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

Draft DS 481

September 2016

C-41 (May 13)

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 systems for nuclear power plants are established in the safety requirement publication, safety standards series no. SSR 2/1 Rev. 1 on safety of nuclear power plants: design [2], which it supplements.

1.2 This publication is a revision of a Safety Guide published in 2004 as IAEA Safety Standards Series No. NS-G-1.9, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, and supersedes it.

OBJECTIVE

1.3 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 Reactor Coolant System (RCS) and associated systems, hereinafter referred to as RCSASs.

1.4 This Safety Guide aims at providing engineering recommendations for the design of the RCSASs as identified in section 2 of this document in order to meet the requirements established in Ref. [2] for these systems.

SCOPE

1.5 This Safety Guide applies primarily to land based stationary nuclear power plants with water cooled reactors designed for electricity generation. 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 Recommendations given in this Safety Guide are targeted primarily to new nuclear power plants. For plants designed with earlier standards, comprehensive safety assessments are to be carried out considering these recommendations in order to identify safety improvements that are oriented to prevent accidents with radiological consequences and mitigate such consequences should they occur. Reasonably practicable or achievable safety improvements are to be implemented in a timely manner.

1.7 Section 2 provides the scope of RCSASs addressed in this Safety Guide. To be design independent to the extent possible, design recommendations are given on the basis of the safety functions to be accomplished by the systems.

1.8 Design limits and engineering criteria, together with the system parameters that should be used to verify them, are design specific and are therefore outside the scope of this Safety Guide. However, qualitative recommendations are provided.

STRUCTURE

1.9 Section 2 describes the scope of the RCSASs addressed in this Safety Guide.

1.10 Section 3 provides generic design recommendations that are common to Pressurized Water Reactor (PWR), Boiling Water Reactor (BWR) and Pressurized Heavy Water Reactor (PHWR) technologies, and that apply to RCSASs designed to control the core reactivity and to remove residual decay heat from the RCS in all plant states without a molten core.

1.11 Section 4 provides design recommendations for the different heat transfer chains and generic considerations for the Ultimate Heat sink (UHS).

1.12 Sections 5, 6 and 7 provide supplementary design recommendations which are specific to systems for PWR, BWR and PHWR technologies, respectively.

1.13 The Annexes I, II and III provide diagrams of the reactor coolant system and associated systems for PWR, BWR and PHWR technologies, respectively.

2 EXTENT OF THE RCS AND ASSOCIATED SYSTEMS

2.1 Guidance and recommendations provided by this publication apply to RCSASs designed for the following functions:

- Provide and maintain adequate core cooling conditions to ensure compliance with fuel design limits in operational states;
- Maintain sufficient coolant inventory and cooling conditions to prevent to the extent practical significant fuel damage in accident conditions;
- Remove decay heat from the core and transfer residual heat from RCS to the ultimate heat sink in operational states and in accident conditions;
- Prevent an uncontrolled loss of inventory at the reactor coolant pressure boundary;
- Protect the RCS against over pressure,
- Shut-down the reactor and control the core reactivity to ensure compliance with fuel design limits in operational states and in accident conditions;
- Perform a depressurization of the RCS in accident conditions.

REACTOR COOLANT SYSTEM

2.2 For all reactor types, the RCS includes the components necessary to provide and maintain the adequate core cooling conditions for the fuel in operational states (pressure, temperature, and coolant inventory and coolant flow rate). However fuel elements and control rods for controlling the core reactivity and shutting down the reactor elements are not addressed in this Safety Guide but in Ref. [2].

2.3 For all water cooled reactor types, the reactor coolant pressure boundary of the RCS extends up to and including the outermost isolation device(s).

2.4 For indirect cycle reactors, i.e. PWRs, the pressure retaining boundary of the RCS includes the primary side of the steam generators (see section 5). For direct cycle reactors, i.e. BWRs, the pressure retaining boundary of the RCS also includes the primary coolant recirculation system and the steam and feed water lines up to and including the outermost containment isolation valve (see section 6). Specific features of PHWRs are provided in section 7.

SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES

2.5 Those systems are systems designed to remove residual heat from the reactor coolant system during operational states. They include systems that operate once the reactor is shut down and systems to cool down RCS to cold shut-down condition including refuelling condition for PWR and BWR.

SYSTEMS FOR COOLANT INVENTORY IN OPERATIONAL STATES

2.6 Those systems are systems designed to compensate leaks and to control the reactor coolant inventory in operational conditions.

SYSTEMS FOR CORE REACTIVITY CONTROL IN OPERATIONAL STATES

2.7 Those systems are systems designed to control the core axial off set in power operation and to control margins to re- criticality in shut-down modes.

SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS

2.8 Those systems are systems designed to remove decay heat from the core in the event of accident with or without a loss of the RCS integrity, systems designed to remove residual heat from and cool RCS in accident conditions till safe shut-down conditions are reached and systems designed to maintain safe shut-down conditions in the long term.

SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS

2.9 Those systems are systems designed to shut down the reactor alone, to stop uncontrolled or excessive positive reactivity insertion caused by accident conditions, to limit fuel damage in the event of Anticipated Transients Without Scram (ATWS) and to ensure the core reactivity control till the safe shut-down conditions are reached in accident conditions.

ULTIMATE HEAT SINK AND RESIDUAL HEAT TRANSFER SYSTEMS IN ALL PLANT STATES

2.10 Heat sink is defined as a medium into which the transferred residual heat can always be accepted, even if all other means of removing the heat have been lost or are insufficient. The ultimate heat sink is usually a body of water, the groundwater or the atmosphere.

2.11 Residual heat transfer systems include systems designed to transfer residual heat from the heat removal systems to the ultimate heat sink.

2.12 Capabilities to discharge of residual heat to the ultimate heat sink suppose that one heat sink and one heat transfer chain at least is always available for the different shut-down modes and shut-down condition.

3 DESIGN BASIS OF RCS AND ASSOCIATED SYSTEMS

This section describes general design concepts and recommendations for design that are common to the RCSASs and that are applicable to all water cooled reactors. Design considerations which are specific to one reactor technology are mentioned in Section 5 for PWR, in Section 6 for BWR and in Section 7 for PHWR.

GENERAL

3.1 The design of RCSASs should be conducted taking into account the recommendations of GS-G-3.1 [21] and GS-G-3.5 [22] to meet the requirements 1 to 3 of SSR-2/1 Rev.1 [2] and the requirements of GSR Part 2 [3].

3.2 The design of RCSASs should be conducted taking into account design recommendations for safety and security in an integrated manner in such way that safety and security measures do not compromise each other. Recommendations for security are detailed in [4].

3.3 RCSASs are required to be designed in compliance with requirements 46 to 53 of [2], with account taken of all other requirements of [2] relevant for:

- Protection of workers, the public and the environment in all plant states against the effects of ionizing radiation;
- Adequate reliability of the different systems;
- Prevention of early or large radioactive releases.

3.4 To achieve the above mentioned objectives, RCSASs should be designed to accomplish the functions indicated in paragraph 2.1.

3.5 A number of RCSASs are design dependent and may be different in their design principles (e.g. use of active or passive systems for emergency core cooling or for removing residual heat etc.). Nevertheless, systems having to accomplish the same safety function in different technologies should be designed in compliance with similar design requirements.

3.6 A design basis should be defined for every structure, system and component and should specify the following:

- The safety function(s);
- The postulated initiating events they have to cope with;
- The safety classification;
- Design limits and acceptance criteria;

- The protection against the effects of external hazards;
- The protection against the effects of internal hazards;
- The engineering design criteria applicable to the system;
- Recommended instrumentation and monitoring;
- Provisions against common cause failures within a system and between systems belonging to different levels of defence in depth;
- Environmental conditions for qualification;
- Selection of materials;
- Provisions for testing, inspection, maintenance and decommissioning.

SAFETY FUNCTIONS

3.7 The safety functions to be accomplished by the system and the contribution of each major component should be described in a level of detail sufficient for a correct safety classification.

POSTULATED INITIATING EVENTS

3.8 From the list of the postulated initiating events (PIEs) established for the design of the plant, PIEs that affect the design of the RCSASs should be identified, and categorized,

3.9 For each of the conditions above, the list of systems necessary to bring the plant to safe and stable shut-down condition within the applicable acceptance criteria should be established.

3.10 Bounding conditions caused by the PIEs should be determined to define capabilities and performances of equipment.

INTERNAL HAZARDS

The following recommendations provide guidance to fulfil the overarching Requirement 17 of [2] with its associated requirements, and the requirement 5.16 specific to “Internal Hazards”.

3.11 Recommendation provided in [8] should be considered to understand the general concept for a complete identification of the relevant hazards and for an adequate protection of the systems against the effects of the selected internal hazards.

3.12 Items necessary for a safe shutdown of the reactor and for the mitigation of the accident conditions should be protected against the effects of internal hazards. That protection should also consider the consequences of the failures of items non-protected.

3.13 Protection and layout should be adequate to ensure that the modelling of the system response described in the analysis is not compromised by the effects of the PIE.

3.14 Protection of the safety systems should be adequate to give evidence that an internal hazard cannot be a common cause failure for the total loss of the function to be accomplished by the system.

3.15 Methods, design and construction codes used should provide adequate margins to justify that cliff edge effects would not occur in the event of an increase of the severity of the internal hazards.

EXTERNAL HAZARDS

The following recommendations provide guidance to fulfil the requirements relevant for "External Hazards" of Requirement 17 of [2] with its associated requirements and the requirements 5.17-5.21A specific to "External Hazards".

3.16 Recommendations provided in [5] should be considered to understand the general concept for a complete identification of the relevant hazards and for an adequate protection of the systems against the effects of the selected external hazards.

3.17 With regard to the effects of external hazards, physical protection should be applied to the extent possible to prevent damage to RCSASs. Physical protection can rely on an adequate layout and physical protection of the buildings at the site. When physical protection is not effective SSCs should be designed to withstand the hazard loads and their combinations.

3.18 The design of the components of the reactor coolant system should be such that the effects of the external hazards derived from the site evaluation cannot be the cause of an accident for the reactor.

3.19 RCSASs designed to shut down the reactor and to mitigate consequences of accident conditions should be protected against the effects of external hazards or designed to withstand the loads caused by the external hazards.

3.20 For each relevant hazard or likely combinations of hazards, components whose operability or integrity is required during or after the hazard should be identified and specified in the design basis of the components.

3.21 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. [7]. Irrespective of the safety class to which SSCs are assigned, safety systems and safety features for accidents without significant core degradation should be designed to withstand SL-2 seismic loads.

3.22 Methods, design and construction codes used should provide adequate margins to justify that cliff edge effects would not occur in the event of an increase of the severity of the external hazards.

3.23 Margins provided by the design of the associated systems ultimately necessary to avoid an early or a large radiological release (if any) should be large enough so that it can be demonstrated that the integrity and operability of those systems would be preserved in case of natural hazards causing loads exceeding those resulting from the site hazard evaluation.

3.24 In the event of external hazards, short term actions necessary to preserve the reactor coolant pressure boundary (RCPB) integrity and to prevent conditions from escalating to core melting conditions should be accomplished by permanent systems (Requirement 5.17 of [2]).

3.25 Capability for adequate core cooling should be longer than time necessary prior to crediting off-site support services.

ACCIDENT CONDITIONS

3.26 Accident conditions relevant for the design of RCSASs should be accident conditions having the potential to cause excessive mechanical loads to RCS components or those for which cooling of the fuel and the reactor shut-down would no longer be completed with operational systems.

3.27 Accident conditions should be used as inputs for determining capabilities, loads and environmental conditions in the design of the RCSASs structures and systems. Accident conditions to be considered for RCSASs include but not necessarily limited to:

- Loss of coolant accidents (LOCA);
- Steam generator tube rupture(s) (PWR and PHWR);
- Main steam/SG feed water piping break (PWR and PHWR);
- Loss of residual heat removal in shutdown conditions;
- Uncontrolled positive reactivity insertion.

3.28 Codes and engineering rules that are used for design should be documented, validated and, in the case of new codes, developed according to up to date knowledge and recognized standards for quality assurance. Users of the codes should be qualified and trained with respect to the operation and limits of the code and with respect to the assumptions made in the design.

3.29 Calculation of boundary conditions for design basis accidents and design extension conditions should be adequately documented, indicating the relevant assumptions for the evaluation of parameters, the engineering criteria and the computer codes that are used.

3.30 Computer codes should not be used beyond their identified and documented domain of validation.

Design basis accidents

The following recommendations provide guidance to fulfil the overarching requirement 19 of [2].

3.31 Design basis accident (DBA) conditions should be identified and calculated for each of the associated systems.

3.32 For the performances of the RCSASs, design basis accident conditions should be calculated taking into account the least favourable initial conditions and equipment performances, and the single failure[1] which has the largest impact on the performance of the safety systems. Care should be taken when introducing adequate conservatism, since:

- For the same event, as an approach considered conservative for designing one specific system could be non-conservative for another, various analyses should be performed for the different cases;

- Making assumptions too conservative could lead to the imposition of too high stresses on components and structures.

Design extension conditions (without significant fuel degradation)

The following recommendations provide guidance to fulfil the overarching requirement 20 [2].

3.33 Mitigation of design extension conditions (DECs) should be accomplished by permanent systems.

3.34 Design extension conditions should be identified and used to establish the design bases of systems necessary to prevent postulated sequences with multiple failures from escalating to core melting.

