

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



Documents

Document Sharing Hub

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/

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	TAJIKISTAN
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

IAEA NS-G-1.9 2004

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 RCSAs. 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).¹ 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;²
- Residual heat removal systems;

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

² 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;³
- 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;

³ 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 uncontrolled⁴ 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 RCSAs as defined in paras 3.2 and 3.3 should not be compromised by the failure of the components of the RCSAs.

3.7. The design recommendations for the RCSAs 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 RCSAs.

SAFETY SYSTEMS IN THE RCSAs

3.8. Some connected and associated systems in the RCSAs 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 RCSAs 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.

⁴ 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 RCSAs 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 RCSAs 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 RCSAs 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 RCSAs 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 RCSAs 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.⁵

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 RCSAs. 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 RCSAs should also be considered, in accordance with Ref. [1].

3.23. Examples of PIEs that could significantly influence the design of the RCSAs 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;

⁵ 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 RCSAs 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 RCSAs 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 RCSAs, 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 RCSAs 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 RCSAs 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.