and analysis of operating experience, or a combination of these.

## PROVISION FOR OVERPRESSURE PROTECTION

3.39. All pressure retaining components of the RCSAs should be protected against overpressure conditions in compliance with applicable codes and standards.

3.40. All pressure retaining components of the RCSAs should be designed with an appropriate safety margin to ensure that the pressure boundary will not be breached and that the fuel design limits will not be exceeded in operational states or in design basis accident conditions.

3.41. The design of the RCS should include adequate features for overpressure protection; that is, it should provide the capability to deal with vapours and liquids in the RCS. Safety and/or relief valves should be included in the design.

3.42. The defence in depth concept should be applied to the overpressure protection. The diversity principle should be applied in the design of the overpressure protection of the RCS to reduce the likelihood of common cause failures. The design of overpressure protection devices should reflect their safety significance and it should be consistent with their expected performance in the most limiting PIEs.

3.43. Overpressure protection of the reactor coolant pressure boundary can be achieved by means of the following provisions or actions:

- Monitoring the system pressure [9];
- Means of controlling the pressure of the system within operational limits (e.g. using the inventory control systems);
- Devices for overpressure relief such as safety valves or relief valves;
- The reactor protection system [9].

3.44. Examples of means to decrease and/or control the pressure in the RCS include:

- Spraying in the pressurizer (in PWRs);
- Opening of pressurizer relief valves for PWRs and pressurizer bleed valves for PHWRs;
- Opening of safety valves;
- Opening of turbine bypass valves;
- Opening of main steam line relief valves;
- Reactor trip initiated by the reactor protection system;



- Prevention of excessive injection of coolant (e.g. when operation of the RCS is conducted with the pressurizer isolated during a warm-up transient in a PHWR);
- During the startup or shutdown of the reactor, discharge of the reactor coolant through the RCSASs, or in PWRs through let-down functions in chemical and inventory control systems.

3.45. In the design and location of safety and/or relief valves in the RCS, its pressurizer (in PWRs) and other interconnected vessels (if any), account should be taken of the single failure criterion so that the pressure boundary of the RCS can be maintained within the design limits in all operational states and in design basis accident conditions.

3.46. The discharge capacity of safety and/or pressure relief valves in the RCS should be sufficient to limit pressure increases and to keep the pressure within the prescribed design limits during all operational transients and in the accident conditions considered in the design of the RCS, in accordance with the applicable pressure vessel code and standard. The number of valves should be sufficient to provide the necessary degree of redundancy.

## PREVENTION OF COMBUSTIBLE GAS ACCUMULATION

3.47. Hydrogen and oxygen generated by the decomposition of  $H_2O$  (or  $D_2O$ ) in the core can dissolve in the water and steam and be carried to any part of the RCS and connected systems. Gases dissolved in steam piping can easily accumulate when steam in a closed off section of piping cools down and condenses into water. A local accumulation of hydrogen gas in the RCS could give rise to the potential for an explosion that could result in severe damage. The design should be such that the possibility of combustible gas accumulation can be excluded.

## LAYOUT CONSIDERATIONS

3.48. The design layout of the RCSASs should take into account:

- Radiological protection of site personnel;
- Protection against the consequences of pipe failure;
- Protection against internal missiles;
- Provisions for venting and draining the reactor coolant;
- Provisions to facilitate testing and inspection.

3.49. The layout of safety systems should be such that the minimum required capability is maintained in the event of a failure in one train of protection or in the event of needing to survive any internal and/or external hazards (e.g. earthquake, fire and flooding).

3.50. Needs for room and floor drainage should be considered and provisions for these should be commensurate with the maximum level of external flooding for the site.

3.51. The layout of the RCS should be such that, in the event of a total loss of power supplies to pumps in operational states as well as in specific design basis accident conditions, the removal of residual heat is ensured by the natural circulation of the reactor coolant.

### **Protection against radiation exposure**

3.52. The design of the layout of RCSAs should allow for the inspection, maintenance, repair and replacement of SSCs, with account taken of the need for the radiological protection of site personnel.

3.53. For the purposes of radiological protection:

- Systems and components that could circulate contaminated water should be provided with adequate radiation shielding.
- Parts of a connected system situated between the RCS and its first isolation valve, including the valve itself, that are normally closed during normal operation should be designed to the same safety standards as the RCS.
- Fluid systems that penetrate the containment envelope and extend outside the containment should be robust and should possess adequate devices for flow isolation that are capable of preserving the safety function and performance of the containment envelope. The section that penetrates the containment, up to and including the flow barrier, should be considered an extension of the containment boundary and should be designed to the appropriate levels of quality and performance in accordance with the applicable codes and standards. These systems, if they are not provided with the capability for prompt and reliable leak detection and rapid isolation, should be considered extensions of the containment boundary and should be designed accordingly.
- Fluid systems interfacing with components and systems that circulate contaminated water should be designed to prevent or minimize leakage

so that either no leakage of radioactive products is possible or else any measurable leaks can be promptly detected.

- The length of the piping that carries radioactive material in areas where personnel may be exposed should be minimized.
- Crevices and other local configurations where radioactive sludge and debris could accumulate should be minimized in the detailed design of the plant.

3.54. Design measures for radiological protection are discussed further in Ref. [10].

### **Protection against the consequences of pipe failures**

3.55. Consideration should be given to the layout of the piping system and to the design of the piping supports in order to protect the SSCs against the consequences of pipe failure.

3.56. The design specifications for the RCSAs should identify high energy pipes in which sudden ruptures are postulated to occur and systems that must be protected from the dynamic effects of such ruptures. For more information, see Ref. [6].

### **Venting and draining**

3.57. Provision should be made to collect coolant vented and drained from the RCSAs. Leaks can occur from, among others, double packed valve stems, valve seats, pump seals and intergasket cavities during reactor operation.

## **INTERFACE CONSIDERATIONS**

3.58. Appropriate interface devices should be provided for connections between systems or components belonging to different safety classes (see Annex III). These interface devices should prevent the loss of the safety function of the system or component with the higher safety classification and should prevent the release of radioactive material. An interface device should have the same safety classification as the system or component with the higher safety classification to which it is connected.

3.59. The reliability of the interface should be commensurate with the safety functions of the involved systems and should be in accordance with the considerations discussed under Reliability in this section (paras 3.28–3.35).

3.60. In the design of the structures of RCSASs, account should be taken of their impact on the overall safety of the plant. The plant designer should ensure that the temperatures of the structures and components interfacing with the RCSASs are maintained within acceptable limits and that provision is made for in-service inspections. Components and structures that are directly anchored to the containment should be designed so that their failure would not cause the loss of containment leaktightness.

3.61. Interface considerations should include flow rates, various loading conditions, response times<sup>6</sup> and heat transfer capabilities.

3.62. Examples of loads on the supporting structures for RCSASs are:

- The dead weight of components in normal and abnormal operation;
- Thermal expansion in steady state or transient conditions;
- Earthquake loads;
- Transient loads.

3.63. Structures interfacing with the RCSASs include items such as:

- Buildings supporting or housing the RCSASs;
- Equipment and piping supports;
- Snubbers and their anchors;
- Pipe whip restraints;
- Building penetrations;
- Barriers, shields and protective structures;
- Reactor building sumps.

3.64. The design of the RCSASs should also reflect constraints imposed by the support systems and structures. Support systems include, for example, ventilation systems, compressed air systems, electric power systems and the instrumentation and control system.

---

<sup>6</sup> The response time is the period of time necessary for a component to reach a specified output state.

3.65. In designing a system, appropriate consideration should be given to the consequences of the design conditions of other systems, i.e. RCSAs and/or systems considered in other IAEA publications as follows.

- (1) The consequences of different sizes and/or locations of breaks in the RCS pressure boundary for:
  - Recommendations for the design of the spray system (see Ref. [3]),
  - Recommendations for the containment design (see Ref. [3]),
  - The net positive suction head needed for the injection and recirculation pumps of the emergency core cooling system.
  
- (2) The consequences of the layout of components of the RCS for (see Ref. [3]):
  - Considerations of containment isolation in determining the locations of the isolation valves and their closure times,
  - The design of the ventilation system.
  
- (3) The consequences of the design of the steam generator for the design conditions of the emergency feedwater system.

## CONSIDERATIONS OF ISOLATION

3.66. Adequate isolation should be provided at the interfaces between the RCS and connecting systems operating at lower pressures to prevent the overpressure of such systems and possible loss of coolant accidents. Consideration should be given to the characteristics and importance of the isolation and its reliability targets. Isolation devices either should usually be closed or should close automatically on demand. The response time and speed of closure should be in accordance with the acceptance criteria defined for postulated initiating events (see Ref. [3] for guidance).

3.67. Lines that penetrate the primary containment boundary and lines that are connected to the reactor coolant pressure boundary should be provided with adequate isolation. The isolation devices could be either open or closed in operational states and in accident conditions, depending on their design requirements and required safety functions.

3.68. If the system piping had to penetrate the containment wall, containment extensions should satisfy the recommendations for safe design in terms of design qualification and containment isolation (see Ref. [3] for guidance).

3.69. Safety grade isolation valves and devices should be environmentally qualified to the most severe conditions expected (see Ref. [3] for guidance).

## INSTRUMENTATION AND CONTROL SYSTEM

3.70. A safety grade instrumentation and control system [9] should be provided to activate the appropriate safety systems and to provide sufficient information to reactor operators to enable them to determine the state of the RCSASs [11]. The instrumentation and control system should be capable of continually monitoring plant conditions during normal plant operations as well as in anticipated occurrences.

3.71. Instrument lines<sup>7</sup> should be so designed that the detected parameters (e.g. magnitude, frequency, response time, chemical characteristics) are not distorted.

3.72. For all PIE events, the instrumentation and control system should function as assumed in the transient analysis and accident analysis with regard to manual or automatic actuation.

3.73. Means for monitoring the activity in all fluids that could become radioactive should be provided in accordance with Ref. [9].

3.74. Provisions should be made for the detection of any leakage of reactor coolant, and to the extent practicable for the identification of the location of the leak. Provisions should also be made to monitor for and collect leaks from all sources. These provisions should be adequately complemented by indicators and alarms in the main control room.

---

<sup>7</sup> Instrument lines are part of the sensors as defined in Ref. [9]. Instrument lines are thus subject to the general requirements for the reactor protection system and related features and the safety related instrumentation and control systems.

## PROVISION FOR IN-SERVICE INSPECTION, TESTING AND MAINTENANCE

3.75. Structures, systems and components of the RCSASs should be designed to facilitate the performance of inspection and testing tasks without undue exposure of the site personnel to radiation. Appropriate in-service inspection programmes should be established for the entire plant lifetime as well as for the commissioning period.

3.76. Intervals<sup>8</sup>, methods, locations and acceptance criteria for inspections should be established according to the safety significance of the SSCs of the RCSASs, in order to increase the likelihood of timely detection of any deterioration in the structural integrity of the RCSASs. Alternatively, risk informed methods of in-service inspection may be used to determine the intervals of inspections as well as the locations for inspections.

3.77. Structures, systems and components important to safety should be inspected during their service life with regard to their capability to perform their intended safety functions as well as their physical integrity, including any change in the properties and characteristics of the materials used. The specified inspection and testing methods should not demand capabilities for the performance of inspection and testing that go beyond well established techniques or other acceptable methods.

3.78. Periodic testing, when required, should simulate the conditions under which systems and/or components are expected to operate. Test conditions should not be such as to jeopardize plant safety, however.

3.79. Automated or remotely operated equipment can be used for in-service inspection to keep the exposure to radiation of the inspection personnel as low as reasonably achievable and within any limits specified by legislation or by the regulatory body.