3.35 Calculations performed to specify the design bases of RCSASs equipment may be less conservative than those used for design basis accidents provided that margins are still sufficient to cover uncertainties. Performing sensitivity analyses could also be useful to identify the key parameters for which uncertainties should preferably be considered.

---

1 IAEA safety glossary, 2007 edition: A single failure is 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(s) from it.

3.36 DECs relevant for the design of additional safety features should be identified on the basis of engineering judgement as well as deterministic and probabilistic assessment.

3.37 As typical examples, the following three types of DECs should be considered:

- Very unlikely events that could lead to situations beyond the capability of the safety systems to meet acceptance criteria relevant for DBAs;
- Multiple failures (e.g. common cause failures in redundancies) that prevent the safety systems from performing their intended function to control the PIE;
- Multiple failures that cause the loss of the heat transfer chain to the Ultimate Heat Sink while the chain is operated in normal operation.

3.38 As multiple failures are likely caused by the occurrence of dependent failures that may lead to the failure of the safety systems, an analysis of dependencies between redundant trains of safety systems or between diverse installed capabilities to shut down the reactor, to remove residual heat from the core and transfer residual heat to the ultimate heat should be conducted to identify relevant possibilities for DECs.

3.39 Following conditions could be considered as generic candidates for design extension conditions relevant for the design of RCSAS systems:

- Station Blackout;
- Anticipated Transient Without Scram (PWR and BWR);
- Total loss of the feed water systems (PWR and PHWR);
- Small LOCA with failures in the emergency core cooling system;
- Loss of residual heat transfer systems to the ultimate heat sink;
- Loss of the ultimate heat sink.

DESIGN LIMITS AND CRITERIA

The following recommendations provide guidance to fulfil the overarching requirements 15 and 28 of [2].

3.40 The performance of RCSASs should be defined and specified to fulfil a well-defined and accepted[2] set of design limits and criteria.

- RCS components should be designed so that the relevant limits for process parameters and stresses ensuring their integrity and operability, when required, are not exceeded;

- Associated systems should be designed so that the relevant design limits and criteria for fuel are not exceeded;

- Associated systems should be designed not to cause unacceptable stresses on the reactor coolant pressure boundary.

3.41 Design limits and criteria should be specified for each plant state category.

RELIABILITY

The following recommendations provide guidance to fulfil the overarching requirements 21, 22, 23, 24, 25, 26, 29 and 30 of [2].

3.42 The following factors should be considered to achieve the adequate reliability of the systems necessary to control reactivity of the core, to remove residual heat from fuel and to transfer residual heat to the ultimate heat sink:

- Safety classification and the associated engineered requirements for design and manufacturing;

- Design criteria relevant for the systems (number of redundant trains, seismic qualification, qualification to harsh environmental conditions, power supplies);

- Prevention of common cause failures by implementation of suitable defensive measures such as diversity, physical separation, functional independence;

- Layout provisions to protect the system against the effects of internal and external hazards;

- Periodic testing and inspection;

- Maintenance;

- Use of equipment designed to fail-in a safe direction.

[2] 'Well defined and accepted' generally means either widely accepted by Member State regulatory bodies or proposed by international organizations.

Systems designed to mitigate design basis accidents

3.43 Shutting down the reactor, cooling of the core, control of the core reactivity, residual heat removal and transfer to the ultimate heat sink in the event of design basis accidents should be possible despite the consequential failures caused by the postulated initiating event and a single failure postulated in any system needed to accomplish the function. Additionally, unavailability for maintenance or repair should be considered.

3.44 Systems operated to maintain the reactor in a safe state in the long term should be designed to accomplish their function despite a single failure postulated in any of those systems.

3.45 The on-site AC power source (Emergency power source) should have adequate capability to supply power to electrical equipment operated in DBA conditions for shutting down the reactor, cooling the core, removing and transferring residual heat removal to the ultimate heat sink and for maintaining the reactor in a safe state in the long term [9].

3.46 Adequate physical separation should be implemented between the redundancies of the safety systems to prevent common cause failure due to the effects of hazards considered for design.

3.47 Recommendations related to the reliability of the system with regard to the effects of internal or external hazards and environmental conditions are addressed in paragraphs 3.12, 3.13, 3.14 and 3.21, respectively.

Safety features for design extension conditions without significant fuel degradation

3.48 A reliability analysis of the safety systems designed to remove residual heat and to transfer residual heat to the ultimate heat sink should be conducted to identify needs for additional safety features in order to reinforce prevention of core melting.

3.49 The more likely combinations of PIEs and common cause failure (CCF) between the redundancies of the safety systems should be analyzed. If consequences exceed the limits given for DBAs, reliability of the safety systems should be improved (e.g. vulnerabilities for CCF should be removed) or additional design features should be implemented to prevent escalation to core melt accident in such events. The additional features for residual heat removal and residual heat transfer should be designed and installed such that they should be unlikely to fail for the same cause.

3.50 Additional safety features should have an adequate reliability to meet the core damage frequency target.

3.51 Similar recommendations as indicated for systems designed to mitigate design basis accidents should be applied, taking into account that meeting the single failure criterion is not required, that additional safety features for DECs are supplied by the Alternate AC power source and that the relevant additional features are expected to be unlikely to fail for the same CCF leading to the failure of the systems designed for design basis accidents.

DEFENCE IN DEPTH

The following recommendations provide guidance to fulfil Requirement 7 of [2].

3.52 Alternative means belonging to different levels of defence, necessary to shut down the reactor or to accomplish residual heat removal and heat transfer to the ultimate heat sink in the different plant states should be implemented .

3.53 Vulnerabilities for CCF between those items should be identified and the consequences assessed. The vulnerabilities for CCF should be removed to the extent possible where escalation to core melt accident would be the consequence.

3.54 Independence implemented between systems should not be compromised by CCF in I&C systems or other support systems necessary for their actuation and operation.

3.55 Instrumentation for safety system actuation and for monitoring of plant status should be independent to the extent practical.

SAFETY CLASSIFICATION

The following recommendations provide guidance to fulfil the overarching requirement 22 of [2].

3.56 Consequences of a SSC failure should be considered both on the accomplishment of the function, and on the level of the radioactive release. For items for which both effects are relevant, the safety class and the associated quality requirements needed to achieve the expected reliability are defined with due account taken of those two effects. For items which do not contain radioactive materials the safety class and the quality requirements are directly derived from the consequences assuming that the function is not accomplished.

3.57 Engineering requirements applicable to the design of a whole system (e.g. single failure criterion, independence, emergency power supplied, etc.) should be derived from the consequences assuming that the function is not accomplished.

3.58 The classification should be established in a consistent manner such that all systems necessary for the accomplishment of a single function are assigned in the same class or justification should be provided.

3.59 Pressure retaining equipment should be designed and manufactured according to requirements established by proven codes and standards widely accepted by industry.

3.60 According to recommendations given in the Safety Guide SSG-30 [10]:

- Systems designed not to exceed the dose limits accepted in the event of a design basis accident should be assigned in SSG-30 safety class 1 or may be assigned in SSG-30 safety class 2 if they are needed to bring the reactor to a safe state;

- Systems implemented as a back-up of the safety systems for design extension conditions should be assigned at least in SSG-30 safety class 2;

- Systems designed to keep the key reactor parameters (e.g. pressure temperature, pressurizer water level, steam generator water level) within their range specified for normal operation should be at least assigned in SSG-30 safety class 3;

- Systems designed for normal operation and whose failure would not lead to radiological consequences exceeding the limit specified for operational conditions need not be safety classified.

3.61 The application to RCSASs is indicated in sections 5, 6 and 7.

3.62 More detailed guidance is given in the Safety Guide SSG-30 [10].

ENVIRONMENTAL QUALIFICATION

The following recommendations provide guidance to fulfil the overarching requirement 30 of [2].

3.63 RCSASs components and instrumentation should be qualified to perform their functions in the entire range of environmental conditions that might prevail prior to or during their operation within mission time, or should otherwise be adequately protected from those environmental conditions.

3.64 The relevant environmental and seismic conditions that may prevail prior to, during and following an accident, the ageing of structures, systems and components throughout the lifetime of the plant, synergistic effects, and margins should all be taken into consideration in the environmental qualification [11].

3.65 Environmental qualification should be carried out by means of testing, analysis and the use of experience, or by a combination of these.

3.66 Environmental qualification should include the consideration of such factors as temperature, pressure, humidity, radiation levels, and local accumulation of radioactive aerosols, vibration, water spray, steam impingement, flooding and contact with chemicals. Margins and synergistic effects (in which the damage due to the superposition or combination of effects may exceed the total damage due to the effects separately) should also be considered. In cases where synergistic effects are possible, materials should be qualified for the most severe effect, or the most severe combination or sequence of effects.

3.67 Techniques to accelerate the testing for ageing and qualification can be used, provided that there is an adequate justification.

3.68 For components subject to the effects of ageing by various mechanisms, design life time and, if necessary, the replacement frequency should be established. In the qualification process for such components, samples should be aged to simulate the end of their design lives before being tested under design basis accident conditions.

3.69 Components that have been used for qualification testing should generally not be used for construction purposes.

3.70 Qualification data and results should be documented as part of the design documentation.

LOADS AND LOAD COMBINATIONS

3.71 The design basis of each component of the RCSASs should include, for each plant state, the loads and load combinations that components must withstand.

3.72 Loading conditions, loads and stresses should be calculated applying adequate methodology and rules giving confidence in the robustness of the design and margins to cover uncertainties and avoid cliff edge effects.

- Uncertainties in process parameters;
- Uncertainties in initial conditions and performances of systems or components;
- Uncertainties in models,
- Structural tolerances;
- Uncertainties in relation to the decay heat;

3.73 All loads (static and dynamic) that are foreseen to occur should be quantified and grouped according to their probability of occurrence, on the basis of operating experience and engineering judgment.

3.74 Loads should be identified and analysed with account taken of:

- Load type (i.e. static and permanent loads, or transients and dynamic, global or local);

- Timing of each load (to avoid the unrealistic superposition of load peaks if they cannot occur coincidently).

3.75 Design basis loading conditions should be assigned in different categories (e.g. Normal conditions, Upset conditions, Emergency conditions, Faulted conditions) according to their estimated frequency of occurrence[3] or according to requirements of accepted codes and regulations.

3.76 The appropriate stress levels to be met for integrity should be defined and be appropriate to each load combination with account taken of the load combination category. The stress levels may be different for the different types of damage (e.g. progressive deformation and fatigue or excessive deformation and plastic instability). Meeting the criteria given by codes and standards internationally recognized provides reasonable assurance that structures and components are capable of performing their intended functions.

3.77 When operability needs to be demonstrated, additional analyses or tests should be conducted by applying the relevant stress limits.

3.78 Normal service and upset conditions should be defined by modelling the plant response under realistic conditions.

3.79 Emergency and faulted conditions should be defined with conservatism: e.g.by taking unfavourable uncertainties in the initial conditions, in performances of the systems and not crediting the operational systems and controls when their operation is favourable.

3.80 SSCs necessary for the mitigation of accident conditions should be designed to withstand the effects of natural phenomena in order to keep their capability to perform their intended safety functions. The design bases of these SSCs should reflect appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena.

---

[3] • Normal service conditions: loading conditions to which the equipment may be subjected during in the course of normal operation including normal operating transients and start up/shutdown conditions;
• Upset conditions: loading conditions to which the equipment may be subjected during transients resulting from the occurrence of a PIE categorized as an AOO;
• Emergency conditions: loading conditions to which the equipment may be subjected during transients resulting from the occurrence of a PIE categorized as an accident of low frequency;
• Faulted conditions: loading conditions to which the equipment may be subjected during transients resulting from the occurrence of a PIE categorized as an accident of very low frequency

3.81 SSCs designed to accomplish their functions in plant conditions categorized as "emergency conditions" or "faulted conditions" should be designed to meet adequate[4] service limit ensuring their integrity and operability (when required) while subjected to sustained loads resulting from system operation in the event of PIEs for which they are designed to respond.

MATERIALS

The following recommendations provide guidance to fulfil the overarching requirement 47 of [2].

3.82 The materials used for the pressure retaining boundary of the Reactor coolant systems 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 radiolysis 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;

3.83 Use of materials with sensitivity for activation under neutron irradiation should be minimized to the extent practical.

[4] Meeting the stress limit proposed by codes for emergency or faulted conditions is generally not considered as adequate by Regulatory Bodies.

3.84 Materials should be selected to be suitable for the service conditions expected in all operational states and accident conditions. 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.

Materials in contact with radioactive fluids

3.85 Materials should be highly resistant to all the corrosion phenomena in operating conditions including any deterioration from chemical attack by the fluid and abrasive effects of suspended solids under operating conditions.

3.86 Materials used should be easy to be decontaminated.

Material exposed to high neutron flux

3.87 The materials used in this application should take into consideration:

- Embrittlement due to neutron irradiation (including Irradiation-Assisted Stress Corrosion Cracking (IASCC)),
- Swelling due to neutron irradiation,
- Neutron activation,
- Irradiation creep.

CALIBRATION, TESTING, MAINTENANCE, REPAIR, REPLACEMENT, INSPECTION AND MONITORING

The following recommendations provide guidance to fulfil the overarching requirement 29 of [2].

3.88 The design should incorporate provisions recognizing the need for those in service activities, as well as to permit the repair, replacement and modification of those SSCs likely to require such actions, due to operational service conditions. In addition, activities which need to be carried out during the construction and commissioning phases should be identified.

3.89 SSCs important to safety should be designed and located to make surveillance and maintenance simple, to permit timely access, and in case of failure, to allow diagnosis and repair, and minimize risks to maintenance personnel.

3.90 The development of strategies and programs to address in-service inspection, testing, maintenance and monitoring is a necessary aspect of the RCSAS design phase. The strategies and programs to be implemented for these activities should be developed so as to ensure that RCSAS SSCs remain capable and available to perform their safety functions.

3.91 The design should establish a technical basis of SSCs that require in-service inspection, testing, maintenance and monitoring.

3.92 If the plant design contains safety equipment that cannot be tested in situ (e.g. explosively actuated valves) an appropriate surveillance program should be implemented that includes preservice and in service provisions.

Specific recommendations for in-service inspection of the Reactor Coolant System

Pre-service inspection and testing

3.93 Prior to commissioning, the RPV and RCS should be subject to tests to ensure that the vessel and components have been correctly manufactured and installed. These include the following:

- Manufacturer hydrostatic pressure test of the RPV prior to installation;
- Non-destructive examination of the RPV and RCS welds utilizing volumetric (through wall) and surface examinations in what is commonly referred to as pre-service inspection (PSI). These examinations are important to establish the baseline condition to be used as comparison to the in-service examination results;
- Code hydrostatic test of the RPV and RCS once installation is complete;
- Establishment of a surveillance sample program utilizing material samples that are installed in the RPV and removed on a scheduled basis. These samples when removed are subject to testing, including tensile strength and Charpy impact test. Other samples are analysed to measure the irradiation flux that the RPV wall is being exposed to.
- During the performance of the PSI program, design features to facilitate and simplify the implementation of the in service inspection (ISI) program during operation should be identified. This should include consideration that many areas will not be easily accessible once operation commences.

In service inspection (ISI) and testing

3.94 The welds of the RPV and RCS should permit volumetric (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.

3.95 Non-inspectable welds of the RPV and RCS should be limited to the extent possible and analyses of the consequences of the failure should be performed.

3.96 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 accident conditions;
- Sourcing of RPV welded and base metal coupons to be made into ultrasonic testing calibration blocks;
- The maximum acceptable defect in operational states;
- Commissioning (Code) Hydrostatic Pressure test;
- Periodic Leak Rate and Hydrostatic tests;
- Code mandated periodic in service inspection program;
- Controls of the manufacturing at the shop: Reference and traceability for the operational lifetime;
- Implementation of the surveillance sample program.

Specific recommendations for in-service inspection of the steam generators:

The design of the steam generators 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.

OVERPRESSURE PROTECTION

3.97 All pressure retaining components of the RCSASs should be protected against overpressure conditions generated by component failures or by abnormal operations in order to fulfil the pressure limits, in compliance with applicable proven codes and standards.

3.98 A same code should be used for the design, manufacturing and overpressure analysis of a given component.

LAYOUT

3.99 The design layout of the RCSASs should take into account:

- Radiological protection of site personnel;
- Protection against the consequences of pipe failure; (pipe whip, flooding, high pressure jet);
- Protection against internal missiles;
- Provisions for venting and draining the reactor coolant;
- Provisions to avoid water stratification and accumulation of gases;
- Provisions to avoid erosion;
- Provisions to avoid water hammer;
- Provisions to minimize stresses in the piping and to facilitate thermal expansion;
- Provisions to facilitate testing and inspection.

RADIATION PROTECTION

The following recommendations provide guidance to fulfil the overarching requirement 81 of [2].

3.100 The design of the layout of RCSASs should allow for the inspection, maintenance, repair and replacement of components, with account taken of the need for the radiological protection of site personnel.

3.101 Appropriate design provisions (shielding, remote control valves, etc.) should be implemented to enable local actions required for DBA management without undue radiation exposure of the field operator.

3.102 Similar design provisions should be implemented to enable the recovery of systems necessary to maintain safe conditions in the long term.

3.103 Cobalt content of all materials in contact with the reactor coolant should be minimized to avoid activation in the core radiation field of entrained corrosion products leading to production of cobalt 60.

3.104 If advanced materials are used in the design of RCSASs, samples of these materials should be subjected to a high neutron flux and exposed to the environment of the reactor core. 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.

3.105 More recommendations for design measures for radiological protection are given in Ref. [14].

COMBUSTIBLE GAS ACCUMULATION IN NORMAL OPERATION

3.106 Design and layout provisions should be taken to prevent accumulation of combustible gases at the upper parts of components and piping (e.g. upper part of the reactor pressure vessel, pressurizer, safety valves).

VENTING AND DRAINING

3.107 Provision should be made for venting and draining RCSASs.

3.108 Provisions should also be provided for collecting leakages during normal operation. Leaks can occur from, among others, valve stems, valve seats, pump seals and inter gasket cavities during reactor operation.

INTERFACE

3.109 Appropriate interface devices should be provided for connections between systems or components belonging to different safety classes [10]. These interface devices should prevent that the failure of a system or component could cause the loss of the safety function of the system or component with the higher safety classification and should limit 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.

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

3.111 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.

CONTAINMENT ISOLATION

The following recommendations are provided to fulfil the requirement 56 of [2].

3.112 Piping that penetrates the primary containment boundary should be provided with adequate isolation devices [15].

3.113 For system piping crossing the containment wall(s) containment extensions should satisfy the design recommendations [15].

INSTRUMENTATION

3.114 RCSASs should be provided with adequate instrumentation with the purposes of:

- Monitoring the process parameters (e.g. pressure, temperature, water level, flow rate) indicating that the system or component is operated within the range specified for its normal operation;
- Early detection of abnormal operating conditions;
- Automatic operation of systems necessary for the mitigation of accident conditions;
- Providing the operator in the MCR with appropriate and reliable information for the post-accident management.
- Periodic testing of systems and components.

3.115 Consequences of sharing of sensors for different purposes should be considered in order to preserve adequate independence between the different levels of defence in depth. Following recommendations should be implemented to the extent possible:

- Not sharing sensors for the automatic actuation of the operation of the systems and the accident monitoring of the plant;
- Not sharing the same sensors for the automatic actuation of the reactor shut-down or of the operation of the safety systems, and for the actuation of the safety features implemented to reinforce the prevention of accidents with core melting.

3.116 Instrument lines[5] should be so designed that the detected parameters (e.g. magnitude, frequency, response time, chemical characteristics) are not distorted.

3.117 Means for monitoring the activity in all fluids that could become radioactive should be provided in accordance with [16].

MULTI UNITS AT THE SITE

3.118 According to the overarching requirement 33 of [2] each unit is required to have its own safety systems and its own safety features for design extension conditions.

CODES AND STANDARDS

The following recommendations provide guidance to fulfil the requirement 4.15 of the overarching requirement 9 of [2].

3.119 For the design of RCSASs proven and widely accepted codes and standards should be used. The selected codes and standards:

- Should be applicable to the particular concept of the design;
- Should form an integrated and comprehensive set of standards and criteria;
- For design and construction the newest edition of the codes/standards should be preferably considered.

3.120 Codes and standards have been developed by various national and inter- national organizations, covering areas such as:

- Materials;
- Manufacturing (e.g. welding);
- Civil structures;
- Pressure vessels and pipes;
- Instrumentation and control;

[5] 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.

- Environmental and seismic qualification;
- Pre-service and in-service inspection and testing;
- Quality assurance;
- Fire protection.

USE OF PROBABILISTIC ANALYSES IN DESIGN

3.121 Probabilistic analyses should be combined with the deterministic approach for confirming the reliability of RCSASs in preventing significant fuel damage and for identifying the more likely CCF and multiple failures which could be considered as initiators of DECs.

3.122 The use of probabilistic analyses should be part of the process to select optimal design options and to judge their effectiveness.

4 ULTIMATE HEAT SINK AND RESIDUAL HEAT TRANSFER SYSTEMS

ULTIMATE HEAT SINK

Many plants use river water, sea water or lake water as ultimate heat sink but others rely upon the atmosphere for performing the UHS function to some extent in conjunction with the assured supply of cooling water, such as in the case of spray ponds and cooling towers. Some passive reactor plant designs also rely more exclusively on the atmosphere for dissipating reactor decay heat immediately following plant transient and accident conditions. Cooling towers include seismically and environmentally qualified structures with internal water storage to support DBA heat loads. This includes screens/strainers, spray nozzles, de-icing features, mechanical fans, with includes an ensure air flow path. If the cooling tower internal water storage does not support long term water inventory, a make-up water should be provided. Also a UHS blow-down system should be provided to ensure water chemistry is maintained within specifications.

4.1 Where 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, river or natural or human made reservoir);
- Make-up sources to the ultimate heat sink;
- The capability of the heat sink to deliver the necessary flow of cooling water at appropriate temperatures specified for the different plant states.

4.2 In the selection of the type of ultimate heat sink, account should be taken of the specific site conditions in which the plant will operate and of its impact on the environment.

4.3 In determining the necessary capacity of the ultimate heat sink, 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 transfer 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.

4.4 The environmental parameters considered in the design of the ultimate heat sink should be appropriate to the site specific conditions. Recommendations and guidance on the consideration of external events in the design of the ultimate heat sink (seismicity, extreme temperatures and conditions, floods, tsunamis, high winds, biological phenomena, collision with floating bodies, etc.) are provided in Ref. [5].

4.5 Site conditions should be appropriate and, if necessary, supplemented by the installation of additional provisions to ensure with a high reliability the long term capacity[6] and availability of the ultimate heat sink for removing residual heat from all the units installed at the site.

4.6 Design provisions for capacity and availability should be defined taking into account short and long term site conditions caused by extreme meteorological conditions and the effects of every site external hazard.

4.7 Provisions ensuring effectiveness and availability of the ultimate heat sink with regard to the site natural hazards should be designed with adequate margins to cope with levels of natural hazards exceeding those derived from the hazard evaluation for the site.

4.8 The effectiveness of the ultimate heat sink should not be much sensitive to short term variations.

4.9 Depending on the site conditions and hazards, the need for a diverse ultimate heat sink should be assessed and considered as necessary.

4.10 The plant states for which the UHS is required and the heat loads for each plant state should be specified.

4.11 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[7]. 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, availability of interconnections and the complexity of the procedures for replenishment.

4.12 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 build-up of sand and silt on the effectiveness and performance of the proposed design.

4.13 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.

4.14 In determining the capacities demanded of the ultimate heat sink and its directly associated heat transfer 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:

---

[6] An autonomy of 7 days at the site should be considered as a minimum.

[7] 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.

- The residual heat of the reactor coolant system;
- The decay heat of the spent fuel with the storage system at its maximum capacity;
- The heat rejected from pumps and other components (if heat produced by components is transported by the residual heat transfer chain);
- Other related heat sources (e.g. chemical reactions).

4.15 In establishing the residual heat loads of the reactor (including decay heat, heat due to shut-down 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.

4.16 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-shut-down times applied to the various fuel elements, or a conservative average post-shut-down time for all fuel elements should be used.

4.17 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 accident conditions.

4.18 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 transfer 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.

4.19 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.

RESIDUAL HEAT TRANFER CHAIN

Residual heat transfer chain includes the intermediate cooling systems and the cooling system directly associated to the ultimate heat sink. The intermediate cooling system is designed as a closed loop system which transfers heat loads from heat residual systems to the cooling system directly associated to the ultimate heat sink. The cooling system directly associated to the ultimate heat sink is an open loop system that takes water from the ultimate heat sink (pumping station) and provides cooling to the intermediate cooling system, and discharges transferred heat loads to the ultimate heat sink.

The following recommendations provide guidance to fulfil the overarching Requirements 7 and 53 of [2].

4.20 All residual heat sources at the nuclear power plant should be considered for the design of the heat transfer systems[8].

4.21 According to the defence in depth strategy, the design should provide multiple means to transfer residual heat to the ultimate heat sink.

4.22 Where heat removal system is not designed to operate RCS in hot conditions, residual heat removed by the secondary side can be directly released to the atmosphere which constitute a second ultimate heat sink (PWR and PHWR in AOOs and accident conditions). For diversity purpose, the operation of components necessary to feed and bleed steam generators should not be dependent from the heat transfer chain.

4.23 To ensure effectiveness of the defence of depth strategy the different means should be independent to the extent practicable, in particular a different and independent heat transfer chain should be implemented for accidents with core melting [15].

4.24 Heat transfer chain(s) should be designed applying design recommendations commensurate to its safety significance.

4.25 Where an ultimate heat sink of limited capacity is provided, the choice of the heat transfer 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.

Residual heat transfer in operational states

The following recommendations provide guidance to ensure that Requirement 51 of [2] and supplement the generic recommendations indicated in section 3.

4.26 Systems should be designed to transfer all heat loads generated for controlling primary coolant temperature in shut-down modes and the spent fuel pool temperature within their ranges specified for operational states.

4.27 Heat transfer should be possible despite a single failure postulated at any component necessary for transferring residual heat to the ultimate heat sink.

4.28 Residual heat transfer should be possible in the event of the loss of the off-site power sources.

4.29 The heat transfer chain should include an intermediate cooling system to prevent leak of primary coolant to be released into the ultimate heat sink.

---

[8] If heat produced by the operation of some components is also removed and transported by those systems, the corresponding additional heat loads should be included

4.30 Heat load transfer capabilities should be designed to be consistent with the requested performances of the reactor residual heat removal system and spent fuel cooling system.

4.31 Heat transfer capacity with the spent fuel pool should be designed at its maximum storage capacity taking into account boundary conditions for the heat loads. .

4.32 Heat transfer capacity should be designed to transfer heat loads generated during operational sates for a temperature of the ultimate heat sink within the range defined for normal operation.