3.80. Recommendations and guidance on inspection and maintenance during plant operation are provided in Ref. [12].

---

<sup>8</sup> In many States, the specified interval for volumetric inspection of the pressure boundary of light water reactors is 8–10 years; however, in practice, part of the RCS is inspected each year so that the entire pressure boundary inspection is completed within the specified intervals.

## CONSIDERATIONS FOR MULTI-UNIT NUCLEAR POWER PLANTS

3.81. If SSCs important to safety are shared between two or more nuclear power reactors, it should be demonstrated that all the safety recommendations and considerations are met for each reactor. In the event of a design basis accident involving a reactor that shares SSCs with other reactors, it should be demonstrated that an orderly cooldown and removal of residual heat are achievable in the other reactor(s). The reliability of the shared SSCs should be commensurate with the safety functions being performed, and due consideration should be given to the possibility that an event could give rise to the need to shut down two or more reactors simultaneously.

3.82. The performance and the qualification of the shared SSCs should be adequate to accommodate the effects of the most limiting PIE. This limiting PIE may be an event that affects one or more reactors.

## ADVANCED REACTOR DESIGNS

3.83. The identification and evaluation of the differences in key design features between proposed advanced reactor designs and the present generation of LWRs and HWRs should be considered in assessing whether the recommendations and guidance in this Safety Guide are applicable to advanced reactor designs.

3.84. For reactor designs that differ in significant ways from the designs that have provided the current experience base in licensing and operation, the new systems and components should be tested sufficiently to ensure that their thermal-hydraulic behaviour is understood and predictable. Data analyses and code assessments should be performed and the established code should be used to predict the behaviour of the advanced reactor design with regard to transient analysis and accident analysis required for licensing. This Safety Guide could be used in assessing whether the reliability of SSCs is commensurate with their intended safety functions if they perform functions similar to those of the present generation of LWRs.



## 4. SPECIFIC CONSIDERATIONS IN DESIGN

4.1. Section 4 discusses the specific design considerations for the RCSAs for performing their specified safety functions. The safety functions may be fulfilled in different ways for the various designs of water cooled and moderated reactors. Simplified flow diagrams showing the main components and functional features of several typical designs of RCSAs are presented in Annex II.

4.2. The specific considerations described below relate to PWRs and BWRs. Specific considerations for PHWRs are given in the appendix.

### REACTOR COOLANT SYSTEM

4.3. The RCS forms a pressure retaining boundary for the reactor coolant and is therefore a barrier to radioactive releases in all modes of plant operation. The RCS transports the coolant and thereby heat from the reactor core either to the steam generating systems or directly to the turbine generator. The RCS also forms part of the route for the transport of heat from the reactor core to the ultimate heat sink during shutdown and in all transient conditions that are considered in the design of the RCS.

#### **General considerations**

4.4. In the design of the RCS, consideration should be given to ensuring the integrity of its pressure boundary and to providing a high level of operational reliability. In addition, the leak before break concept or techniques of break preclusion should be considered for use in mitigating the consequences of localized failures.

4.5. Undue challenges to the integrity of the RCS should be prevented. As a minimum, measures should be provided for the following:

- To detect any degradation of the capability for core cooling or any deterioration of components important to safety (e.g. by means of the measurement of operating parameters for heat transport, monitoring for leaks of reactor coolant and the detection of loose parts in the system);
- To ensure that failures in the RCS outside the reactor vessel do not result in significant radiological consequences for the public.

4.6. In order to prevent disruption of the natural circulation of the reactor coolant, remotely operated valves should be provided at high points in the RCS to vent non-condensable gases to the containment building in accident conditions. These valves should be so designed that:

- They follow all the safety recommendations and accommodate the effects of the environmental conditions expected to be encountered in their intended use;
- They are operable from the control room;
- There is sufficient redundancy between the valves to meet the requirements relating to the reliability of venting, if any;
- The risk of spurious opening is minimized.

The capability for venting should be consistent with the capacity of the make-up system.

### **Reactor pressure vessel**

4.7. Since gross failure of the reactor pressure vessel would result in severe core damage, special consideration should be given to ensuring that there is an extremely low probability of such a failure. To design the vessel in accordance with established codes and safety standards is one of the approaches to making such a failure extremely unlikely.

4.8. The design considerations for the pressure vessel should include the following:

- (1) The number of welds in the pressure vessel should be minimized; in particular the need for welds in the active core region should be assessed.
- (2) Pressure and temperature limits should be established for the pressure vessel and the vessel wall should be designed to withstand all the cyclic loads that are expected to occur over the plant lifetime. The design documentation should include clear specifications of those loads that are necessary for the determination of the cumulative usage factor.
- (3) The choice of material, the structural design, the welding and the heat treatment should be such as to ensure a sufficiently ductile state of the material of the pressure vessel throughout the plant lifetime. The ductility of the pressure vessel wall facing the core should be ensured by limiting the maximum neutron fluence and by the use of base material and weld metal of a chemical composition such as to keep radiation embrittlement below an acceptable level.

- (4) The design of the pressure vessel should be such that it can withstand pressurized thermal shocks<sup>9</sup> without incurring a failure of integrity.
- (5) The welds should permit through-wall examination of the entire volume of the wall. For example, ultrasonic, eddy current or magnetic flux methods could be used for such examinations.
- (6) Non-inspectable welds should be limited to those areas where a failure would not result in an accident that could have significant radiological consequences for the public.
- (7) The following issues should be considered in deriving the inspection criteria:
  - The minimum detectable indication in non-destructive examinations,
  - The expected crack growth in operational states and in design basis accident conditions,
  - The maximum acceptable defect in operational states.

4.9. If advanced materials were to be used in the reactor pressure vessel or the RCSAs, samples of these materials should be subjected to a high fast neutron flux and exposed to the environment of the pressure vessel. They should be examined periodically throughout the plant lifetime to monitor changes in physical properties (in particular ductility and toughness) and to enable predictions to be made of the behaviour of the material.

### **Reactor pressure vessel internals**

4.10. The reactor pressure vessel internals (core support structures, the core shroud in a BWR and other internals, but excluding fuel elements, reactivity

---

<sup>9</sup> In overcooling transients of some types in PWRs, rapid cooldown could be accompanied by the repressurization of the primary system. The stresses due to pressurization would add to the effects of the thermal stresses. If the fracture toughness of the steel of the reactor pressure vessel remains relatively high, such transients would not be expected to cause failure of the pressure vessel. However, if an overcooling event occurs after the fracture toughness of the pressure vessel has been reduced by neutron irradiation, a severe pressurized thermal shock (PTS) event might cause a pre-existing flaw near the inner surface of the pressure vessel to propagate through the vessel wall. Depending on the progression of the accident, a through-wall crack could lead to a core melt; the issue is therefore recognized as important in assessing the integrity of the reactor pressure vessel. Various States are carrying out significant PTS research programmes, both probabilistic and deterministic, to refine and validate PTS analyses.

control elements, control rod drive mechanisms and in-core instrumentation) should be designed:

- To withstand the effects of earthquakes without loss of capability;
- To accommodate the effects of the environmental conditions expected in normal operation, in anticipated operational occurrences and in design basis accident conditions, including loss of coolant accidents, in maintenance and in testing;
- To prevent unacceptable flow induced vibration;
- To accommodate asymmetric blowdown loads caused by pipe ruptures;
- To ensure that fuel design limits are not exceeded in normal operation or anticipated operational occurrences.

4.11. The selection of materials, fabrication practices, examinations, testing procedures and chemical control of the reactor coolant to prevent stress corrosion cracking should be such as to preclude in-service deterioration and to ensure structural integrity.

4.12. The effects of stress corrosion cracking in causing the degradation of reactor pressure vessel internals that are important to safety should be considered.

4.13. Horizontal loading caused by seismic loads, for example, which may increase the stress corrosion cracking, should also be considered.

4.14. Plant safety evaluations should include consideration of, for example, the material used, the water chemistry, the neutron fluence and the use of clamping devices with regard to ensuring the structural integrity.

### **Reactor coolant pumps including reactor recirculation pumps for BWRs**

4.15. The RCS and reactor coolant pumps should be such as to provide an adequate flow of reactor coolant with suitable hydraulic parameters to ensure that the fuel design limits are not exceeded in operational states.

4.16. The pumps in the RCS should have adequate flow coastdown characteristics in the event of a pump trip under transient or design basis accident conditions to avoid undesirable thermal-hydraulic conditions of the reactor coolant with regard to the integrity of the fuel.

4.17. The pumps should be designed to withstand the thermal-hydraulic conditions of the reactor coolant and all cyclic loads expected in operational states and design basis accident conditions. Special consideration should be given in the design to maintaining the leaktightness of the pumps.

4.18. The design of the pumps should be such that adverse thermal-hydraulic conditions in the RCS or pump malfunctions do not result in the generation of missiles. Alternatively, provision should be made to protect items important to safety from any such missiles.

### **Steam generators in PWRs and HWRs**

4.19. The steam generator tubes and their internal structures should be designed for the maximum stresses and most severe fatigue conditions expected to occur in operational states and in design basis accident conditions (e.g. the conditions resulting from a steam line break). The flow pattern in the steam generators should be optimized to prevent the occurrence of areas of stagnant flow (to avoid the accumulation of precipitates) and unacceptable flow induced vibration of the tubes.

4.20. The design should allow for inspection of the steam generator tubes over their entire length. The equipment and procedures for examination of the tubes should be capable of detecting and locating significant defects.

4.21. A permanent record of the test data should be kept. This should include selection of samples for the testing of tubes, the inspection intervals and the procedures or action to be taken in the event of the identification of defects, as well as the results of a baseline tube inspection conducted prior to the startup of the plant.

4.22. The design should also provide for the following:

- Control of the pH and oxygen concentration;
- Limitation of the concentration of contaminants and impurities in the feedwater and in the secondary side of the steam generator;
- Fluid sampling from the secondary side;
- Addition of chemical additives to the feedwater;
- Monitoring of the conductivity and for contamination of the sampled fluid;
- Purging.

4.23. The design of the steam generators should provide an adequate system for tube leak detection and alarm.

4.24. Overfilling of the steam generator may occur as a consequence of a PIE; this should be addressed primarily in the design or else in procedures.

4.25. Complex loadings such as those due to water hammer and thermal and/or hydraulic stratification should be addressed for the operating modes in which they may occur.

### **Piping systems**

4.26. The layout of the piping and equipment should be such that flow induced vibration, ageing effects, acoustic excitation, thermal fatigue and the accumulation of radioactive material are minimized. Harmful consequences of accidental flooding should also be minimized.

4.27. The arrangement of piping and the location of equipment should facilitate natural circulation where necessary. Capability should be provided for venting and drainage of the piping system. The design should meet the needs for the separation of redundant equipment and should preclude the common mode failure of redundant components and systems.

4.28. The layout of the piping and equipment should provide sufficient accessibility to allow maintenance and inspection, including maintenance and inspection for welds and for the functionality of piping supports, to be conducted where necessary. It should also allow the surveillance and monitoring of the performance of equipment and components where and when necessary.

4.29. The design of piping supports should be commensurate with the piping system standard. Stress assessment for piping and components should be conducted in compliance with applicable nuclear codes and standards.

4.30. Operating conditions should be such that the risk of stress corrosion cracking is minimized.

4.31. Special consideration should be given to minimizing the leakage of radioactive fluid from valves. Permissible rates of leakage of reactor coolant for continuing normal operation should be specified. A system should be provided to monitor for and to collect any leaks.