4.33 Residual heat transfer systems should be designed in compliance with all the recommendations given in section 3 if they are also operated to transfer residual heat after a design basis accident (see paragraph Residual heat transfer in accident conditions).

Specific Design aspects

4.34 An activity monitoring system should be designed to detect activity in the intermediate cooling system.

4.35 The intermediate cooling system should be protected against over pressure caused by leaks occurring on heat exchangers with interfaces with coolant systems operated at higher pressure. In this case, the intermediate cooling system should be designed to prevent primary coolant leaks outside of the containment.

4.36 Pumps of the cooling system directly connected to the ultimate heat sink should be protected against debris and biofouling effects:

- A monitoring of the heat exchangers fouling and a cleaning program should be implemented with appropriate frequency in order to limit the degradation of the system heat removal capability;
- A program of surveillance and control techniques should be implemented to reduce significantly the incidence of flow blockage problems from biofouling.

4.37 Capabilities of the cooling system directly associated with the ultimate heat sink should be designed considering:

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

Residual heat transfer in case of design basis accidents

4.38 The design of the plant should include additional systems to transfer residual heat to the ultimate heat sink in the event of design basis accidents when systems operated in normal shut-down conditions are not designed in compliance with engineering design requirements applicable to safety systems.

4.39 Heat transfer capacity should be designed to transfer heat loads generated during DBA conditions for a temperature of the ultimate heat sink defined for accident conditions.

4.40 The heat transfer chain should be designed according to the recommendations provided in section 3 for safety systems.

4.41 The heat transfer chain should have capabilities designed to accomplish the following functions in the event of DBAs;

- Transfer residual heat from RCS to the ultimate heat sink;
- Transfer heat from the fuel pool cooling system to the ultimate heat sink;
- Transfer heat from the containment to the ultimate heat sink;
- Transfer heat from water cooled components required in accident conditions.

Specific Design aspects

4.42 Design and manufacturing of individual components should be conducted in compliance with the requirements established by national and international codes and standards widely used by the nuclear industry. For each individual component, the requirements to be applied should be selected with due account taken of the two effects resulting from its failure (function not accomplished and radioactive release)[9].

4.43 A failure on a lower classified part would not cause the failure of a higher classified part and the isolation devices should have a safety class similar to the highest one.

Residual heat transfer in case of design extension conditions

4.44 Conditions requiring additional needs (safety features for DECs) are reactor technology/ design dependent, and they should be postulated applying a deterministic approach in combination with PSA level 1. In particular (see recommendation 3.36):

- Residual heat transfer to the ultimate heat sink should be possible in the event of station blackout (SBO).

[9] However, according to international practices, the pressure retaining boundary of components necessary for the accomplishment of the residual heat removal after DBA conditions should be designed and manufactured in compliance with. ASME Section III, Division 1, subsection NC, RCC-M2 code, JSME SNC2, or similar standards).

Examples: Cooling chain supplied by the Alternate AC power source / Passive Secondary Residual Heat Removal system.

- Needs to transfer residual heat to the ultimate heat sink in the event of a loss of the cooling chain designed for DBAs should be evaluated.

Examples: Passive Secondary Residual Heat Removal system/ Credit of the heat transfer chain for DEC with significant fuel damage.

4.45 Additional safety features for DECs should be implemented according to recommendations provided in section 3.

5 SPECIFIC CONSIDERATIONS IN DESIGN OF PWRS

REACTOR COOLANT SYSTEM

The RCS forms a pressure retaining boundary for the reactor coolant and is therefore a barrier to radioactive releases to be preserved to the extent possible in all modes of plant normal operation and accident conditions. The RCS transports the coolant and thereby heat from the reactor core to the steam generators (for PWR and PHWR) or directly to the turbine (BWR). The RCS also forms part of the route for the transfer of heat from the reactor core to the ultimate heat sink during shut-down and in all transient conditions that are considered in the design of the RCS.

Structural design of the reactor coolant system

The following recommendations are provided to fulfil Requirement 47 of [2].

5.1 Specifications for the design and manufacturing of the large components of RCS (reactor pressure vessel, pressurizer, steam generators) should be appropriate to make the probability of their failure very low so that their failure may not be retained as a PIE for the plant design, (consequences of such failure cannot be reasonably mitigated). Such high quality level should be achieved in accordance with the latest edition of established codes and safety standards taking into consideration of available experience. Specifications should request for:

- An analysis of the relevant potential damage modes and choice of material adapted to them and having proven structural characteristics;
- A comprehensive identification of loads and load combinations in any plant state (including hazards) and appropriate margins regarding the failure criteria;
- An in service inspection programme that aims at periodically verifying the absence of cracks or defects of significance to safety on equipment.

5.2 The assurance that the quality will be achieved should make necessary a qualification of the manufacturing process implemented at the factory.

5.3 The following types of failure modes should be considered in the design according to the relevant code requirements and limits:

- Excessive deformation;
- Elastic or elastoplastic instability (buckling);
- Progressive deformation and ratcheting;
- Progressive cracking initiation (fatigue);
- Fast fracture including brittle fracture, in case of existing defects in the structure.

5.4 To preserve the integrity of the RCS, any condition that would affect the geometry or structural characteristics of equipment, or cause the apparition of defects should be identified and prevented by design, manufacturing or operating and in service inspection provisions (in particular chemical corrosion, stratification, etc.).

5.5 Equipment of the RCS should be designed so that the stresses imposed upon it remain below the values defined for structural materials to prevent a fast growth crack during normal operational conditions, anticipated operational occurrences and accidents without significant core degradation.

5.6 At low operating temperature the ductility and pressure resistance of some materials may be significantly lower. Where such materials are used for the manufacturing, the allowable loadings at low operating temperatures should be defined, the permitted operational ranges for pressure and temperature should be determined and a protection system should be implemented to prevent the risk of brittle fracture of the component.

5.7 The cyclic plant conditions that may cause the apparition of cracks due to fatigue should be identified at the design stage in order to be monitored during the plant operation, and a number of occurrences should be assigned to each of them in respect of the usage factor.

5.8 Adequate system(s) with appropriate accuracy, reliability and response time should be installed to detect a coolant leak and make its quantification possible in operational conditions.

5.9 Structural design of the Reactor Coolant Pressure Boundary/Secondary Side Pressure Boundary should be established on the basis of a limited number of loads and load combinations (Design basis loading conditions) defined as envelopes of loads to which the equipment could be subjected over its lifetime taking into account the normal plant operation, postulated plant events, natural phenomena and site related hazards considered in the design basis of the equipment.

5.10 Stresses caused by normal service and upset conditions should be less than the stress limits specified for those loading conditions categories. Moreover, the design pressure and temperature should not be exceeded, and the cumulative usage factor should be less than 1.

5.11 For loading conditions assigned in emergency conditions category, the design criteria should aim at preventing the fast fracture of the equipment subjected to the primary loads, and at avoiding excessive deformation or buckling. Stresses should be less than the stress limits specified for that loading conditions category. Pressure reached during an emergency condition may exceed the design pressure, provided the overshoot is limited and of a short duration (e.g. does not exceed 110% of the design pressure).

5.12 For these loading conditions assigned in faulted conditions category, the design criteria should aim at preserving the integrity of the equipment. Stresses should be less than the stress limits specified for that loading conditions category. Pressure reached during a faulted condition may exceed the design pressure, provided the overshoot is limited and of a short duration (e.g. does not exceed 130% of the design pressure).

Control of cooling conditions in operational states

The following recommendations are provided to fulfil Requirement 49 of [2].

5.13 Design provisions should be implemented for monitoring, display and control of the key RCS parameters (coolant pressure, coolant temperature, coolant inventory, SG pressure and water levels, etc.) to maintain those parameters within their range specified for during normal operation and anticipated operational occurrences and to detect early deviation. Maintaining those parameters within their range for normal operation contributes to assuring adequate cooling conditions of the fuel.

5.14 Provisions to maintain adequate cooling conditions of the fuel should be classified items related to safety and be designed and manufactured accordingly (see section 3, safety classification).

Pressure control and overpressure protection

The following provisions and design recommendations should be considered for the design of the pressure control of the Primary and Secondary Side circuit.

5.15 The concept of defence-in-depth should be applied in the design of the pressure control of RCS and Secondary Side. According to this concept, systems and components with different capacities should be used for pressure control to ensure that counter measures are proportional to the severity of an anticipated operational occurrence or accident.

5.16 The diversity principle should be applied in the design of the pressure control systems to reduce the likelihood of common cause failures.

5.17 Provisions should be made for normal operation and anticipated operational occurrences by means of systems intended for pressure control to ensure that it will not be necessary to use safety valves to limit the pressure increase.

5.18 Setting and system performances of control systems for operational conditions should be determined on the basis of realistic assumptions.

5.19 The pressure control system of the RCS should be designed to maintain the pressure within the limits ensuring the cooling of the fuel in operational states as long as two-phase conditions are maintained in the pressurizer.

5.20 Pressure control in RCS and Secondary Side circuit should be ensured even in the event of a loss of off-site power.

5.21 CVCS should have capabilities for RCS depressurization and RCS pressure control when pressurizer spraying is not available.

The following recommendations are provided to fulfil Requirement 48 of [2], but also apply to the over pressure protection system of the Secondary Side circuit.

5.22 The Reactor Coolant Pressure Boundary and the Secondary Side Pressure Boundary should be provided with an overpressure protection system relying on redundant safety valves. The setting should be designed on the basis of a sequential opening of the safety valves to ensure that no more valves than required are opened to relieve overpressure.

5.23 The discharge capacity should be designed to meet the pressure limits prescribed by the industry codes and applying design rules specified by the code. Typically:

- Analyses do not credit non-safety classified systems unless their operation can aggravate the consequences of the initiating event;
- Safety classified systems are assumed to operate at their less favourable performances regarding the criterion to be met;
- Discharge capacity of the safety valves is determined on the basis of the applicable standard;
- The total discharge capacity credited in the analysis is calculated taking into account the sequential opening of the safety valves and that one safety valve at least fails to open (or more for systems with more safety valves);
- Loss of the off-site power is combined if it can aggravate the consequences of the initiating event.

5.24 RCPB/SSPB over pressure protection system should be designed to keep pressure below the design limits specified for the different categories of postulated initiating events in conjunction with the reactor scram.

5.25 RCPB integrity should be assured for load combinations of high pressure and low temperature when the reactor coolant system is operated at low temperature (protection of RCS equipment with materials of less ductility at low temperature).

5.26 Equipment ensuring the RCPB/SSPB integrity should be supplied by the uninterruptible power sources.

5.27 No shut-off valves should be placed in the discharge line of a safety valve, nor between the item being protected and a safety valve.

5.28 When a relief valve is used for pressure control, its reliable closing should be secured by means of a relief line shut-off valve.

5.29 Where the over pressure protection is ensured by pilot operated safety valves:

- No shut-off valve should be installed in the control line required for opening a safety valve. If an exception is made to facilitate testing or maintenance or to prevent a safety valve from being stuck open, the inadvertent closing of the shut-off valve should be reliably prevented.

- The safety valve should be provided with a position indicator that is independent of the control equipment.

5.30 Due consideration in the design of the safety valves, their pilot valves and connecting piping should be given for the potential accumulation of non-condensable gases and condensate as well as the adverse effects they may have.

5.31 When necessary, the set of safety valve used for overpressure protection and the associated piping should be designed to discharge steam as well as a steam-water mixture and water.

5.32 Spurious opening of a safety valve should be prevented and its frequency should not be higher than the frequency considered for loss of coolant accidents.

5.33 Components that can increase pressure in the primary circuit (e.g. pressurizer heaters or pumps) should be equipped with a system that stops the operation of the component to prevent inadvertent pressure increase and is capable of performing the protection function also in the event of a single failure.

The following recommendations are provided to fulfil Requirement 20 of [2].

5.34 The RCS over pressure protection system should also be designed to preserve the integrity of the RCPB in case of postulated sequences involving multiple failures. Typically, the design of the over pressure protection system should be adequate to limit the pressure in the event of ATWS.

5.35 A fast RCS depressurization system should be implemented to prevent direct containment heating loads caused by the RPV failure at high pressure. That function should be accomplished by the operation of dedicated discharge valve(s) designed with a large discharge capacity. This fast depressurization system should be designed with an appropriate reliability to contribute to the practical elimination of such conditions.

5.36 Spurious opening of that system should be prevented and its frequency should not be higher than the frequency considered for loss of coolant accidents.

5.37 Equipment ensuring RCS depressurization should be supplied by the uninterruptible power sources.

Isolation of the Reactor Coolant Pressure Boundary

RCPB comprises pressure retaining components of the RCS that cannot be isolated from the reactor by two isolation valves in series or by a safety valve and whose failure would result in a leakage non-compensable by the normal water make-up system.

The following recommendations are provided to fulfil the requirement 6.13 of [2].

5.38 Isolation devices between RCPB and connected systems less safety classified should be designed to close quickly and reliably in order to limit the loss of primary coolant in the event of a piping failure affecting a connected system. The loss of primary coolant caused by the failure of a connected piping should not necessitate the operation of safety systems.

5.39 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). In particular, to keep the full efficiency of the safety injection, all the systems connected to the RCS should be automatically isolated in a timely manner unless necessary to meet the requirements applicable to a LOCA accident.