4.32. Recommendations and guidance on protection against the consequences of pipe failure are provided in Ref. [6]. In assessing the consequences of pipe failure the following should be considered:

- The effects of the reactor coolant on the thermal-hydraulic parameters;
- The effects on chemical parameters such as the concentration of boron in the reactor coolant (for PWRs and PHWRs);
- The drag forces in and the loading on the RCS owing to the stream of discharging fluid;
- Pressure waves (water hammer) in the RCS.

### **The pressurizer and pressure discharge devices**

4.33. A pressurizer, if provided, should be directly connected to the RCS for PWRs and PHWRs. Its main function is to ensure that variations in the reactor coolant inventory or in thermodynamic conditions would not result in unacceptable challenges to the RCS boundary. To this end, the pressurizer should be so designed that:

- An adequate steam space is maintained to bear pressure transients in the RCS;
- Systems such as spray systems or heaters and overpressure protection devices are provided to maintain the pressure within acceptable limits in normal operation and in transient conditions up to and including design basis accident conditions.

4.34. An adequate set of safety valves and relief valves should be provided in the RCS so that the pressure in the system does not exceed that allowed by design. This function may also be necessary as a result of faults in the normal pressure and inventory control system. The fluid discharged from the safety and/or relief valves should be collected at lower pressure and returned to the RCS when normal operating conditions have been restored. If the collection system is another pressure vessel operating at lower pressure, this should be fitted with adequate overpressure protection (e.g. by means of a set of safety and/or relief valves). These valves may discharge the fluid collected to the reactor building sump, where a recovery system would enable the collection, purification and recovery of the inventory.

### *Functions*

4.35. The pressurizer and the safety valve system should fulfil the following functions:

- To provide overpressure protection for the reactor coolant pressure boundary in all operational states and all other conditions considered in their design;
- To limit the reactor pressure in operational states;
- For PWRs, to provide overpressure protection during low temperature operation (i.e. during startup and shutdown when the pressurizer is water solid).

### *Interfaces*

4.36. For PWRs and BWRs, the pressurizer and depressurization systems may interface with the following systems:

- The RCS;
- The AC and DC power supply systems;
- The heating, ventilation and air conditioning systems;
- The instrumentation and control system;
- The instrument air system;
- The containment and/or suppression pool (in BWRs).

### *Isolation considerations*

4.37. At least one relief path should remain available at all times during reactor operation. Relief paths should be provided with the capability for isolation to mitigate the consequences of spurious operation of the relief valves. The pressurizer relief tank, if provided, should be equipped with rupture disks or an equivalent.

### *Safety function considerations*

4.38. The relief valves that provide the overpressure protection during power operation should be designed with sufficient redundancy and capacity to preclude actuation of the safety valves.

4.39. The safety valves should be designed with sufficient capacity to maintain the pressure below the specified limit.



4.40. Safety and/or relief valves should be qualified for their anticipated operating conditions during transients and accidents.

4.41. The capacities, set points and set point tolerances for all safety valves and relief valves should be selected to protect the reactor coolant pressure boundary for all transients considered in the design that could lead to an increase in pressure.

4.42. Operability of the overpressure protection system should be maintained in the event of a loss of off-site power. The system should be operable with a power supply backed up by a battery or completely independently of any electrical power supply.

4.43. In the design of the overpressure protection system and its components, it should be ensured that no unacceptable consequences could result from the possible spurious operation of relief valves in the overpressure protection system (e.g. by incorporating a system for monitoring valve positions in the main control room).

4.44. Loads and load combinations resulting from operation of the overpressure protection system should be taken into consideration in the design of the components that are affected by such operation of the pressurizer and pressure discharge devices.

4.45. The pressurizer relief tank, if provided, should have sufficient volume to accommodate steam discharged from pressure relief devices during valve testing activities or normal operating transients.

4.46. The relief capacity of the rupture disks should be at least equal to the combined capacity of the pressurizer relief valves and safety valves with sufficient allowance.

4.47. Overpressure protection should also be ensured during the startup or shutdown of the reactor. As stated in para. 3.44, means to decrease and/or control the pressure in the RCS during the startup or shutdown of the reactor include discharge of the reactor coolant through the RCSASs, or in PWRs through let-down functions in chemical and inventory control systems.

## CHEMICAL AND INVENTORY CONTROL SYSTEMS INCLUDING THE CLEANUP SYSTEM FOR BWRs

### **Functions**

4.48. The chemical and inventory control systems should provide at least the following functions:

- Chemical control of the reactor coolant (for PWRs and PHWRs);
- Inventory control for the reactor coolant;
- Cleanup and purification for the reactor coolant;
- Reactivity control for the reactor;
- The provision of seal water for the reactor coolant pump (in PWRs);
- The provision of water for the auxiliary pressurizer spray (in PWRs).

4.49. The chemical and inventory control functions listed in para. 4.48 are mainly for normal operation and are not usually performed during accidents. However, parts of the system may be used to reach a safe shutdown state following abnormal events or accidents.

4.50. Chemical and inventory control systems should be considered safety related systems. Redundant pumps and an emergency power supply (see Ref. [13]) should be used.

### **Interfaces**

4.51. The chemical and inventory control systems may interface with the following systems:

- The RCS;
- The AC and DC power supply systems;
- The intermediate cooling water system;
- The make-up water system;
- The systems for processing radioactive waste;
- The heating, ventilation and air conditioning systems;
- The instrumentation and control system;
- The instrument air system.

## **Isolation considerations**

4.52. There are no additional recommendations on isolation considerations beyond those made in Section 3.

## **Chemical control of the reactor coolant**

4.53. The chemistry of the reactor coolant (for PWRs and PHWRs) should be controlled to inhibit corrosion of the core and components of the RCS, to minimize the deposition of crud on the fuel and to adjust the concentration of the neutron absorber in the RCS.

4.54. In the design of the reactivity control and shutdown systems, account should be taken of the effects of chemical additives on core reactivity (see Ref. [2]).

## **Cleaning and purification of the reactor coolant**

4.55. Means should be provided to clean (i.e. demineralize) and purify (i.e. remove chemical impurities and fission and activation products from) the reactor coolant in all operational modes. The cleaning and purification systems for the reactor coolant should be capable of removing chemical impurities and fission and activation products from the reactor so as:

- To maintain the chemical conditions and characteristics of the coolant within the limits specified in the design for the reactor core (with regard to both neutronic effects and limitation of corrosion; see Ref. [2]). Such conditions should be consistent with the materials used and the operating parameters of the reactor.
- To protect components of the RCS against corrosion.
- To minimize radioactive contamination of the components of the RCS.

4.56. Means should be provided for degassing the reactor coolant. Gases (such as fission product gases, hydrogen and oxygen) are produced in or absorbed into the RCS. The local accumulation of combustible gases such as hydrogen in the RCS should be taken into account.<sup>10</sup> When it is necessary to remove these

---

<sup>10</sup> In 2001 a hydrogen explosion occurred in a BWR nuclear power plant in Japan as a result of the accumulation of hydrogen in a dead-end pipe close to the emergency core cooling system.

gases to observe safety limits, appropriate chemical or mechanical means such as gas venting should be used. The capacity of degassing devices should be based on the maximum predicted rate of gas formation (see Ref. [10]).

### **Reactivity control**

4.57. In some types of reactor (e.g. PWRs) a soluble neutron absorber such as boric acid is one of the means of controlling core reactivity. In designing the system used to control the concentration of neutron absorber in the reactor coolant (the chemical reactivity control system), the recommendations in Ref. [2] should be followed.

4.58. The possibility of inadvertent dilution of the neutron absorber in the reactor coolant should be taken into account in the design by means of specific provisions combined with adequate procedures.

4.59. Operator error or equipment malfunction may result in an increase in reactivity caused by the addition of unborated water to the RCS via the chemical and inventory control systems. Boron dilution events should be analysed for all modes of operation and for the entire fuel cycle to demonstrate that the design limits for the fuel and for the RCS are not exceeded.

4.60. The need to prevent the precipitation of boric acid during operation of the chemical reactivity control system should be taken into account in the design.

### **Control of the reactor coolant inventory**

4.61. The control system for the reactor coolant inventory should provide for the controlled make-up and discharge of coolant to accommodate variations in volume in all operational states so that operational limits and conditions are not exceeded. Examples of variations in the coolant inventory that may occur during plant operation include those due to heat-up and cooldown of the coolant, planned and unplanned power changes, extraction of the reactor coolant for purification, flows to the reactor coolant pumps for seal cooling (in PWRs and PHWRs), auxiliary spray in pressurizers (in PWRs) and minor leaks of coolant.

## EMERGENCY BORATION SYSTEM

### **Functions**

4.62. Some reactor designs provide an emergency boration system to inject soluble neutron absorber promptly into the RCS and the core after an accident.

### **Interfaces**

4.63. The emergency boration system may interface with the following systems:

- The RCS;
- The AC and DC power supply systems;
- The intermediate cooling water system;
- The emergency core cooling system;
- The chemical and inventory control systems;
- The heating, ventilation and air conditioning systems;
- The make-up water system;
- The instrument air system.

### **Isolation considerations**

4.64. The emergency boration system should be functionally isolated from the RCS during normal operation.

### **Safety function considerations**

4.65. Isolation devices should not impair the adequate co-ordination of the system with the RCS when its operation is needed.

4.66. The emergency boration system should function in such a way that the design limits of the fuel and of the RCS pressure boundary are not exceeded in accidents in which its operation is needed.

4.67. The emergency boration function should be maintained in the event of the loss of off-site power.

## EMERGENCY CORE COOLING SYSTEM

### Functions

4.68. The main function of the emergency core cooling system is to inject water into the RCS to remove heat from the core in the event of design basis accidents.

4.69. In some designs, the emergency core cooling system also fulfils other functions such as:

- Emergency injection of boron;
- Transfer of residual heat to an interfacing cooling system;
- Removal of heat during shutdown for refuelling;
- Filling of refuelling cavities.

### Interfaces

4.70. The emergency core cooling system may interface with the following systems:

- The RCS;
- The intermediate cooling water system;
- The AC and DC power supply systems;
- The instrumentation and control system;
- The instrument air system;
- The chemical and inventory control systems (in PWRs);
- The containment system;
- The heating, ventilation and air conditioning systems;
- The automatic depressurization system (in BWRs);
- The make-up water system (in BWRs);
- The condensate storage tank (in BWRs);
- The suppression pool (in BWRs and PHWRs).

### Isolation considerations

4.71. The number and type of isolation devices should be determined on the basis of the following considerations:

- The emergency core cooling system should be isolated from the RCS during normal operation;

- In the event of actuation of the emergency core cooling system, the minimum expected performance of the system should not be impaired;
- Isolation from the RCS should be possible in the event of spurious actuation of the emergency core cooling system or if necessary in an accident (e.g. to prevent overfilling of the pressurizer);
- The isolation configuration may be selected on the basis of deterministic criteria (e.g. use of the single failure criterion) supplemented by risk informed considerations.

4.72. Assessments should be made, on the basis of deterministic criteria supplemented by risk informed considerations, of the behaviour of passive components (e.g. check valves in discharge lines from accumulators or core make-up tanks) to ensure that their reliability is commensurate with their safety importance.

### **Redundancy considerations**

4.73. The emergency core cooling system should be designed with sufficient redundancy to meet reliability targets, if any. To this end, deterministic considerations supplemented by risk informed considerations may be taken into account. If it is intended to perform maintenance of components of the emergency core cooling system during plant operation, the emergency core cooling system should be so designed that no single failure, even during such maintenance, could prevent the fulfilment of its intended safety functions.

### **Safety function considerations**

4.74. The design should be such that the emergency core cooling system fulfils its intended safety functions on the assumption of a single failure for all design basis accident conditions.

4.75. The capability of the emergency core cooling system, alone or in conjunction with other safety systems, should be such that releases, if any, of radioactive material into the atmosphere are maintained within the prescribed limits for accident conditions.

4.76. The emergency core cooling system should be designed to ensure that enough coolant is available for adequate long term core cooling. In particular, it should be demonstrated that for low levels in the make-up water storage tank:

- The inventory of coolant in the containment sump or the suppression pool (in BWRs) is adequate to allow recirculation of the coolant in the reactor core;
- The system, when assigned for long term cooling, interfaces with an associated system that transfers heat to the ultimate heat sink.

4.77. The layout of the system should be such that an adequate capability for core cooling can be maintained on the assumption that the break occurs in the worst possible location.

4.78. The trains of the emergency core cooling system, including the strainers, should be physically separated from one another. The fulfilment of the intended safety functions of the emergency core cooling system should be demonstrated by either experiment or analysis, or by a combination of the two. Analyses should be performed to verify that the emergency core cooling system has been designed to provide an adequate capability for core cooling for the entire range of breaks in the RCS that were considered in the design.

4.79. For PWRs, the system should be designed to prevent the precipitation of solid boron in the core in a loss of coolant accident.

4.80. Provision should be made to prevent the entrainment of debris which might obstruct the circulation of coolant in the emergency core cooling system.

4.81. Equipment for emergency core cooling should be adequately protected from the consequences of internal and external hazards such as seismic hazards that have the potential to jeopardize its safety functions.

4.82. All possible loadings that may occur over the plant's operating lifetime should be considered in the mechanical design of the emergency core cooling system. For example:

- Thermal loads at the interface with the RCS;
- Water hammer;
- Seismic loads;
- Impact loads (e.g. loads due to pipe whip).

A careful selection of load combinations should also be considered.

4.83. The mechanical design should be assessed against acceptance criteria that are consistent with the mode of operation of the system; namely, that its primary



purpose is to mitigate the consequences of loss of coolant accidents. All the consequences of actuation of the emergency core cooling system for other systems (e.g. the RCS) should be evaluated in the design of the connected systems.

4.84. Devices of the emergency core cooling system should be so organized that manual actuation or restart (if required) of the system is possible from either the main control room or the remote shutdown panel.

4.85. If applicable, reconfiguration of the systems from the injection mode to the recirculation mode should be automatic. Manual actuation should be contemplated only when there is adequate time available to the operator to perform the actuation safely. Recommendations and guidance on adequate time for operator action are provided in Ref. [9].

4.86. The emergency core cooling function should be maintained in the event of the loss of off-site power. The necessary power supply to perform the function of emergency core cooling should be provided by the emergency power supply system (see Ref. [13]). It should be verified that the starting and loading times of the emergency power supply are adequate to ensure the performance of the emergency core cooling functions in an accident.

4.87. Certain systems for emergency core cooling can operate only at low pressure. If actuation of the emergency core cooling system requires the prior operation of other systems (e.g. a depressurization system), it should be shown that the system has both a proven safety capability and reliability commensurate with the expected function and performance of the emergency core cooling system.

4.88. The design of the emergency core cooling system should be such that periodic functional testing of the active components in the system is possible during normal reactor operation at power.

4.89. The design of the emergency core cooling system should be such that inspection tasks do not impair its functional capability.

4.90. The design of the emergency core cooling system should be such that its readiness is monitored at all times.

4.91. Monitoring of the performance of the emergency core cooling system in operational states and/or after an accident should be possible by means of adequate instrumentation and monitoring (see Ref. [9]).

## RESIDUAL HEAT REMOVAL SYSTEM

4.92. For systems with the capability of removal of residual heat that are not part of the RCSAs (e.g. the containment spray system, the pressure suppression pool in BWRs), recommendations and guidance are provided in Ref. [3].

### **Functions**

4.93. The function of the residual heat removal system is to remove residual heat from the RCS to the associated systems so as to reach safe shutdown conditions. For most designs this is achieved after a partial cooldown has been effected.

### **Interfaces**

4.94. The residual heat removal system may interface with the following systems:

- The RCS;
- The intermediate cooling circuit;
- The AC and DC power supply systems;
- The instrumentation and control system;
- The instrument air system;
- The heating, ventilation and air conditioning systems;
- The suppression pool (in BWRs);
- The make-up water system (in BWRs).

### **Isolation considerations**

4.95. The residual heat removal system should be functionally isolated from the RCS during normal operation.

4.96. Where the residual heat removal system has been designed to operate at low pressures only, appropriate isolation measures should be adopted to preserve its integrity when the RCS is pressurized.

### **Safety function considerations**

4.97. For a residual heat removal system that operates at the normal operating pressure of the RCS, the rate of removal of residual heat should be such that

the design limits of the fuel and of the RCS pressure boundary are not exceeded.

4.98. A residual heat removal system that operates at low pressure should be designed to take over performing the function of the shutdown cooling of the plant after the temperatures and pressures in the RCS have been reduced to predetermined limits.

4.99. For any PIE (e.g. a total loss of feedwater event), it should be shown that at least one combination of associated systems would be available to remove residual heat. In a loss of coolant accident, residual heat should be either entirely or partially removed by the emergency core cooling system.

4.100. The function of residual heat removal should be maintained in the event of a loss of off-site power and a single failure of an active component. The necessary power supply to perform the function of residual heat removal should be provided by the emergency power supply system (see Ref. [13]).

4.101. Spurious connection between the high pressure RCS and the lower pressure part of the residual heat removal system could result in an accident, namely a loss of coolant accident with an interfacing system. In some States plant specific risk informed analyses are used to estimate the probability and consequences of such an event. The low pressure parts of the residual heat removal system that interface with the RCS should be capable of withstanding the full pressures and temperatures of the RCS.

4.102. The design of the residual heat removal system should allow functional testing of the system during normal operation at power.

4.103. The piping arrangements should be such that damage to the pumps by air entrainment is prevented.

4.104. Control of the performance of the residual heat removal system should be possible by means of adequate instrumentation and monitoring. The possibility should be provided for manual actuation of the system from the supplementary control room.

## STEAM AND MAIN FEEDWATER SYSTEM

### Functions

4.105. The function of the steam and main feedwater system is to transfer the heat produced in the reactor core to the turbine for the generation of power.

4.106. In normal operation, the steam and main feedwater system should allow stable operation of the reactor at the rated power level. The production and dissipation of heat should be balanced at any level of power production.

4.107. In BWRs, provision should be made to control the water level in the reactor pressure vessel during startup and in operational states.

4.108. In PWRs, provision should be made to control the system pressure and the coolant inventory in the steam generator during startup.

### Interfaces

4.109. The following systems may be provided as support systems for the steam and main feedwater system:

- The make-up system;
- The extraction steam system;
- The chemical control system;
- The cleanup system;
- The sampling system;
- The power supply system;
- The compressed air system;
- The instrumentation and control system;
- The instrument air system;
- The heating, ventilation and air conditioning systems;
- The feedwater heating system;
- The condensate system including the condensate storage tank (in BWRs).

### Isolation considerations

4.110. In the design of the steam and feedwater system in BWRs, provision should be made to allow the adequate isolation of the system in the event of its failure or the failure of the RCS. Examples of PIEs that would affect the steam and feedwater system are the loss of condenser vacuum, the closure of all steam

line isolation valves, turbine trip with locked bypass valves, and failure of the integrity of the pressure boundary of the steam and feedwater system. In PWRs and PHWRs, the capability for isolation of the steam generators should be considered.

4.111. In direct cycle reactors (BWRs) that have a suppression pool within the containment, an adequate capability for isolation of the main steam line, the release of steam through safety relief valves to the suppression pool and a corresponding feedwater system should be ensured (see Ref. [3]).

### **Safety function considerations**

4.112. Functionality of the components of the steam and main feedwater system that are important to safety (e.g. isolation devices) should be maintained in the case of a loss of off-site power.

4.113. In operational states, the steam and feedwater system should be capable of removing the heat from the reactor core and the RCS to the ultimate heat sink at such a rate that the design limits of the fuel are not exceeded and the capability of cooling the core is maintained. In particular the pressures in the RCS and the main steam system should be maintained below the design limits.

4.114. Instrumentation and control and monitoring systems should be provided to monitor the conditions of the steam and feedwater system in all operational states and during or after accidents. Appropriate devices should be provided to detect fluid leaks.

## **AUXILIARY FEEDWATER SYSTEM**

### **Functions**

4.115. The auxiliary feedwater system is used as a backup to maintain the heat sink capability of the plant in the event that the main feedwater system becomes unavailable. The capability for heat removal of the auxiliary feedwater system may be used to reduce the pressure in the RCS when necessary.

4.116. The auxiliary feedwater system is used to maintain the plant in a hot standby condition for an extended period. It may also have to be used to bring the plant to a cold shutdown. The auxiliary feedwater system should provide

sufficient capacity to fulfil these functions efficiently. Some designs may feature a separate emergency feedwater system to fulfil safety functions independently while the auxiliary feedwater system is reserved for normal operating functions. In this case, clear and distinct performance and safety objectives should be defined for both systems.

4.117. In indirect cycle reactors (PWRs), if there is no separate emergency feedwater system, the auxiliary feedwater system is used as a safety system (emergency feedwater system) to remove residual heat from the RCS. The transfer of heat to the ultimate heat sink could be effected through the pressure relief devices of the steam generator or through the condenser.

4.118. In BWRs, the auxiliary feedwater system is usually termed the reactor core isolation cooling system. This system is used to maintain the water level in the reactor vessel in the event of a loss of feedwater in hot shutdown conditions (in such an event residual heat is removed from the reactor core by means of the release of steam through safety relief valves to a suppression pool). Another function of this system is to supply the necessary inventory of reactor coolant in the event of a small loss of coolant during normal operation.

4.119. In a BWR, an isolation cooling system for the reactor core should be provided as a standby source of cooling water to provide a capability for feedwater supply whenever the main feedwater system is isolated from the reactor pressure vessel. Abnormal events that could cause such an isolation include the inadvertent isolation of the main steam lines, the loss of condenser vacuum, the failure of a pressure regulator, the loss of feedwater and the loss of off-site power.

The reactor core isolation cooling system should be designed:

- To withstand the full pressure of the RCS;
- To provide a capability for the removal of decay heat in conjunction with the high pressure safety injection system (or the high pressure core spray), the safety and/or relief valves and the suppression pool.

## **Interfaces**

4.120. The following systems may be provided as support systems:

- The extraction steam system;
- The chemical control system;

- The cleanup system;
- The sampling system;
- The power supply system;
- The compressed air system;
- The heating, ventilation and air conditioning systems;
- The instrumentation and control system;
- The feedwater heating system.

4.121. In addition, pressurized steam may be required when steam driven pumps are used.

### **Isolation considerations**

4.122. In BWRs that have a suppression pool within the containment, an adequate capability for isolation of the main steam line, the release of steam through safety relief valves to the suppression pool, and a corresponding make-up of coolant should be ensured.

### **Safety function considerations**

4.123. The auxiliary feedwater system(s) may be provided with redundancy and/or diversity to fulfil their safety function(s) adequately. An assessment of the adequacy of redundancy and/or diversity may be made on the basis of deterministic criteria supplemented by risk informed considerations.

4.124. The system should provide a sufficient storage capacity for water to fulfil its intended function.

4.125. The minimum rated cooling capability of the system should be such that the design limits of the fuel and of the reactor coolant pressure boundary are not exceeded.

4.126. Since secondary side pipe breaks in PWRs could lead to overcooling events, the maximum capability of the system should be such that a return to criticality will not be caused and there will be no unacceptable thermal shock to the reactor pressure vessel.