5.40 RCPB isolation should be designed according to the single failure criterion.

5.41 RCPB isolation should be ensured even in the event of a loss of off-site power.

5.42 Adequate isolation should be provided at the interfaces between the RCS and connected systems operating at lower pressures to prevent the over pressurization of such systems and possible loss of coolant accidents.

5.43 Isolation devices should be considered as RCS components and hence should be designed and manufactured in compliance with the requirements and recommendations that apply to RCS components.

Postulated Initiating events

5.44 Failures of any component or system and operator errors whose consequences would modify RCS conditions or loads defined for normal operation should be identified and primarily categorized in a plant state category on the basis of its frequency to occur (see paragraph 3.4).

- Malfunctioning of RCS control systems;
- Piping break;

- Spurious opening of a relief/safety valve;
- Loss of forced coolant circulation;
- Reactor Coolant Pump failure;
- Positive core reactivity insertion.

Internal Hazards

5.45 The layout of RCS piping supplemented by local protection devices (anti whipping devices, shields, etc.) should be such that domino effects are prevented in the event of a high energy pipe break:

- A single initiating break of a reactor coolant leg should neither propagate to neighbouring loops or to main steam /feed water piping;
- A single initiating break of a main steam/feed water piping should neither propagate to neighbouring main steam/feed water piping or to reactor coolant loops;
- A single initiating break of pressurizer piping should neither propagate to neighbouring pressurizer piping.

5.46 Fail safe instrumentation and layout provisions to protect the instrumentation should be implemented to ensure the actuation of necessary automatic actions and the accident management.

External Hazards

5.47 The integrity of the Reactor Coolant Pressure Boundary should be maintained in the event of earthquake (SL2).

5.48 RCS components which are not part of the Reactor Coolant Pressure Boundary and that are not seismically classified should be reliably isolated from the Reactor Coolant Pressure Boundary by isolation devices seismically classified and qualified to operate under SL 2 seismic loads.

5.49 RCS components necessary to operate the reactor to safe shut-down conditions should be seismically classified in order to keep their integrity and qualified to operate under SL 2 seismic loads.

5.50 RCS components necessary to operate the reactor to safe shut-down conditions should be designed to keep their integrity and to operate in the event of external hazards causing high energy impact on the containment structure.

Layout

5.51 The arrangement of piping and the location of equipment should enable removal of residual heat from the reactor core by natural circulation.

5.52 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.

Design limits

5.53 Design limits not to be exceeded in a plant state should be defined for RCS components, as for examples:

- Pressure and temperature (limits in AOOs, DBAs, DEC and ATWS);
- Max cooling rate, max heating rate for normal operation;
- DT max between hot leg and pressurizer;
- Delta P max Primary/Secondary;
- Max RCS leak rate;
- Max RCS/SG leak rate;
- Limits regarding the brittle fracture of RPV;
- Component parameters (e.g. Delta P for reactor coolant pump seals, T seals).

More detailed recommendations are given in [17].

Safety classification

5.54 Pressure boundary component which are part of the reactor coolant pressure boundary should be classified so that it is designed and manufactured in compliance with the highest standards defined by the industry for nuclear application (e.g. ASME Section III, Division 1, subsection NB, RCC-M1 code or similar standards).

5.55 Other pressure boundary component and non-pressure boundary component should be classified with due account taken of the two effects resulting from its failure (function not accomplished and radioactive release) according to detailed guidance given by SSG-30 [10].

Environmental qualification

5.56 The following RCS components should be designed or qualified for the worst harsh environmental conditions that could prevail inside the containment prior to or during accident conditions without significant core degradation until their mission time is completed:

- Reactor Coolant Pressure Boundary components (for integrity);
- Reactor Coolant Pressure Boundary isolation devices (for operability);
- Over pressure protection components (for operability);
- RCS components designed to protect the RPV against brittle fracture(for operability);
- RCS components necessary to operate the reactor to safe shut-down conditions (for operability);
- Components designed to depressurize the RCS in order to prevent Direct Containment Heating loads caused by the RPV failure at high pressure (for operability).

Pressure tests

5.57 Hydrostatic pressure test of the RCS should be performed at commissioning stage and repeated periodically, with possibly different criteria. The aim of these tests may be:

- To prove the absence of permanent deformation when the structure is brought to a pressure close to the elastic limit;
- To prove the absence of leak that would not have been detected earlier.

The pressure test operating mode and pressure level are usually defined in national regulations and are reflected in industry codes and standards.

5.58 RCS equipment should not undergo any damage during pressure test.

Venting

5.59 In order to prevent disruption of the natural circulation of the reactor coolant, remotely operated valves should be provided to vent non-condensable gases in accident conditions.

5.60 RCS venting should be possible in the event of a loss of the off-site power.

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

Specific design aspects

Reactor pressure vessel

5.62 The design considerations for the pressure vessel should include the following:

- 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;

- 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;

- 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;

- The design of the pressure vessel should be such that it can withstand pressurized thermal shocks without incurring a failure of integrity.

5.63 If advanced materials were to be used in the reactor pressure vessel, 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.

5.64 For design with in vessel retention strategy, evidence of robustness of the reactor pressure vessel to sustained loads caused by such severe conditions should be demonstrated with a high degree of confidence.

Reactor pressure vessel internals

5.65 Pressure vessel internals should be designed to:

- Prevent unacceptable flow induced vibration;

- Accommodate asymmetric blow-down loads caused by pipe ruptures;

- Ensure that fuel design limits are not exceeded in normal operation or anticipated operational occurrences.

5.66 Pressure vessel internals should be designed to withstand loads to ensure the insertion of the control rods in the core and the coolability of the fuel elements in any plant state without significant core degradation.

Reactor Coolant Pumps

5.67 The RCS and reactor coolant pumps should be such as to provide an adequate flow of coolant with suitable hydraulic parameters to ensure that neither the fuel applicable design limits nor the RCS equipment and RPV internal applicable structural limits are exceeded in operational states and accident conditions.

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

5.69 The design of RCS 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.

5.70 Correct operation of pads and bearings should be monitored and automatic stop of RCS pumps should be implemented in order to prevent operation under vibrations that could result in the shaft failure.

5.71 RCP seal leakage should be controlled by maintaining adequate cooling of seal system in any plant state (normal operation and accident conditions) including plant conditions with loss of electrical power sources. In normal operation, seal leakage should be compensated and, in plant states where compensation is not available, seal leakage should be preferably isolated. RCP should be automatically tripped in any case where seal operational parameters cannot be maintained, in order to prevent any further damage on seal system.

Steam generators

5.72 Steam generators tubes belong to the Reactor Coolant Pressure Boundary and hence should be designed with the same recommendations.

5.1 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. should be designed to withstand loads from a main steam line break).

5.73 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.

5.74 The design should also provide provisions for taking samples of secondary side water.

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

5.76 Overfilling of the steam generator should be prevented by design provisions.

5.77 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.

5.78 The design should include blow-down provisions to control the amount of solids (sludge) that could accumulate in areas of stagnant flow.

5.79 The design should include provisions for sampling of fluids from relevant location of the secondary side.

Piping system

5.80 All the primary loop piping should be of stainless steel or protected with stainless steel cladding.

5.81 Capability should be provided for venting and draining of the piping system.

5.82 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.

Leak before break or break preclusion piping

5.83 Whether a leak before break or break preclusion concept is claimed for the design and manufacturing of piping, the specific and additional design/manufacturing requirements should be met, based on similar considerations as for non-breakable equipment.

5.84 In addition, and in spite of the very low probability of the piping failure, the consequences of the double ended break of a pipe should be analysed with appropriate rules regarding:

- Structural behaviour of RCS equipment and associated internals;
- Core cooling;
- Pressure build up inside the Primary Containment.

Insulation materials

5.85 Insulation material used in reactor building should be selected in order to minimize sump clogging in case of high energy breaks.

5.86 For design relying on In Vessel Retention (IVR) strategy with an ex vessel cooling, the following design considerations apply to the reactor vessel insulation:

- A means of allowing water free access to the region between the reactor vessel and insulation should be provided and the design of the associated water inlets should minimize the pressure drop during ex-vessel cooling to permit water inflow to cool the vessel;

- A means to allow steam generated by water contact the reactor vessel to escape from the region surrounding the reactor vessel should be provided;

- The insulation support frame and the insulation panels should form a structurally reliable flow path for water and steam.

SYSTEMS FOR COOLANT INVENTORY AND CORE REACTIVITY CONTROL IN OPERATIONAL STATES

RCS water inventory control in normal operation is performed by the Chemical and Volume Control System (CVCS). The CVCS is also designed to control RCS pressure when RCS pumps are shut down by spraying RCS pressurizer, and to adjust the boric acid concentration of the primary coolant in power operation and shut-down modes. Typical functions of CVCS are:

- Control of the reactor coolant inventory;

- Control of the RCS pressure in shut-down modes;

- Control of the core reactivity;

- Supply seal water to the reactor coolant pumps;

- control of the chemistry of the reactor coolant;

- Clean-up and purification for the reactor coolant.

These functions are mainly dedicated to normal operation and are not usually performed during accidents. However, parts of the system may be used to reach a safe shut-down state following abnormal events or accidents.

Inventory control for the reactor coolant

5.87 The CVCS should be designed to accept the let-down for reactor coolant expansion during plant heat up and provide the makeup for reactor coolant shrinkage during plant cool-down at heat up and cool-down rates.

5.88 The CVCS should be designed to provide makeup water due to power decreases or accept let-down due to power increase.

5.89 For any mode of normal operation or event that does not require the operation of safety systems, CVCS should provide and maintain sufficient reactor coolant inventory to ensure core cooling such that fuel design limits are not exceeded, and provide sufficient flow to the reactor coolant pump seals for the pressure boundary integrity.

5.90 Low pressure systems connected to the RCS should be provided with overpressure protection devices. Other portions and components where design conditions can be exceeded during operations also should be provided with overpressure protection devices.

Core reactivity control

5.91 The CVCS should be designed to adjust RCS boric acid concentration in order to control core axial off set during power operation.

5.92 The CVCS should have capabilities to achieve RCS boric acid concentration required for refuelling operation.

5.93 The CVCS should have capabilities to achieve RCS boric acid concentration needed for power operation for fuel cycle conditions.

SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES

Heat removal in power operation and hot shut-down modes

The heat, including residual heat, generated in the core in power operation and hot shut-down modes is transferred from the RCS to the steam generators. The heat removal function is ensured by main feed water and main steam systems. The main feed water system is composed of main feed pumps, control valves and isolation valves. In some designs, there are pumps dedicated to low power and shut-down modes and they belong to a system designated as “Start up and shutdown feed water system”. The steam system includes main steam lines, isolation valves, safety valves and dump valves to the main condenser.

5.94 Main feed water and main steam systems are primarily designed to remove heat generated by the reactor at full power, but should also have capabilities to remove and transfer residual heat to an ultimate heat sink after the reactor is shut-down.

5.95 Residual heat removal capabilities should be designed to cool down RCS from hot shut-down conditions to primary pressure and temperature compatible with the operation of the Reactor Heat Removal System (RHRS).

5.96 The main feed water system should have capabilities to feed steam generators at rated temperatures and to control the steam generator levels within the range specified for operational conditions.

5.97 The failure of one feed water pump should not lead to a reactor trip.

5.98 Main feed water lines should be automatically closed after a reactor trip in order to prevent an excessive cooling of the core.

5.99 The over filling of steam generators should be reliably prevented.

5.100 It the event of an uncontrolled and excessive SG depressurization (e.g. in the event of a main steam pipe or main feed water pipe break), the affected steam generator should be reliably isolated from other steam generators.

5.101 It the event of a significant activity level detected in one SG, the affected steam generator should be reliably isolated.

5.102 Adequate activity monitoring should be available to allow detection of steam generator tube rupture. The accuracy of this monitoring should be adequate to meet limits specified for radiological consequences in DBAs.

5.103 Leak-tightness of SG isolation valves should be adequate to meet limits specified for radiological consequences in case of a SG tube rupture.

5.104 The main steam system should provide capability to automatically and manually bypass the turbine and discharge steam directly to the condenser. The capacity of the bypass should be adequate to accommodate a full load rejection.

5.105 Main steam system should be designed such that one main steam line break could not lead to the depressurization of more one steam generator despite a single failure in the SG isolation system.

5.106 Main steam and feed water piping should be routed, protected and restrained to prevent concurrent pipe breaks (main steam or feed water pipe breaks, primary pipe breaks).

Residual heat removal in RHR mode

In cold shut-down mode of normal operation, the residual heat is transferred from the RCS to the cooling chain by the residual heat removal system. RHR system can be connected after RCS has been cooled down by steam generators. A RHR system train is composed of a shut-down cooling pump and a heat exchanger with the intermediate cooling system; it takes suction from RCS and injects back into RCS after cooling in the heat exchanger.

The following recommendations provide guidance to fulfil Requirement 51 of [2] and supplement the generic recommendations indicated in section 3.

5.107 The design of the plant should include appropriate systems to remove residual heat from RCS in the different RCS shut-down conditions (e.g. RCS in hot shut-down conditions, in cold shut-down conditions and in refuelling conditions).

5.108 Heat removal capacity should be designed to cool down RCS from hot shut-down conditions (once the reactor is shut-down) to adequate conditions for refuelling operation.

5.109 RHR should be designed to control RCS temperature and achieve controlled cooling rate down to the cold shut-down conditions for refuelling within appropriate time after reactor shut-down.

5.110 Minimal heat removal capacity should be designed to remove residual heat despite a single failure postulated in any component necessary for removing residual heat.