4.127. The chemical properties of the feedwater system should be maintained to minimize detrimental consequences (e.g. intergranular stress corrosion cracking and flow assisted corrosion) for the internal structures and components, including tubes, of the steam generators.

4.128. Instrumentation and control and monitoring systems should be provided to monitor the condition of the auxiliary feedwater system in operational states and during or after accidents.

## INTERMEDIATE COOLING CIRCUITS

### **Functions**

4.129. The functions of the intermediate cooling circuits are:

- To transfer heat from the RCSASs or other heat sources to the ultimate heat sink,
- To act as a barrier to the dispersion of radioactive material to the environment or the ingress of unsuitable chemicals into the RCSASs.

### **Interfaces**

4.130. The following support systems may be provided:

- The chemical control system;
- The sampling system;
- The power supply system;
- The heating, ventilation and air conditioning systems;
- The compressed air system;
- The instrumentation and control system.

### **Isolation considerations**

4.131. When a system or an item of equipment not important to safety is connected to an intermediate cooling circuit system, appropriate measures should be taken to ensure that the necessary safety functions are not jeopardized. The parts of the systems that are important to safety may have to be isolated automatically from the rest of the systems.

### **Safety function considerations**

4.132. When an intermediate cooling circuit system is essential for post-shutdown cooling, the provision of a diversity of ultimate heat sinks may be considered in addition to the redundancy necessary to meet the single failure criterion. When a diversity of ultimate heat sinks (e.g. a river or the



atmosphere) is necessary, this may necessitate special considerations in the design of the intermediate cooling circuits (e.g. the need for different heat exchangers or pumps).

4.133. The capacity for heat transport of the intermediate cooling circuit system should be commensurate with the heat sources these circuits serve and the most severe instance of temperature differential and other environmental parameters for the design that may arise during the plant lifetime should be taken into account. The rate of heat transfer to the ultimate heat sink should be established and account should be taken of the necessary rate of removal of heat from the RCSAs.

4.134. Functional parameters of the intermediate cooling circuit system should be maintained within specified limits when subjected to adverse environmental phenomena that are relevant for the site and the type of ultimate heat sink (freezing, tornadoes, missiles, hurricane winds, floods, earthquakes, blockage of water flow, extreme maximum temperatures, poor water quality).

4.135. In setting the specifications for components and equipment of the intermediate cooling circuit system that interface with the upstream and downstream systems, particular attention should be paid to leaktightness. The intermediate cooling circuit systems should be designed to withstand water hammer loads, to cope with flooding and to resist corrosion.

4.136. Instrumentation should be provided to control and monitor the intermediate cooling circuit system in all operational states and in design basis accident conditions. Appropriate devices may be provided to detect leaks.

4.137. Appropriate isolation capabilities should be provided to prevent unacceptable flooding of building areas and the consequent failure of safety systems.

## THE ULTIMATE HEAT SINK AND ITS HEAT TRANSPORT SYSTEMS

### **Site and environmental conditions**

4.138. In the selection of the type of ultimate heat sink and its directly associated heat transport systems for a plant, account should be taken of the specific site conditions in which the plant will operate and of its impact on the environment.

4.139. In determining the necessary capacity of the ultimate heat sink and its directly associated heat transport systems, design basis environmental parameters should be established. These parameters include the water temperature of the ultimate heat sink for once-through water cooling systems and the air dry bulb temperature for dry cooling towers. Both wet bulb and dry bulb air temperatures are needed for wet cooling towers, cooling ponds or spray ponds, and for other heat transport systems that use evaporative cooling. Other parameters such as water quality (mud content and chemical impurities), wind speed and insulation factors should be included where necessary.

4.140. The environmental parameters considered in the design of the ultimate heat sink and its directly associated heat transport systems should be appropriate to the site specific conditions and the specific systems. Recommendations and guidance on the consideration of external events in the design of the ultimate heat sink are provided in Ref. [5].

### **Heat loads**

4.141. The ultimate heat sink should be capable of absorbing the heat generated under any plant conditions.

4.142. The long term capacity of the ultimate heat sink is ensured by means of designs that provide immediate access to inexhaustible natural bodies of water or to the atmosphere. For sites without such access, it should be demonstrated that sufficient capacity exists to accept the heat load until the heat sink can be replenished.<sup>11</sup> In such a demonstration account should be taken of factors that could delay the replenishment process. Such factors include evaporation, human induced events, plant accident conditions, the availability of interconnections and the complexity of the procedures for replenishment. The locations and sizes of the intake and discharge structures should be carefully evaluated in terms of yearly temperature excursions, and the recorded patterns and effects of biofouling and of the buildup of sand and silt on the effectiveness and performance of the proposed design. Depending on the site characteristics, the need for a backup ultimate heat sink should be carefully assessed.

---

<sup>11</sup> In some States the acceptable minimum capacity of the immediately available sources of water, including water stored on-site in tanks or reservoirs, absorbs all heat loads generated in 30 days, unless a shorter time period can be justified by conservative analysis.

4.143. In establishing the maximum heat rejection rate, the most severe combination of individual heat loads should be identified for all PIEs for which the system is called upon to perform a normal operation or a safety function.

4.144. In determining the capacities demanded of the ultimate heat sink and its directly associated heat transport systems, the various heat sources and their time dependent behaviour should be precisely identified to ensure that the temperature of the coolant remains within specified limits. The heat loads that should be taken into consideration include the following:

- The residual heat of the reactor,
- The decay heat of the spent fuel with the storage system at its maximum capacity,
- The heat rejected from pumps and other components,
- Heat from other accident related sources (e.g. chemical reactions).

4.145. In establishing the residual heat loads of the reactor (including decay heat, heat due to shutdown fission and stored energy), it should be assumed that the fuel has been exposed to operation at power for a period of time that would produce the maximum decay heat load and the decay heat should be evaluated consistently with applicable standards.

4.146. The total heat load and rejection rate of heat from spent fuel should be evaluated on the basis of the maximum number of spent fuel elements that can be stored on-site at any one time. Either the decay heat curves for the particular fuel, with appropriate individual post-shutdown times applied to the various fuel elements, or a conservative average post-shutdown time for all fuel elements should be used.

4.147. The heat loads rejected by active components such as the pumps, motors and other heat generating devices that are necessary for the operation of the auxiliary systems serving and dependent on the ultimate heat sink should be considered in selecting the ultimate heat sink for all operational states and design basis accident conditions.

4.148. The time dependent behaviour of the individual heat loads should be superimposed to establish the peak heat rejection rate which will form the basis for sizing the heat transport systems. In performing this calculation, consideration may be given to the temporary storage of heat in heat sinks within the plant, such as structures within the core, the primary and secondary systems, the containment structure, suppression pools, spent fuel storage pools and heat transport media.

4.149. Accident conditions may produce additional sources of heat, such as the heat emanating from metal–water reactions of the fuel cladding or from other heat producing chemical reactions within the containment. If potential metal–water reactions are determined to be significant as an additional heat source, then they should be quantified as a function of time and included in the sizing criteria.

### **Heat transport systems**

4.150. With regard to safety considerations, the following factors will govern the sizing of the heat transport systems directly associated with the ultimate heat sink:

- The maximum heat rejection rate;
- Environmental parameters for design (water or air temperatures, relative humidity);
- The supplies of coolant.

4.151. Where an ultimate heat sink of limited capacity is provided, the choice of the heat transport system that is directly associated may be dictated by the need to conserve the inventory of the ultimate heat sink; this would increase the required time for make-up water to be available. If the required time to restore the make-up water is short, a more stringent justification of the applicable procedures should be required.

4.152. The peak rate of heat rejection demanded may be reduced for the heat transport systems directly associated with the ultimate heat sink by storing the heat and by delaying the time when use of the ultimate heat sink is necessary.

### **Multi-unit sites**

4.153. Where sharing of the ultimate heat sink between reactors at a multi-unit site is found to be permissible, the ultimate heat sink and its directly associated heat transport systems should be capable of meeting the design objectives for:

- The simultaneous safe shutdown and cooldown of all the reactors they serve and their preservation in a safe shutdown state;
- The dissipation of heat following an accident in one reactor, plus the simultaneous safe shutdown and cooldown of all remaining units and their preservation in a safe shutdown state.

4.154. Sharing of the ultimate heat sink between reactors at a multi-unit site should not degrade its overall reliability. In this regard, unnecessarily complex design features such as multiple interlocks and automatic switchover of equipment between several reactors should be avoided. Furthermore, where heat transport systems directly associated with the ultimate heat sink are shared, account should be taken of the greater potential consequences of failure of the system.



## Appendix

### THE RCS AND ASSOCIATED SYSTEMS IN PRESSURE TUBE HEAVY WATER REACTORS

A.1. This appendix provides additional recommendations and guidance specific to PHWRs. The appendix is not in contradistinction to the main text of this Safety Guide nor are the two mutually exclusive. However, in certain cases it may replace or be complementary to the recommendations and guidance in the main text.

#### REACTOR COOLANT SYSTEM

A.2. The RCS comprises the pressure retaining components of the primary heat transport system including the isolation valves, the primary coolant pumps, the primary side of the steam generators, the reactor inlet and outlet headers and the piping up to and including the isolation devices. The recommendations for the RCS in PHWRs are equivalent to those for PWRs once due consideration has been given to the differences in layout, in the numbers and types of components and in their safety significance. The configuration of RCSASs is shown in Fig. II-4 of Annex II and is described below.

#### CONNECTED SYSTEMS

A.3. The systems that are connected to the RCS should be considered to be fulfilling the safety function of directly ensuring the integrity of the RCS. They include but are not limited to:

- The fuel channel assemblies, including the fuel bundles;
- Two shutdown systems;
- The fuelling machines;
- The pressure control and inventory control systems;
- The pump seal cooling system;
- The emergency core cooling system;
- The shutdown cooling system;
- The heavy water (D<sub>2</sub>O) collection system.

## ASSOCIATED SYSTEMS

A.4. As with PWRs, the associated systems are those essential to the safe functioning of the RCSASs. The associated systems in a pressure tube reactor are:

- The moderator and its cooling system;
- The shield cooling system;
- The liquid injection shutdown system;
- The steam and feedwater system;
- The auxiliary feedwater system.

## SPECIFIC DESIGN CONSIDERATIONS

A.5. The following are general and detailed design considerations that complement those set out in the main text and are specific to pressure tube type reactors.

### **The fuel channel assemblies**

A.6. The fuel channels constitute a connected system of the RCS in Canada deuterium uranium (CANDU) type PHWRs. They should be designed to provide a low neutron absorbing pressure boundary to support and locate the fuel bundles and they should allow for a controlled flow of the pressurized coolant around and through the fuel bundles.

### **Liquid injection shutdown systems**

A.7. Two diverse and separate shutdown systems should be provided. These are typically systems for shutdown by rod injection and by liquid injection. Each shutdown system should be capable of independently shutting down the reactor in all operational states and in design basis accident conditions.

A.8. The function of the rod injection system is similar to that in PWRs. A liquid injection shutdown system should be capable of injecting a neutron absorbing solution directly into the heavy water moderator in the calandria, shutting down the reactor. This system should have a shutdown capability comparable with that of the rods but with trip set points such that the rods actuate first.



A.9. Each shutdown system should be capable of independently shutting down the reactor in all controlled and design basis accident conditions.

### **The fuelling machines**

A.10. When aligned with the fuel channels being refuelled, the fuelling machines should be considered and designed to constitute an integral part of the RCS pressure boundary. Hence, the pressure boundary of the fuelling machine should be designed to the same safety recommendations as those for the RCS.

### **Pressure and inventory control system**

A.11. If the pressurizer, if provided, can be isolated from the RCS in certain operating conditions (i.e. during warmup or cooldown), the pressure and inventory control system should include alternative means of controlling the pressure and inventory in the RCS, such as a set of automatically controlled feed and bleed valves. In this case, the pressurizer should have an independent safety and/or relief device.

A.12. The bleed condenser, which is a vessel connected to the pressurizer and maintained at a lower pressure in normal operation, should be fitted with passive relief devices (e.g. rupture discs, relief valves or safety valves operated by pilot valves) capable of transmitting steam, liquids and flashing liquids, since the condenser may be flooded in the event of large discharges of fluid from the RCS or the pressurizer. In the design of the bleed condenser, account should be taken of the range of pressures and temperatures of the RCS.

A.13. The pressure and inventory control system should include a purification system designed to control the chemical characteristics and activity of the coolant within specified limits by the removal of dissolved chemical impurities, radioactive substances including fission products, and suspended solids.

### **Emergency core cooling system**

A.14. The emergency core cooling system supplies cooling water (light water) to the RCS following a loss of coolant accident in which the inventory of heavy water is lost. It should be designed to remove residual heat from the reactor.

A.15. The emergency core cooling system in PHWRs with reactor headers should be designed to cool the core adequately in the event of a double ended guillotine break of a header.

### **Emergency water or reserve water systems**

A.16. An emergency water or reserve water system or the equivalent should be designed to provide emergency make-up water (light water) to the RCS and other systems such as the moderator when all sources of heavy water in the plant have been depleted.

A.17. When necessary, the reserve water system or equivalent should provide make-up water to the secondary side of the steam generators to mitigate the consequences of a sequence of events giving rise to a total loss of feedwater.

### **Shutdown cooling system**

A.18. When necessary, the shutdown cooling system should be designed also to remove decay heat when the reactor is shut down following an accident by functioning as an alternative heat sink to the steam generators.

A.19. The system should allow the lowering, raising and controlling of the level of coolant in the RCS to allow maintenance of the heat transport pumps and the steam generators.

### **Associated systems**

A.20. Differences from PWRs are not major. Safety and engineering recommendations such as those relating to grouping, separation, redundancy, isolation and methods of analysis such as risk informed and probabilistic safety assessment are similar to those for other types of water cooled reactors, which all apply. Only specific differences in functionality and terminology are highlighted here.

### **Moderator system**

A.21. The heavy water moderator that allows the use of natural uranium or slightly enriched uranium as fuel may also serve as a means for the dispersion of moderating chemicals to shut down the reactor in an emergency and to control the reactivity of the reactor core. (Removing or dumping the moderator can also be used as a means of shutting down the reactor.)

A.22. The moderator system should have its own cooling system to remove heat transferred from the reactor structure and the heat generated by radioactive decay in the moderator system.

A.23. The moderator system and the shield cooling water reservoir surrounding it should be intrinsically capable of maintaining the integrity of the fuel channels when all other normal and emergency cooling media are impaired. They could be used as backup ultimate heat sinks to mitigate the consequences of beyond design basis accidents.

### **The shield cooling system**

A.24. The cylindrical shell of the calandria is capped by the end shields and surrounded by a shield cooling tank. The end shields should be designed to allow access to the fuelling machine area and to the reactor face and to fulfil any structural and support function that they may have. The space between the calandria shell and the shield cooling tank shell is filled with light water, which serves as a thermal and biological shield. It should be designed to allow access by personnel to the reactor's inner vault for inspection and maintenance during reactor shutdown.

A.25. The light water in the shield tank and the end shield cavities should be circulated and cooled. The end shield and the shield cooling systems should be designed to remove heat generated in the shielding material as well as heat transferred from the RCS into the end shields and the shield tank.

A.26. The end shield and the shield cooling systems should be capable of maintaining the structural components of the reactor at acceptable temperatures so as to prevent intolerable deformation under all design basis accident conditions.

### **The heavy water (D<sub>2</sub>O) collection system**

A.27. The heavy water collection system should be designed to collect leaks from any anticipated leak source in the RCS, such as double packed valve stems, pump seals and intergasket cavities. The system should also be used to collect venting and draining fluids from the RCSASs and from equipment of other systems.

A.28. The heavy water collection system should also be designed for cooling vapours, if any, and should have a provision for venting.



## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Core for Nuclear Power Plants, Safety Standards Series No. NS-G-1.12, IAEA, Vienna (2004).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, Safety Standards Series No. NS-G-1.10, IAEA, Vienna (2004).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Hazards for Nuclear Power Plants, Safety Standards Series No. NS-G-3.3, IAEA, Vienna (2002).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, Safety Standards Series No. NS-G-1.13, IAEA, Vienna (in preparation).
- [11] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-Service Inspection in Nuclear Power Plants, Safety Standards Series No. NS-G-2.6, IAEA, Vienna (2002).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).



## Annex I

### MAIN COMPONENTS OF THE RCS

I-1. The following listings are typical of the main components and equipment of the RCSs of various types of reactor.

#### PRESSURIZED WATER REACTORS

- (a) Reactor vessel with its closure head assembly;
- (b) Reactor vessel internals (other than fuel assemblies and core support structures) necessary for the proper flow of the primary coolant, such as the core barrel;
- (c) Steam generators;
- (d) Reactor coolant pumps;
- (e) Pipes that, together with the steam generators and the reactor coolant pumps, constitute the coolant loops:
  - A hot leg between the reactor vessel and the steam generator of each loop,
  - Crossover leg(s) between the steam generator and the pump(s) of each loop,
  - Cold leg(s) between the pump(s) of each loop and the reactor vessel;
- (f) The pressurizer with its relief valves and safety valves and the piping connecting it to the coolant loop piping (e.g. surge line);
- (g) Pipes bypassing the steam generators and the reactor coolant pumps and used for measuring the temperature of each loop;
- (h) Reactor vessel appurtenances such as the pressure housing for the control rod drive mechanism or the reactor vessel head vent;
- (i) Auxiliary systems connected to a loop up to and including the first isolation devices;
- (j) Components such as valve actuators and pump drives associated with (d)–(i).

## BOILING WATER REACTORS

- (a) Reactor vessel with its closure head assembly and support skirt;
- (b) Reactor vessel internals (other than fuel assemblies and the core support structure) necessary for the proper flow of the primary coolant, such as the core shroud, jet pumps, internal recirculation pumps or separators;
- (c) Reactor vessel appurtenances such as flow venturi, orifices and control rod drive housings;
- (d) Steam and feedwater lines up to and including the outermost isolation valve;
- (e) Reactor coolant recirculation system components such as pumps, pipes and valves;
- (f) Safety and relief valves and depressurization valves;
- (g) Components such as main steam line flow restrictors, pressure relief equipment, valve actuators and pump drives associated with (a)–(f).

## PRESSURIZED HEAVY WATER REACTORS (PRESSURIZED TUBE TYPE REACTORS)

- (a) Coolant channels including end fitting, closure plug and refuelling machines when connected to a channel;
- (b) Reactor coolant side of the steam generator;
- (c) Reactor coolant pump including seal injection system up to and including the first isolation devices;
- (d) Pipes that, together with the steam generators and the reactor coolant pumps, constitute the coolant loops:
  - Inlet and outlet feeder pipes,
  - Reactor inlet and outlet headers,
  - Pump suction headers (if any);
- (e) Pressurizer (if any) with its relief valves and piping connecting it to the coolant loop piping;
- (f) Overpressure protection lines up to and including relief valves;
- (g) Systems connected to the coolant loop piping up to and including the first isolation devices;
- (h) Moderator system;
- (i) Components such as valve actuators and pump drives associated with (c)–(h).



## PRESSURIZED HEAVY WATER REACTORS (VESSEL TYPE)

- (a) Reactor vessel with closure head, closure plug and refuelling machine when connected to a channel;
- (b) Reactor vessel internals (other than fuel assemblies);
- (c) Reactor coolant side of steam generators;
- (d) Reactor coolant pumps, including the first stage seals and self-seal injection system up to and including isolation devices;
- (e) Pipes that, together with the steam generators and the reactor coolant pumps, constitute the coolant loops:
  - A hot leg between the reactor vessel and each steam generator,
  - A crossover leg between each steam generator and its corresponding main pump,
  - A cold leg between each main pump and the reactor vessel;
- (f) The pressurizer with its relief valves and safety valves, piping and surge line;
- (g) Reactor vessel appurtenances such as the pressure housing for the control rod drive mechanism;
- (h) The moderator side of moderator coolers;
- (i) Moderator pumps;
- (j) Pipes that, together with moderator coolers and moderator pumps, constitute the moderator loops;
- (k) Systems connected to the coolant and moderator loop piping, up to and including isolation devices;
- (l) Components such as valve actuators, flow restrictors and pump drives associated with (a)–(k).


















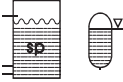



## **Annex II**

### **DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS**

II-1. The following diagrams of the RCSAs present the principal components and main functional features of several reactor types in a simplified form.

II-2. Not all redundant components and piping arrangements are shown. Also, the diagrams are only typical of reactor systems of certain sizes (and powers) and may differ for other reactor systems. For the RCSs, for instance, only one of the multiple loops is shown.

II-3. System names differ from design to design and are sometimes specific to a single vendor. They are intended to be self-explanatory and they may not always correspond to the names of systems or functions as used in this Safety Guide.

	Blowdown tank		Piping
	Check valve		--Connection to other services (outside the scope of this Safety Guide)
	Condenser		Pump
	Coolant (environment)		Regenerative heat exchanger
	Filter		Spray nozzle
	Generator		Steam generator
	Heater		Storage tank
	Heat exchanger		Sump, reservoir
	Loaded safety valve		Tank
	Motor		Turbine
			Valve

ACC	Accumulator	LHP	Low head injection pump
ADS	Automatic depressurization system	PRT	Pressurizer relief tank
CICS	Chemical and inventory control system	PS	Pressurizer
CS	Containment sump	RCIC	Reactor core isolation cooling
CST	Condensate storage tank	RCS	Reactor coolant system
ECC	Emergency core cooling	RHRS	Residual heat removal system
ECCS	Emergency core cooling system	RPV	Reactor pressure vessel
EFS (AFS)	Emergency (auxiliary) feedwater system	RS	Recirculation system
FWS	Feedwater system	RWCS	Refuelling water cleanup system
HHP	High head injection pump	SG	Steam generator
ICC	Intermediate cooling circuit	SP	Suppression pool
		UHS	Ultimate heat sink

FIG. II-1. Explanation of symbols and abbreviations used in Figs II-2-II-4.