5.111 Residual heat removal should be possible in the event of the loss of the off-site power sources.

5.112 RHR should be designed to keep its operability in the event of a SL2 earthquake.

5.113 Residual heat removal and transfer systems should be designed in compliance with all the recommendations given in section 3 if they are also operated to remove residual heat after a design basis accident (see paragraph “Residual heat removal after design basis accidents”).

Specific Design aspects

5.114 Maximal heat removal capacity should be designed taking into account operational criteria (e.g. time delay to reach refuelling conditions) without exceeding the limits specified in normal conditions for the fuel and the reactor coolant pressure boundary.

5.115 RHR connection temperature should be greater than the minimum RCS temperature that can be achieved by SG cooling.

5.116 During power and hot shut-down operation, the residual heat removal system is not operated and is isolated from the RCS and there should be interlocks or other provisions impeding the connection of the RHR system.

5.117 Adequate instrumentation and isolation capability should be provided to detect leaks or breaks in RHR system if part of the system is implemented outside the containment, in order to limit the amount of radiological releases outside of the containment.

5.118 Adequate instrumentation and isolation capability should be provided to detect leaks in heat exchanger in order to limit the transfer of primary water into the intermediate cooling system or, alternatively, the transfer of clear water to the RCS when it is fully depressurized.

SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS

This section addresses recommendations for the design of systems necessary to control core reactivity, to cool the core and to remove residual heat from RCS in all accident conditions but accident conditions with significant core degradation. Recommendations for the design of residual heat transfer chain and ultimate heat sink in accident conditions are addressed in section 3.

The following recommendations provide guidance to fulfil Requirements 7, 19, and 20 of [2] and supplement the recommendations indicated in section 3.

5.119 As stated in section 3 the needs for different, independent and diverse systems depend on the achieved reliability of the safety systems, and on potential vulnerabilities for common cause failures among their redundancies. However, the design of the plant should be such that multiple means exist for cooling the core, removing and transferring residual heat.

5.120 Systems designed for cooling the core in accident conditions (DBAs or DECs without significant fuel degradation) should be independent to the extent possible to those designed for operational conditions and from those dedicated to the core cooling in the event of core melt.

5.121 The design of systems necessary in DBA conditions or in DEC conditions should comply with all the general design recommendations provided in Section 3 applicable to systems designed to mitigate the consequences of DBAs or to DEC without significant fuel degradation respectively.

5.122 Reliability of specific safety features for DECs should be adequate to meet the objective specified for the total core damage frequency (CDF).

5.123 Safety systems should be designed to meet regulatory criteria specified for DBAs. Their performances should be such that those criteria are met applying the rules specified for the deterministic DBA analysis.

5.124 Performances of safety features for DECs should be adequate to prevent accident conditions without significant core degradation from escalating to conditions with core melting. For design, the same engineering criteria as those retained for DBAs can be used, but less conservative hypothesis and conditions are generally considered. However, in order to give confidence in the efficacy of the safety features for DECs and to avoid cliff edge effects, key parameters should be identified and provisions for covering uncertainties should be taken.

Core cooling in accident conditions

The RCS water inventory control in accident conditions is performed by the Emergency Core Cooling System (ECCS) in conjunction with the Emergency Feed Water System (EFWS) when necessary. This system also performs some functions related to the core reactivity control. The emergency core cooling system includes in general a combination of active and/or passive injection means (pumps, piping and valves). The system can also include heat exchangers to remove residual heat from the containment.[10]

The main function of the emergency core cooling system is to inject borated water into the Reactor Coolant System in order to ensure core cooling when RCS water inventory decreases or in the event of loss of the residual heat removal by the secondary side. The ECCSs are called upon to reach a controlled state in both Design Basis Accidents and Design Extension Conditions without significant fuel degradation such as:

- Loss of coolant accidents postulated as DBAs or DECs;
- Excessive and uncontrolled RCS cooling (piping breaks on the secondary side);
- Steam Generators tube rupture;
- Total loss of feed water – with a primary feed & bleed strategy.

The following recommendations provide guidance to fulfil Requirement 52 of [2] in the event of accidents (DBAs and DECs) with a loss of primary coolant, and to supplement recommendations indicated in section 3 relevant for safety systems or for safety features for DECs:

5.125 The emergency cooling system should be designed to cool the fuel within the criteria relevant for fuel, for fuel cladding and for the core geometry in the event of loss of coolant accidents (see items 5.144 and 5.145).

[10] In this Safety Guide, the sump filtration system is not considered to be part of the ECCS [15].

5.126 In the case of a small pipe break, energy removed at the break may not be sufficient for an effective cooling of the fuel, and therefore complementary system or equipment should be operated to achieve the appropriate cooling capacity (e.g. complementary decay heat removal by the steam generators or depressurization of the RCS to increase the water injection rate).

5.127 The emergency cooling system should be designed with adequate capabilities to prevent from or to limit uncovering of the fuel assemblies for the different sizes and locations of primary piping breaks. That usually requires different points of injection.

5.128 Possibilities that injection flow rates can by passed the core or can directly flow to the break should be considered for designing cooling performances of the system.

5.129 The emergency cooling system should be designed to restore and maintain an adequate coolant inventory in the RCS in order to recover the fuel cooling function.

5.130 The emergency core cooling system boron concentration should be sufficient to achieve core sub criticality in overcooling design basis accident (e.g. Steam line break).

5.131 The emergency core cooling system injection capacity should prevent boron crystallization in the core,

5.132 The emergency cooling system should include capabilities to remove core decay heat in the long term taking into account that RCS integrity cannot be maintained. Those capabilities are part of the safety system.

5.133 In the event of the total loss of the residual heat removal capacities by the secondary side, ECCS performances should be designed to prevent or limit core uncovering taking into the installed capacity for RCS bleeding.

Specific Design aspects

5.134 ECCS Pressure retaining equipment should be designed and manufactured according to requirements established by proven codes and standards widely used by the nuclear industry. For each individual component, the requirements to be applied should be selected with due account taken of the two effects resulting from its failure (function not accomplished and radioactive release)[11].

5.135 ECCS should be reliably isolated from RCS by two isolation devices in series. In order not to decrease the reliability of ECCS those isolation devices should be be designed to open quickly and without external service (e.g. check valves are widely used by Member States). Leak-tightness of the RCS isolation should be designed to be periodically tested. Moreover, ECCS should be protected against over pressurization caused by leakages.

[11] As examples, the pressure retaining boundary of ECCS components necessary for the accomplishment of the functions as expected should be designed and manufactured in compliance with ASME Section III, Division 1, subsection NC (or RCC-M2 code JSME SNC2 or similar standards),

5.136 ECCS equipment should be located outside the containment to the extent possible in order to limit the severity of the environmental conditions for which they should be qualified to and also to facilitate maintenance and repair.

5.137 Operation of ECCS should limit the risk of causing over pressurization of the RCS. In particular, cold shut-down states should be considered at which ECCS operation (spurious or not) could potentially cause damage to the reactor pressure vessel or the residual heat removal system (brittle fracture issue).

5.138 Provisions should be implemented for an early detection of leaks in the parts of the ECCS that are located outside the containment in order to isolate the system before it causes the drainage of the water reserves.

5.139 For accident management, actuation and shut-down of every ECCS train should be possible from the MCR. However, stopping the operation of ECCS should not be possible as long as a need for an emergency cooling of the core exists.

5.140 The emergency core cooling system pumps should be qualified to operate with active water loaded with particles, according to the filtration system capability.

5.141 The minimum net positive suction head (NPSH) for a normal operation of the ECCS pumps should be ensured at any time during DBAs with account taken of accumulation of debris at the surface of the sump filters.

5.142 Mini flow lines should be implemented to enable periodic tests and to prevent the failure of ECCS pumps at low injection flow rates.

Residual heat removal in hot shut-down modes for design basis accidents

The residual heat, generated in the core after reactor shut-down is transferred from the RCS to the steam generators. The heat removal function is ensured by the emergency feed water and steam dump to atmosphere systems. The emergency feed water system is composed of emergency feed water pumps, control valves and isolation valves. The steam dump to atmosphere system is composed of a control valve and an isolation valve located at the outlet of steam generators.

The following recommendations provide guidance to fulfil Requirement 51 of [2] in DBA conditions, and to supplement recommendations indicated in section 3 relevant for safety systems.

5.143 EFW and steam dump to atmosphere systems should have adequate performances to reliably accomplish residual heat removal and RCS cooling without exceeding limits for fuel, the reactor coolant pressure boundary and structures important to safety defined for DBAs.

5.144 EFW capacity and autonomy should be appropriate to reach RCS conditions compatible with RHR operation with adequate margins (24 hour autonomy is generally considered by Member States as a minimum). Interconnections between EFW tanks could be considered in order to extend the system capacity and autonomy provided that the manual operator actions are clearly described in the emergency operating procedures

5.145 The Emergency Feed water (EFW) System should be designed to supply secondary makeup water to the steam generators in DBA conditions where the main or auxiliary feed water system is unavailable.

5.146 Steam dump to atmosphere system should discharge steam from the steam generator in order to remove residual heat and cool down the RCS in plant condition where the condenser is not available or the main steam isolation valves are closed

Specific Design aspects

5.147 EFW Pressure retaining equipment should be designed and manufactured according to requirements established by proven codes and standards widely used by the nuclear industry. For each individual component, the requirements to be applied should be selected with due account taken of the consequences resulting from its failure (function not accomplished[12]).

5.148 Diversity of the EFW pumps could be considered in order to increase the reliability of the system.

5.149 The steam dump valves to atmosphere should be qualified to operate (open and close) for both steam, water and mixture of both as water could be carried by steam in case the level is high in the SG.

5.150 Isolation of EFW of, and steam dump valves from the affected SG should be performed in case of steam line break in order to limit the RCS overcooling.

5.151 Isolation of EFW of the affected SG should be performed in case of SGTR in order to prevent SG filling up and limit possible active water release to the environment.

5.152 Isolation of steam dump valves of the affected SG should be performed in case of SGTR in order to limit release to the environment.

Residual heat removal in the long term of design basis accidents

The function of this residual heat removal system is to transfer residual heat from the RCS to the intermediate cooling system and achieve safe shut-down state in accident conditions. This system can be connected after sufficient RCS cooling. This function is necessary for the safety demonstration after any DBA where RCS water inventory is adequate and controlled.

[12] However, according to international practices, the pressure retaining boundary of EFW components necessary for the accomplishment of the functions as expected should be designed and manufactured in compliance with. ASME Section III, Division 1, subsection NC or ND, RCC-M2 or M3 code, JSME SNC3, or similar standards).

Such a system train includes several redundant trains, each of them includes a pump and a heat exchanger with the intermediate cooling system; it takes suction from RCS and injects back water into RCS after be cooled by the heat exchanger. This system should be considered as the first element of the heat transfer chain to the ultimate heat sink in accident conditions.

The following recommendations provide guidance to fulfil Requirement 51 of [2] in DBAs.

5.153 This system should be designed according to the same recommendations given in section 3 for safety systems.

5.154 This system should be designed to remove core decay heat and to cool down RCS to safe shut-down conditions.

Specific Design aspects

5.155 Pressure retaining equipment should be designed and manufactured according to requirements established by proven codes and standards widely used by the nuclear industry. For each individual component, the requirements to be applied should be selected with due account taken of the two effects resulting from its failure (function not accomplished and radioactive release)[13].

5.156 Recommendations 5.107 to 5.113 should also be considered.

Residual heat removal in hot shut-down modes for design extension conditions without significant core degradation

The following recommendations provide guidance to fulfil Requirement 51 of [2] in DEC without significant core degradation.

5.157 Although needs for DECs are design dependent additional design provisions should be considered to cope with multiple failures resulting in the loss of the systems and the safety systems designed to remove residual heat during RCS conditions non compatible with the RHR operation. Typically consideration should be given to:

- Extend EFW autonomy with on-site refilling capabilities;
- Maintain EFW capabilities and operation of the steam dump valves to atmosphere in the event of a prolonged SBO;
- Implementation of a secondary side passive heat removal system;

[13] As examples, the pressure retaining boundary of components necessary for the accomplishment of the residual heat removal after DBA conditions should be designed and manufactured in compliance with. ASME Section III, Division 1, subsection NC],(or RCC-M2 code JSME SNC2 or similar standards),

- Remove decay heat from the core by operating a primary feed and bleed strategy;

- Implementation of a Passive Secondary Residual Heat Removal system.

5.158 To facilitate accident management of conditions beyond postulated accident conditions, EFW system should include connection lines to supply water into steam generators from external means, (eg. the fire engines or mobile diesel-pumps).

RCS fast depressurization in design extension conditions with core melting

The RCS fast depressurization system is composed of valves and relevant associated piping, directly connected to the pressure boundary of the RCS.

5.159 For the practical elimination of the phenomena associated with the high pressure melt ejection in case of severe accidents (Direct Containment Heating), the design include a fast depressurization of the primary circuit that should be used before the onset of a core melting accident.

Specific design aspects.

5.160 RCS fast depressurization valves should be different and diverse from the safety valves designed the RCS over pressure protection.

5.161 Spurious opening of the fast depressurization valves should be reliably prevented.

5.162 Pressure retaining equipment of the RCS fast depressurization which is part of the RCPB should be designed and manufactured according to requirements established by proven codes and standards for the design and manufacturing of the RCPB.

5.163 The RCS fast depressurization system being used in the early phase of a core melt sequence, temperature and pressure within the RCS are expected to be very high and the system should be designed to open considering such fluid harsh conditions.

5.164 The RCS fast depressurization system should be designed to withstand SL2 seismic loads.

SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS

The following recommendations provide guidance to fulfil Requirement 46 [2] in accident conditions without significant core degradation.

The following recommendations are for the design of the system relying on an adequate injection of water at high boric acid concentration. Recommendations for the shut-down system relying of the drop of solid absorbers are provided in [18].

5.165 That system, designed as a second and diverse mean to shut down the reactor should be designed according to the engineering recommendations for safety systems.

5.166 That system should be independent from the reactor trip system.

5.167 That system should be designed to fulfil items 6.10 and 6.11 of Requirement 46 of [2].

5.168 That system should have capabilities to shut down the reactor without exceeding the fuel limits specified for DECs without significant core degradation in the event of ATWS.

5.169 Acid boric concentration should be sufficient to compensate for the moderator effect at any time during the RCS cooling.

Specific Design aspects

5.170 Pressure retaining equipment should be designed and manufactured according to requirements established by proven codes and standards widely used by the nuclear industry. For each individual component, the requirements to be applied should be selected with due account taken of the consequences resulting from its failure (function not accomplished[14]).

5.171 Provisions should be considered in normal operation to prevent the boron crystallization due to high concentration in the tanks and pipes. Cold conditions derived from site hazard evaluation should be considered.

[14] As examples, the pressure retaining boundary components necessary for the accomplishment of the functions as expected should be designed and manufactured in compliance with. ASME Section III, Division 1, subsection NC or ND (or RCC-M2 or M3 code, JSME SNC2 or SNC3, or similar standards),

6 SPECIFIC CONSIDERATIONS IN DESIGN OF BWRS

REACTOR COOLANT SYSTEM

The Reactor Coolant System (RCS) of a BWR forms a pressure retaining boundary for the reactor coolant and is therefore a barrier to radioactive releases in all modes of plant normal operation and accident conditions. During normal operation the RCS transports the coolant in the form of steam and thereby heat from the reactor core to the main turbine-generator. During shut-down conditions, Anticipated Operational Occurrences (AOOs) and Design Basis Accidents (DBA) residual heat is transferred from the RCS to the Ultimate Heat Sink (UHS) utilizing various systems such as Reactor Core Isolation Cooling System (RCIC) or the Emergency Core Cooling System (ECCS) in conjunction with the Component Cooling Water System (CCWS) and the Essential Service Water System (ESWS).

The following recommendations are provided to fulfil Requirement 47 of [2].

Specifications for the design and manufacturing of the Reactor Pressure Vessel (RPV) of the RCS should be appropriate to make the probability of failure so unlikely that its failure need not be retained as a PIE for the plant design, as the consequences of such failure may not be reasonably limited (see paragraph section3). Such a high quality level should be achieved by complying with the latest edition of established codes and safety standards taking into consideration of available experience including operating experience. These specifications deal with:

- The design of the component: analysis of the relevant potential damage modes and choice of material adapted to them and having proven structural characteristics, comprehensive identification of loads in any plant state (including hazards) and associated design with appropriate margins regarding the failure criteria for all the failure modes;

- The manufacturing and control processes that should provide assurance of a very high quality product, based on proven industrial practices;

- The in service inspection that aims at proving that no damage occurs throughout the life time of the equipment.

6.1 Required reliability of the RCPB should be achieved by:

- Compliance with the regulatory requirements relevant for design and manufacturing;

- Complete identification of loads and load combinations for the different loading conditions categories with the associated stress limits.

- The assurance that the quality will be achieved should make necessary a qualification of the manufacturing process implemented at the factory.

6.2 To preserve the integrity of the RCS, any process that would affect the geometry or structural characteristics of equipment, or cause the apparition of defects should be identified and addressed during the design phase.

6.3 Cyclic plant conditions that may cause the apparition of cracks due to fatigue should be identified for each RCS component. These RCS situations should be formally identified at the design stage in order to be monitored during the plant operation, and a number of allowed occurrences should be assigned to each of them, according to usage factor assessment of each component.

6.4 The following types of failure modes should be considered in the design according to the relevant code requirements and limits:

- Excessive deformation;
- Elastic or elastic-plastic instability (buckling);
- Progressive deformation and ratcheting;
- Flow induced vibration (FIV);
- Progressive cracking initiation; mechanical and thermal fatigue;
- Stress corrosion cracking, erosion, embrittlement, thermal stratification, etc. should also be addressed.

6.5 Equipment of the RCS should be designed so that the stresses imposed upon it remain below the values defined for structural materials to prevent a fast growth crack during normal operational conditions, anticipated operational occurrences and accidents without significant core degradation.

6.6 At low operating temperature the ductility and pressure resistance of some materials may be significantly lower. Where such materials are used for the manufacturing, the allowable loadings at low operating temperatures should be defined, and the pressure and temperature ranges determined to prevent the risk of brittle fracture of the component. Allowances for changes in the nil-ductility transition (NDT) temperature of the RPV over the operational life of the plant should also be accounted for.

6.7 Adequate system(s) with appropriate accuracy, reliability and response time should be installed to detect a coolant leak and make its quantification possible in operational conditions.

6.8 Provisions to ensure that the components can be fully inspected during the life of the component should be addressed during the design. The design, requirements must be fulfilled during the manufacturing of RCS components. Following initial manufacture, a hydrostatic test in accordance with recognized code requirements should be performed prior to installation in the plant.

6.9 During the operating phase, in-service inspection and surveillance sample programs should be conducted in accordance with recognized codes and standards.

Reactor Pressure Vessel

6.10 Appropriate design and manufacturing provisions should be taken to justify the practical elimination of the RPV failure in all conditions[15:].

6.11 The RPV should be designed and manufactured in accordance with the latest edition of established codes and safety standards taking into consideration of available experience including manufacturing and operating experience.

6.12 The design considerations for the RPV should include the following:

- The number of welds in the pressure vessel should be minimized; in particular the need for welds in the active core region (beltline) should be assessed;

- Pressure and temperature limits should be established for the RPV and should be allow it 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.

The following recommendations are provided to fulfil Requirement 49 of [2].

6.13 Design provisions should be implemented for monitoring, display and control of the key RCS parameters (RPV pressure, RPV water level, steam flow, and feed-water flow) to maintain those parameters within their range specified for during normal operation and anticipated operational occurrences and to detect early deviation. Maintaining those parameters within their range for normal operation contributes to assuring adequate cooling conditions of the fuel.

6.14 Provisions to maintain adequate cooling conditions of the fuel should be classified items related to safety and be designed and manufactured accordingly to requirements associated to their safety class.

6.15 The following provisions and design recommendations should be considered for the design of the pressure control of the RCS:

---

[15] Does not apply to design adopting an ex-vessel core retention strategy in the event of an accident with significant core degradation

- The concept of defence-in-depth should be applied in the design of the pressure control of a nuclear power plant. According to this concept, systems and components with variable capacity should be used for pressure control to ensure that counter measures are proportional to the severity of an anticipated operational occurrence or accident;

- The diversity principle should be applied in the design of the pressure control systems to reduce the likelihood of common cause failures;

- Provisions should be made for normal operational conditions and anticipated operational occurrences by means of systems intended for pressure control to ensure that it will not be necessary to use Safety Relief Valves (SRVs) in the safety mode to limit the pressure increase;

- Setting and system performances should be determined on the basis of conservative assumptions based on accepted Codes and Standards;

- Pressure control in RCS should be ensured even in the event of a loss of off-site power;

- The pressure control system of the RCS should be designed to maintain the pressure within the limits ensuring the cooling of the fuel in all operational states;

- The pressure control system of the RCS should be designed to minimize the need during normal operation and anticipated operational occurrences to remove primary coolant outside closed systems.

The following recommendations are provided to fulfil Requirement 48 of [2].

6.16 The RCPB should be provided with an overpressure protection system relying on redundant SRVs. The settings should be designed on the basis of a sequential opening of the SRVs to ensure that no more valves than required are opened to control the overpressure.

6.17 The discharge capacity should be designed to meet the pressure limits prescribed by the industry codes and applying design rules specified by the code. Typically:

- Analyses do not credit non-safety classified systems unless their operation can aggravate the consequences of the initiating event;

- Safety classified systems are assumed to operate at their least favorable performances regarding the criterion to be met;

- Discharge capacity of the safety valves is determined on the basis of the applicable standard;

- The total discharge capacity credited in the analysis is calculated taking into account the sequential opening of the SRVs and that at least one SRV fails to open (or more for systems with a lot of SRVs);

- Loss of the off-site power is combined if it can aggravate the consequences of the initiating event.

6.18 The RCPB over pressure protection system should be designed to keep pressure below the design limits specified for the different categories of postulated initiating events in conjunction with the reactor scram.

6.19 RCPB integrity should be assured for load combinations of high pressure and low temperature when the reactor coolant system is operated at low temperature (protection of RCS equipment with materials of less ductility at low temperature).

6.20 Equipment ensuring the RCPB integrity should be designed to remain available without interruption in the event of the loss of the off-site power sources.

6.21 A reliable RCS depressurization system should be implemented to permit the injection of coolant to the RPV in the event that the high pressure Emergency Core Cooling (ECC) systems are unable to keep RPV water level high enough.

6.22 If the design of the SRVs utilizes pneumatic pressure to actuate the SRVs in the relief mode, the design shall include pneumatic accumulators to ensure that the SRVs can be opened a minimum number of times. The number of times that each valve must be opened utilizing the pneumatic accumulators without recharging should be defined. Primary containment pressure during a DBA needs to be included in determining necessary pneumatic storage capacity.

6.23 RCS depressurization should be completed prior the onset of core melting by opening and maintaining open a set of dedicated SRVs.

6.24 The pneumatic pressure required to open and to maintain open the necessary number of SRVs should be evaluated and dedicated design provisions should be implemented to ensure the opening of the SRVs.

6.25 No shut-off valves should be placed in the discharge line of a SRV, nor between the item being protected and a SRV.

6.26 The SRVs should be provided with a position indication that is independent of the control equipment.

6.27 The outlet of the SRVs should be instrumented in order to detect indications that a SRV is leaking past the seating surface or not fully closed.

6.28 The orientation and piping configuration of the SRVs, should include consideration for the potential accumulation of non-condensable gases and condensate as well as the adverse effects they may have as applicable.

6.29 When necessary, the set of SRVs used for overpressure protection and the associated piping should be designed to discharge steam as well as a steam-water mixture and water.

The following recommendations are provided to fulfil Requirement 20 of [2].

6.30 The RCS over pressure protection system should also be designed to preserve the integrity of the RCPB in case of postulated sequences involving multiple failures. Typically, the design of the over pressure protection system should be adequate to limit the pressure in the event of ATWS.

6.31 The depressurization system should also include dedicated SRVs to prevent direct containment heating loads caused by the RPV failure at high pressure.

Isolation of the Reactor Coolant Pressure Boundary

Reactor coolant pressure boundary means all those pressure-containing components of boiling water-cooled nuclear power reactors, such as pressure vessels, piping, pumps, and valves, which are:

- Part of the reactor coolant system, or

- Connected to the reactor coolant system, up to and including any and all of the following:

- The outermost containment isolation valve in system piping which penetrates primary reactor containment,
- The second of two valves normally closed during normal reactor operation in system piping which does not penetrate primary reactor containment,
- The reactor coolant system safety and relief valves,
- The reactor coolant system extends to and includes the outermost containment, isolation valve in the main steam and feed water piping,
- Small diameter pipe less than a defined diameter may be excluded based on normal makeup capability.

The following recommendations are provided to fulfil the requirement 6.13 of [2].

6.32 Isolation devices between RCS and connected systems with a lower safety classification should be designed to close quickly and reliably in order to limit the loss of primary coolant in the event of a piping failure outside the primary containment affecting a connected system. The loss of primary coolant caused by the failure of connected piping outside the primary containment should not necessitate the operation of safety systems.

6.33 Flow restrictors should be included in the main steam lines to limit the rate of loss of coolant following a main steam line break inside or outside the containment for ensuring that the core remains fully covered by water before the closing of the MSIVs.

6.34 Consideration should be given to the characteristics and importance of the isolation and its reliability targets. Isolation devices either should normally be closed or should close automatically on demand without the need for off-site electrical power. 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). In particular, to keep the full efficiency of the safety injection, all the systems connected to the RCS should be automatically isolated in a timely manner unless necessary to meet the requirements applicable to a Loss of Coolant Accident (LOCA) accident. The closure of various isolation valves and isolation of systems is determined based on selected parameters and set points.

6.35 Adequate isolation should be provided at the interfaces between the RCS and connected systems operating at lower pressures to prevent the over pressurization of such systems and possible LOCA. In any case the possibility of a LOCA occurring in the lower pressure designed piping should be eliminated to the extent practical. This is event is known as an Inter-Systems LOCA (ISLOCA).

6.36 Isolation devices should be considered as RCS components and hence should be designed and manufactured in compliance with the requirements and recommendations that apply to RCS components.

6.37 RCS isolation valves and devices should be qualified to operate under the most severe environmental conditions expected when required to operate.

6.38 The position of the isolation valves following a loss of signal or control power should fail in a position determined to be the safest.