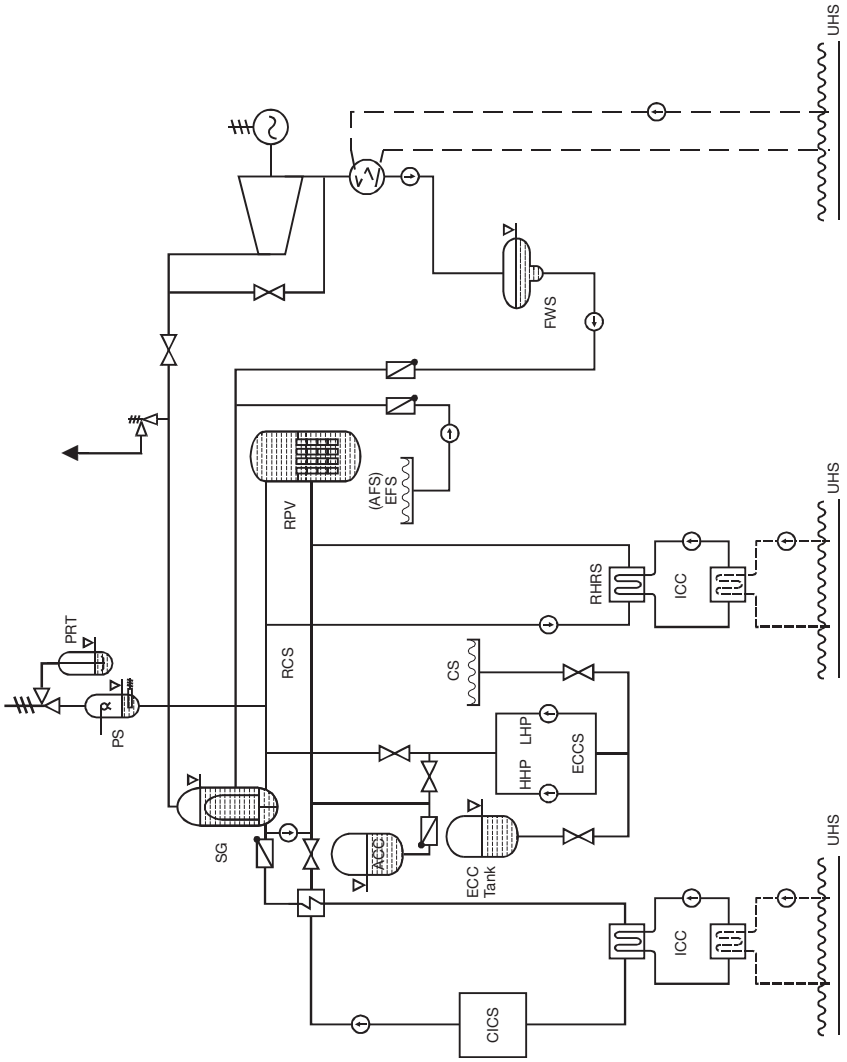
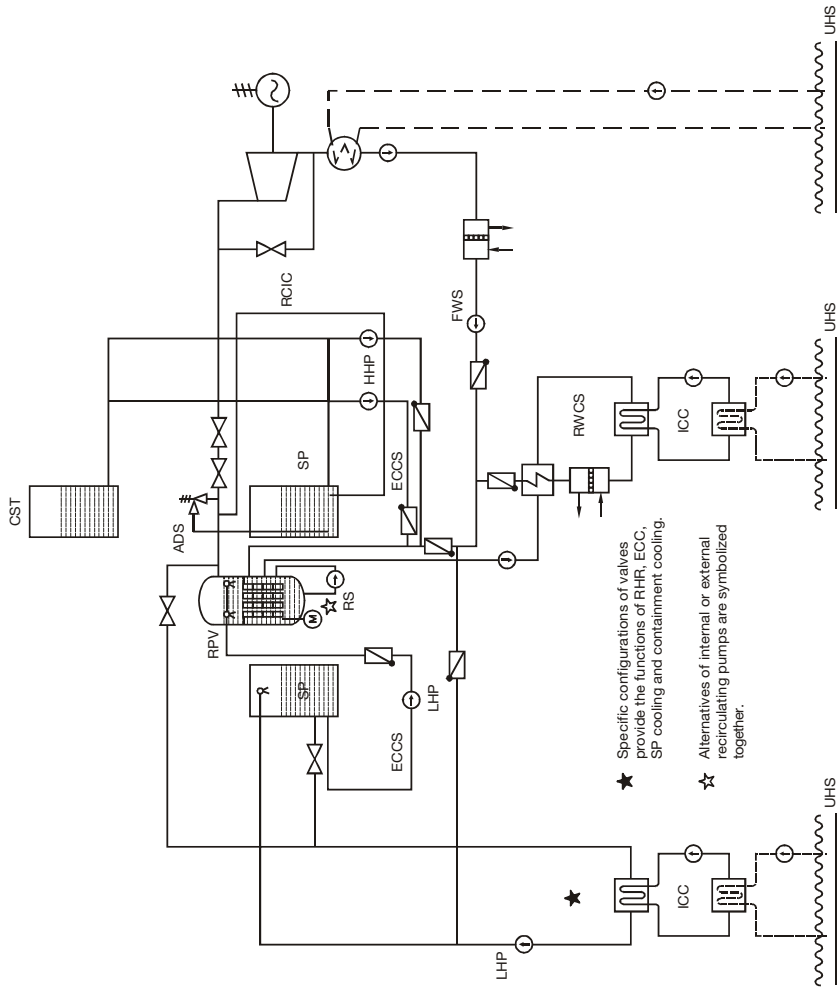


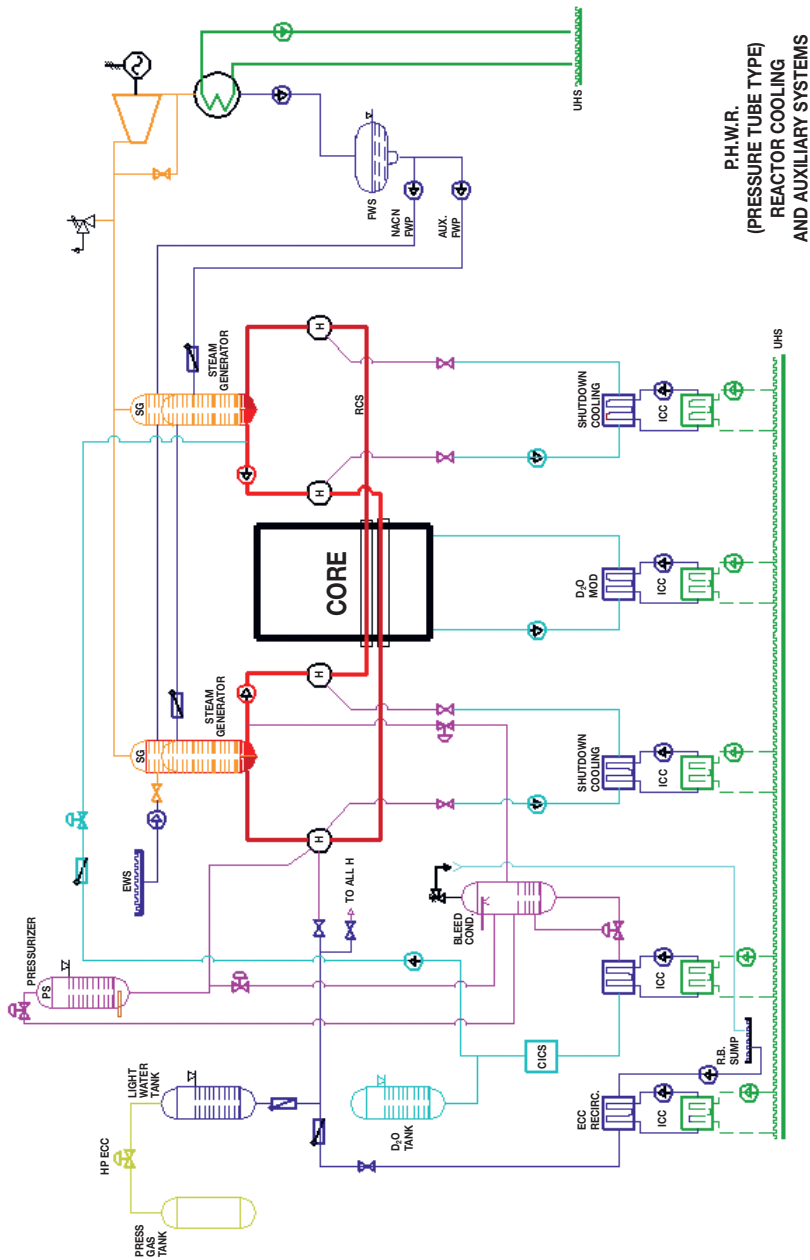
FIG. II-2. RCSAs for a PWR.



★ Specific configurations of valves provide the functions of RHR, ECC, SP cooling and containment cooling.

☆ Alternatives of internal or external recirculating pumps are symbolized together.

FIG. II-3. RCSAs for a BWR.



P.H.W.R.  
(PRESSURE TUBE TYPE)  
REACTOR COOLING  
AND AUXILIARY SYSTEMS

FIG. II-4. RCSAS for a PHWR (pressure tube type reactor).

## **Annex III**

### **SAFETY CLASSIFICATION AND SAFETY CLASS INTERFACE DEVICES FOR FLUID SYSTEMS**

III-1. This annex gives an example of safety classification principles (see under Safety classification in Section 3). In the example presented, four safety classes are used. These four safety classes are briefly described in the following.

#### **DEFINITION OF THE SAFETY CLASSES**

III-2. Safety class 1 includes those safety functions necessary to prevent, in the absence of the appropriate action of safety systems, the release of a substantial fraction of the core inventory of fission products to the environment.

III-3. Safety class 2 includes those safety functions necessary to mitigate the consequences of an accident that would otherwise lead to the release of a substantial fraction of the core inventory of fission products to the environment. The consequences of failure of these safety class 2 functions need only be considered after an initial failure of another safety function.

III-4. Safety class 2 also includes those safety functions necessary to prevent anticipated operational occurrences from leading to accident conditions, except for those safety functions that perform a supporting function to another safety function, namely the following safety functions:

- To transfer heat from other safety systems to the ultimate heat sink;
- To ensure that the necessary services (e.g. the supply of electric power, pneumatic power and hydraulic power, lubrication) are provided as a support function for a safety system;
- To maintain control of the environmental conditions within the nuclear power plant for ensuring the operation of safety systems.

III-5. Safety class 2 also includes other functions whose failure could result in major consequences, and for which there would be a high probability of being demanded in an event, such as the removal of the residual heat from the reactor.

III-6. Safety class 3 includes those safety functions that support safety functions in safety classes 1 and 2.

III-7. Safety class 3 also includes those safety functions necessary to prevent the radiation exposure of the public or of site personnel due to sources outside the RCS from exceeding the applicable limits, and those safety functions associated with reactivity control on a longer time-scale than the reactivity control functions in safety classes 1 and 2. Additionally, safety class 3 includes the safety functions associated with maintaining the subcriticality of fuel stored outside the RCS and with removing decay heat from irradiated fuel stored outside the RCS.

III-8. Safety class 4 includes those safety functions that do not fall into safety class 1, 2 or 3.

III-9. As noted above, the safety classification leads to a set of grade design recommendations (including recommendations with regard to mechanical design, quality, fabrication and inspection). For safety class 4, the design recommendations need to be consistent with normal codes and standards for non-nuclear power plants. For higher safety classes, the design recommendations will be increasingly restrictive and stringent.

## SAFETY CLASSIFICATION

III-10. Safety class 1 includes all components that comprise the RCS pressure boundary,<sup>1</sup> except those whose failure could result in a loss of reactor coolant within the normal operation capability of the coolant inventory control systems, so that sufficient inventory can be maintained for an orderly shutdown and cooldown.

III-11. Safety class 2 includes those components that are part of the RCS pressure boundary and are not in safety class 1. In addition, safety class 2 includes those components that are necessary to accomplish the following safety functions:

---

<sup>1</sup> The RCS pressure boundary comprises those components whose failure could cause a loss of coolant from the reactor core and that cannot be isolated from the core by means of an appropriate interface.



- To maintain a sufficient inventory of reactor coolant for core cooling during and after design basis accidents that do not involve the failure of the RCS pressure boundary (for BWRs, this applies only to appropriate parts of the steam and feedwater systems);
- To remove heat from the core<sup>2</sup> after a failure of the RCS pressure boundary in order to limit fuel damage;
- To remove residual heat (see footnote 3) in operational states and in design basis accident conditions, with the pressure boundary of the RCS intact.

III-12. Safety class 3 includes those components that are necessary to accomplish the following safety functions:

- To prevent unacceptable reactivity transients;
- To maintain the reactor in a safe shutdown condition after all shutdown actions;
- To maintain a sufficient inventory of reactor coolant for cooling the core in and after all operational states;
- To transfer heat from other safety systems to the ultimate heat sink;
- To ensure the provision of the necessary services (e.g. the supply of electrical power, pneumatic power and hydraulic power, lubrication) as a support function for a safety system.

## SAFETY CLASS INTERFACE DEVICES

III-13. Typical interface devices are:

- *Passive barriers (such as heat exchanger tubes)*. For heat exchanger tubes with the possibility of experiencing shock loads under accident conditions or when tube failures are assumed as the single failure of a passive component, the adequacy of these tubes as the sole barrier should be determined and additional measures should be taken if necessary.
- *Remotely operated valves*. Closure times of valves that are normally open and are assumed to be safety class boundaries should be such that the safety function of the components in the higher safety class is maintained.

---

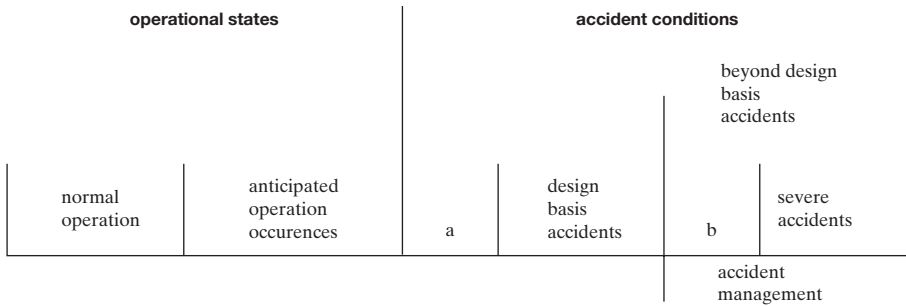
<sup>2</sup> This safety function applies to the first step of the action of the heat removal system(s). The remaining step(s) are encompassed in another safety function, i.e. to transfer heat from other safety systems to the ultimate heat sink.

The closure times of such valves, for example those in steam and feedwater lines, should be specified in the design.

- *Manually operated valves.* Specific administrative procedures should be established to ensure the correct operation of manually operated valves. In addition, it should be demonstrated that there is a means of detecting whether such a valve has been inadvertently left in the wrong state and determining whether there is time to restore the correct state before unacceptable consequences occur.
- *Passive flow restriction devices.* The letdown orifice of the RCS for PWRs, which restricts the flow rate for coolant from the RCS to a value that ensures that the discharge of the RCS is within the normal capability for make-up of primary coolant, is an example of such an interface.
- *Active flow restriction devices.* The letdown valves of the RCS, which restrict the flow rate for coolant from the RCS to a value that ensures that the discharge of the RCS is within the normal capability for make-up of primary coolant, are examples of such an interface.

# GLOSSARY

## plant states



- Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.
- Beyond design basis accidents without significant core degradation.

**accident conditions.** Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents.

**accident management.** The taking of a set of actions during the evolution of a beyond design basis accident:

- to prevent the escalation of the event into a severe accident;
- to mitigate the consequences of a severe accident;
- to achieve a long term safe stable state.

**anticipated operational occurrence.** An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

**design basis accident.** Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

**normal operation.** Operation within specified operational limits and conditions.

**operational states.** States defined under normal operation and anticipated operational occurrences.

**severe accident.** Accident conditions more severe than a design basis accident and involving significant core degradation.

**protection system.** A system which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

**safety function.** A specific purpose that must be accomplished for safety.

**safety system.** A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

**single failure.** A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.

**ultimate heat sink.** A medium to which the residual heat can always be transferred, even if all other means of removing the heat have been lost or are insufficient.

## **CONTRIBUTORS TO DRAFTING AND REVIEW**

Benedetti, C.	Consultant, France
Eltawila, F.	Nuclear Regulatory Commission, United States of America
Inagaki, T.	International Atomic Energy Agency
Mertins, M.	Gesellschaft für Anlagen und Reaktorsicherheit GmbH, Germany
Nuzzo, F.	Atomic Energy of Canada Ltd, Canada
Pedersen, T.	ABB Atom AB, Sweden
Tezuka, H.	International Atomic Energy Agency
Vidard, M.	Electricité de France/SEPTEN, France
Zama, T.	Tokyo Electric Power Company, Japan



## **BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS**

*An asterisk (\*) denotes a corresponding member. Corresponding members receive drafts for comment and other documentation but they do not generally participate in meetings.*

### **Commission on Safety Standards**

*Argentina: Oliveira, A.; Brazil: Caubit da Silva, A.; Canada: Pereira, J.K.; France: Gauvain, J.; Lacoste, A.-C.; Germany: Renneberg, W.; India: Sukhatme, S.P.; Japan: Tobioka, T.; Suda, N.; Korea, Republic of: Eun, S.; Russian Federation: Malyshev, A.B.; Vishnevskiy, Y.G.; Spain: Azuara, J.A.; Santoma, L.; Sweden: Holm, L.-E.; Switzerland: Schmocker, U.; Ukraine: Gryschenko, V.; United Kingdom: Hall, A.; Williams, L.G. (Chairperson); United States of America: Travers, W.D.; IAEA: Karbassioun, A. (Co-ordinator); International Commission on Radiological Protection: Clarke, R.H.; OECD Nuclear Energy Agency: Shimomura, K.*

### **Nuclear Safety Standards Committee**

*Argentina: Sajaroff, P.; Australia: MacNab, D.; \*Belarus: Sudakou, I.; Belgium: Govaerts, P.; Brazil: Salati de Almeida, I.P.; Bulgaria: Gantchev, T.; Canada: Hawley, P.; China: Wang, J.; Czech Republic: Böhm, K.; \*Egypt: Hassib, G.; Finland: Reiman, L. (Chairperson); France: Saint Raymond, P.; Germany: Feige, G.; Hungary: Vöröss, L.; India: Kushwaha, H.S.; Ireland: Hone, C.; Israel: Hirshfeld, H.; Japan: Yamamoto, T.; Korea, Republic of: Lee, J.-I.; Lithuania: Demcenko, M.; \*Mexico: Delgado Guardado, J.L.; Netherlands: de Munk, P.; \*Pakistan: Hashimi, J.A.; \*Peru: Ramírez Quijada, R.; Russian Federation: Baklushin, R.P.; South Africa: Bester, P.J.; Spain: Mellado, I.; Sweden: Jende, E.; Switzerland: Aeberli, W.; \*Thailand: Tanipanichskul, P.; Turkey: Alten, S.; United Kingdom: Hall, A.; United States of America: Mayfield, M.E.; European Commission: Schwartz, J.-C.; IAEA: Bevington, L. (Co-ordinator); International Organization for Standardization: Nigon, J.L.; OECD Nuclear Energy Agency: Hrehor, M.*

## **Radiation Safety Standards Committee**

*Argentina: Rojkind, R.H.A.; Australia: Melbourne, A.; \*Belarus: Rydleviski, L.; Belgium: Smeesters, P.; Brazil: Amaral, E.; Canada: Bundy, K.; China: Yang, H.; Cuba: Betancourt Hernandez, A.; Czech Republic: Drabova, D.; Denmark: Ulbak, K.; \*Egypt: Hanna, M.; Finland: Markkanen, M.; France: Piechowski, J.; Germany: Landfermann, H.; Hungary: Koblinger, L.; India: Sharma, D.N.; Ireland: Colgan, T.; Israel: Laichter, Y.; Italy: Sgrilli, E.; Japan: Yamaguchi, J.; Korea, Republic of: Kim, C.W.; \*Madagascar: Andriambololona, R.; \*Mexico: Delgado Guardado, J.L.; \*Netherlands: Zuur, C.; Norway: Saxebol, G.; \*Peru: Medina Gironzini, E.; Poland: Merta, A.; Russian Federation: Kutkov, V.; Slovakia: Jurina, V.; South Africa: Olivier, J.H.I.; Spain: Amor, I.; Sweden: Hofvander, P.; Moberg, L.; Switzerland: Pfeiffer, H.J.; \*Thailand: Pongpat, P.; Turkey: Uslu, I.; Ukraine: Likhtarev, I.A.; United Kingdom: Robinson, I. (Chairperson); United States of America: Paperiello, C.; European Commission: Janssens, A.; IAEA: Boal, T. (Co-ordinator); International Commission on Radiological Protection: Valentin, J.; International Labour Office: Niu, S.; International Organization for Standardization: Perrin, M.; International Radiation Protection Association: Webb, G.; OECD Nuclear Energy Agency: Lazo, T.; Pan American Health Organization: Jimenez, P.; United Nations Scientific Committee on the Effects of Atomic Radiation: Gentner, N.; World Health Organization: Carr, Z.*

## **Transport Safety Standards Committee**

*Argentina: López Vietri, J.; Australia: Colgan, P.; \*Belarus: Zaitsev, S.; Belgium: Cottens, E.; Brazil: Mezrahi, A.; Bulgaria: Bakalova, A.; Canada: Viglasky, T.; China: Pu, Y.; \*Denmark: Hannibal, L.; Egypt: El-Shinawy, R.M.K.; France: Aguilar, J.; Germany: Rein, H.; Hungary: Sáfár, J.; India: Nandakumar, A.N.; Ireland: Duffy, J.; Israel: Koch, J.; Italy: Trivelloni, S.; Japan: Saito, T.; Korea, Republic of: Kwon, S.-G.; Netherlands: Van Halem, H.; Norway: Hornkjøl, S.; \*Peru: Regalado Campaña, S.; Romania: Vieru, G.; Russian Federation: Ershov, V.N.; South Africa: Jutle, K.; Spain: Zamora Martin, F.; Sweden: Pettersson, B.G.; Switzerland: Knecht, B.; \*Thailand: Jerachanchai, S.; Turkey: Köksal, M.E.; United Kingdom: Young, C.N. (Chairperson); United States of America: Brach, W.E.; McGuire, R.; European Commission: Rossi, L.; International Air Transport Association: Abouchaar, J.; IAEA: Wangler, M.E. (Co-ordinator); International Civil Aviation Organization: Rooney, K.; International Federation of Air Line Pilots' Associations: Tisdall, A.; International Maritime Organization: Rahim, I.; International Organization for*



*Standardization: Malesys, P; United Nations Economic Commission for Europe: Kervella, O.; World Nuclear Transport Institute: Lesage, M.*

### **Waste Safety Standards Committee**

*Argentina: Siraky, G.; Australia: Williams, G.; \*Belarus: Rozdialovskaya, L.; Belgium: Baekelandt, L. (Chairperson); Brazil: Xavier, A.; \*Bulgaria: Simeonov, G.; Canada: Ferch, R.; China: Fan, Z.; Cuba: Benitez, J.; \*Denmark: Øhlenschlaeger, M.; \*Egypt: Al Adham, K.; Al Sorogi, M.; Finland: Ruokola, E.; France: Averous, J.; Germany: von Dobschütz, P.; Hungary: Czoch, I.; India: Raj, K.; Ireland: Pollard, D.; Israel: Avraham, D.; Italy: Dionisi, M.; Japan: Irie, K.; Korea, Republic of: Song, W.; \*Madagascar: Andriambololona, R.; Mexico: Aguirre Gómez, J.; Delgado Guardado, J.; Netherlands: Selling, H.; \*Norway: Sorlie, A.; Pakistan: Hussain, M.; \*Peru: Gutierrez, M.; Russian Federation: Poluektov, P.P.; Slovakia: Konecny, L.; South Africa: Pather, T.; Spain: López de la Higuera, J.; Ruiz López, C.; Sweden: Wingefors, S.; Switzerland: Zurkinden, A.; \*Thailand*