6.39 RCS isolation valves should be supplied by the uninterruptible power sources.

6.40 RCS isolation function should be designed according to the single failure criteria.

Postulated Initiating Events

6.41 Failures of any component or system and operator errors whose consequences would modify the RCS conditions or the loads defined for normal operation should be identified and primarily categorized in a plant state category on the basis of its frequency to occur. The following are some examples:

- Loss of the Off-site power sources;
- Malfunctioning of Reactor Recirculation Flow Control;
- Malfunction of RPV level control;
- Loss of main condenser vacuum;
- Loss of Decay Heat removal system in shutdown modes
- Piping break resulting in LOCA;
- Spurious opening of a SRV valve;
- Loss of Feed water flow;
- Malfunction of Feed water heating control;
- Malfunction of Pressure Control.

Internal Hazards

6.42 The layout of RCS piping supplemented by local protection devices (anti whipping devices, shields, etc.) should be such that domino effects are prevented in the event of a high energy pipe break. The following are some examples:

- A single initiating break of a main steam or feed water line should neither propagate to neighbouring main steam or feed water piping;
- A single initiating break of a main steam or feed water line should not propagate to neighbouring ECC piping;
- A single initiating break of a main steam or feed water line should neither propagate to neighbouring shut-down cooling or reactor water clean-up piping.

6.43 Instrumentation required ensuring the actuation of necessary automatic actions and the accident management should be located outside the primary containment to the extent practical.

6.44 For instrumentation that cannot be practically located outside the primary containment; layout provisions to protect the instrumentation and instrumentation tubing should be implemented. The layout should provide protection to the instruments and tubing to ensure the necessary signals are available for the actuation of necessary automatic actions and the accident management.

External Hazards

6.45 The integrity of the RCPB should be maintained in the event of a SL2 earthquake.

6.46 RCS components which are not part of the RCPB and that are not seismically classified should be reliably isolated from the RCPB by isolation devices seismically classified and qualified to operate under SL 2 seismic loads.

6.47 RCS components necessary to bring the reactor to safe shut-down conditions should be seismically classified in order to keep their integrity and qualified to operate under SL 2 seismic loads.

6.48 RCS components necessary to bring the reactor to safe shut-down conditions should be designed to keep their integrity and to operate in the event of external hazards causing high energy impact on the containment structure or Reactor Building.

Layout

6.49 The design should meet the needs for the physical separation of redundant equipment and should preclude the common cause failure of redundant components and systems due to internal and external hazards.

6.50 The layout and arrangement 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.

6.51 If the plant design includes passive heat removal capability, the arrangement of piping and the location of equipment should enable removal of residual heat from the reactor core by natural circulation.

Design Limits

6.52 During the detailed design, of the RCS and associated systems, the mechanical and thermal limits should be clearly defined. This includes definition of design pressure and temperature (limits in AOOs, DBAs, ATWS as well other DECs). Examples of this are:

- Max cooling rate, max heating rate in Normal Operation (startup and shut-down);
- Max RCS leak rate;
- Component parameters (e.g. Core Delta P, parameters for RCS pump seals);
- RPV shell temperatures.

Design Basis Loads and Load Combination

6.53 Structural design criteria should be established on the basis of a limited number of loads and load combinations (design basis loading conditions) defined as envelopes of loads to which the equipment could be subjected over its lifetime taking into account the normal plant operation, postulated plant events, natural phenomena and site related hazards considered in the design basis of the equipment.

6.54 Stresses caused by normal service and upset conditions should be less than the stress limits specified for those loading conditions categories. Moreover, the design pressure and temperature should not be exceeded, and the cumulative usage factor should be less than 1.

6.55 For loading conditions assigned in emergency conditions category, the design criteria should aim at preventing the fast fracture of the equipment subjected to the primary loads, and at avoiding excessive deformation or buckling. Stresses should be less than the stress limits specified for that loading conditions category. However, the pressure reached during an emergency condition could exceed the design pressure, provided the overshoot does not exceed the pressure that allowed by accepted codes (typically 110%).

6.56 For these loading conditions assigned in faulted conditions category, the design criteria should aim at preserving the integrity of the equipment. Stresses should be less than the stress limits specified for that loading conditions category. Loading conditions and combinations for RCS ranked in different categories are typically defined by accepted codes and/or the regulatory requirements of the licensing authority.

Safety Classification

6.57 Recommendations given by SSG-30 [10] should be considered for establishing an adequate classification of the different components and structures of the RCS.

6.58 Components which are part of the RCPB should be classified so that they are designed and manufactured in compliance with the highest standards defined by the industry for nuclear application (e.g. ASME Section III, Division 1, subsection NB, RCC-M1 code or similar standards).

6.59 Other pressure boundary component and non-pressure boundary component should be classified with due account taken of the two effects resulting from its failure (function not accomplished and radioactive release) according to detailed guidance given by [10].

Environmental Qualification

6.60 The following RCS components should be designed or qualified for the harshest environmental conditions that could prevail inside the containment prior to or during accident conditions without significant core degradation until their mission time is completed:

- RCPB components (for integrity);
- The selection of materials to be used for gasket and seals (e.g. elastomer) should be based on their suitability to maintain their capability when exposed to operating and accident conditions;
- RCPB isolation devices (for operability);
- Over pressure protection components (for operability);
- RCS components necessary to bring the reactor to safe shut-down conditions (for operability);
- Components designed to depressurize and maintain depressurized the RCS in order to allow the use of low pressure ECC systems and to prevent Direct Containment Heating loads caused by the RPV failure at high pressure.

Venting

6.61 In order to accommodate level changes in the RPV during shut-down and start-up, remotely operable valves should be provided to vent the RPV head.

6.62 During normal operation venting of the RPV head to prevent the accumulation of non-condensable gases should be possible.

6.63 The equipment needed for RCS venting should meet the following requirements:

- 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.

Specific design aspects

Reactor pressure vessel

6.64 The design considerations for the pressure vessel should include the following:

- The provisions previously indicated to fulfil Requirement 49 of [2]

- 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;

- Minimization of thermal cycling at the vessel nozzles and penetrations including the use of thermal sleeves as appropriate;

- A corrosion resistant cladding applied to the interior of the RPV.

RPV Internals

6.65 Pressure vessel internals should be removable to facilitate maintenance, replacement and in-service inspection. Use of bolted connections should be considered in lieu of welded connections where appropriate.

6.66 The seismic design of the vessel internals should ensure that the ability to safely shut-down the plant following a Design Basis Earthquake is maintained. This means that the internals that are considered to be part of the core support are classified as SL2. Other parts of the vessel internal need not be classified as SL2 but should not fail in a manner that would prevent the plant being from able to reach and maintain a safe shut-down condition.

6.67 Pressure vessel internals should be designed to:

- Prevent unacceptable flow induced vibration;

- Minimize the susceptibility to stress corrosion cracking;

- Properly channel the coolant flow through the vessel and fuel;
- Accommodate asymmetric blow-down loads caused by pipe ruptures;
- Ensure that fuel design limits are not exceeded in normal operation or anticipated operational occurrences.

Reactor Recirculation Pumps

6.68 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.

6.69 Providing excess flow capability to extend the operating domain of the core should be assessed and defined during the initial design.

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

6.71 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

6.72 The use of seal less design pumps should be preferred.

Piping system

6.73 RCS piping should be of a suitable material such as stainless or alloy steel.

6.74 Capability should be provided for venting and drainage of the piping system.

6.75 Piping should be arranged to limit the possibility of accumulations of non-condensable gases.

6.76 Even though the probability of the piping failure is very small, the consequences of the double ended break of a pipe may have to be analyzed with appropriate rules regarding:

- The structural behaviour of RCS equipment and associated internals;
- The management of the three main safety functions and, in particular, the achievement of core cooling;
- Limiting the differential pressure across the reactor internals.

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

Leak before break piping

6.78 If a leak before break concept is to be applied, the requirements for design and manufacturing of piping should be defined. The required capability of the Leak Detection System should also be defined.

Insulation materials

6.79 Insulation material used inside the primary containment should be selected in order to prevent suppression pool suctions strainer clogging in case of high energy pipe breaks. Use of reflective metallic insulation (RMI) to the extent practical should also be considered.

SYSTEMS FOR COOLANT INVENTORY AND CORE REACTIVITY CONTROL IN OPERATIONAL STATES

Reactor Water Clean-up (RWCU)

6.80 The flow pattern in the RPV should be optimized to prevent the occurrence of areas of stagnant flow (to avoid the accumulation of precipitates) and limit pockets of cooler water which could result in reactivity excursions or unnecessary thermal stresses.

6.81 The design should also provide for the following:

- Limitation of the concentration of contaminants and impurities in the reactor coolant;
- Monitoring of the conductivity of the reactor coolant and for contamination of the sampled fluid;
- Control of water level during shut-down and low power conditions to remove excess water from the RCS.

6.82 Use of the RWCU as the primary or alternate means of residual heat removal during shut-down conditions should be considered.

SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES

The following recommendations provide guidance to fulfil Requirement 51 of [2] and supplement the generic recommendations indicated in section 3.

6.83 The design of the plant should include appropriate systems to remove residual heat from RCS in the different shut-down conditions (e.g. hot shut-down, cold shut-down and in refueling).

6.84 Heat removal capacity should be designed to cool the RCS down from hot shut-down conditions (once the reactor is shut-down) to conditions adequate for refueling operation in a reasonably short period.

6.85 Minimum heat removal capacity should be designed to remove residual heat despite a single failure postulated in any system necessary for removing residual heat. Moreover, the RHR system should be designed with sufficient capacity such that in the event a train or division is unavailable during Hot or cold Shut-down conditions, cool down can continue but at slower rate.

6.86 Maximal heat removal capacity should be designed taking into account operational criteria (e.g. time delay to reach refuelling conditions) without exceeding the limits specified in normal conditions for the fuel and the reactor coolant pressure boundary.

6.87 Residual heat removal should be possible in the event of the loss of the off-site electrical power sources.

6.88 Residual heat removal systems should be designed in compliance with all the recommendations given in section 3 if they are also operated to remove and transfer residual heat after a design basis accident (see paragraph Residual heat removal in accident conditions).

Isolation Condensers (if included in design)

6.89 Isolation Condenser should normally be aligned to the RCS and should be designed with the same recommendations of the RCS.

6.90 The design of the process control and vent valves should be based on the electrical power sources assumed available at the start of the event. The volume of available water to support operation of the ICS should be determined by defining the period of time that operation is ensured without refilling the water in the ICS pools. Recommended capability is a minimum of 72 hours but at a minimum should meet the requirements of the regulatory authority.

6.91 The isolation condenser tubes and tube sheets should be designed for the maximum stresses and most severe fatigue conditions expected to occur in operational states and in design basis accident conditions.

6.92 The design of the isolation condenser should provide an adequate system for tube leakage detection and alarm.

6.93 The design should prevent the collection of gases trapped in the steam space of the upper tube sheet and inlet piping of the isolation condenser.

SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS

Core cooling in case of design basis accidents

6.94 Emergency Core Cooling Systems (ECCS) should be designed and implemented to fulfil Requirement 52 of [2] in the event of DBAs with a loss of primary coolant:

- The ECCS should be designed to cool the fuel within the limits relevant for fuel and fuel cladding in the event of a LOCA taking into account rules specified for DBA analysis;

- In the case of a small pipe break, energy removed at the break may not be sufficient for an effective cooling of the fuel, and therefore complementary system or equipment should be operated to achieve the appropriate cooling capacity (e.g. complementary periodic opening of one or more SRVs to transfer steam (energy) to the suppression pool or to achieve adequate core cooling by the actuation of the low pressure emergency core cooling system;

- The ECCS should be designed with adequate capabilities to prevent or to limit uncovering of the fuel assemblies for the different sizes of primary piping breaks;

- The design of the overall ECCS should include both high pressure and low pressure capability. The availability of high pressure ECCS can be used in response to AOOs and small break LOCAs without the need to depressurize the RCS;

- The ECCS should be designed to restore and maintain an adequate coolant inventory in the RCS in order to maintain an adequate cooling of the core;

- The ECCS should include capabilities to remove residual heat in the long term taking into account that RCS integrity cannot be maintained;

- Taking into account the role of the emergency cooling of the core in the event of DBAs, system(s) should be assigned in SSG-30 safety class 1. Individual components should be designed and manufactured according to the relevant engineering requirements given by the industry codes. Taking into account their own role in the accomplishment of the emergency cooling of the core and the release of radioactive materials in case of its failure (e.g. pressure retaining equipment necessary for the accomplishment of the functions as expected, is widely designed and manufactured applying ASME Code, Section III, Division 1, Subsection NC, or RCC-M2).

6.95 The ECCS should have sufficient capacity to keep the core entirely submerged during the most limiting event.

Residual heat removal in case of design basis accidents

6.96 The design of the plant should include additional systems to remove residual heat from the RCS in the event of design basis accidents when systems operated in normal shut-down conditions are not designed in compliance with engineering design requirements applicable to safety systems.

Core cooling in case of design extension conditions

6.97 Design extension conditions requiring additional needs (safety features for DECs) are reactor technology / design dependent, and they should be postulated either applying a deterministic approach or supported by the outcomes of PSA.

6.98 Needs for additional safety features to assure the emergency cooling of the core in the event of loss of coolant accidents combined with multiple failures in the emergency core cooling system (ECCS) should be evaluated and implemented as necessary.

6.99 The ability to adequately cool the core in the event of a DEC should be focused on ensuring that a DEC does not result in core melt. As such, the primary focus should be in ensuring that most probable CCF sequences identified for consideration as part of DEC without significant core degradation can be successfully mitigated utilizing equipment on the plant site.

SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS

The Control Rod system is not discussed in the context of this guide (see [18]).

6.100 The RCS should have an associated system that is capable of a diverse means of shut-down by injecting a liquid containing a neutron absorbing substance and referred to as the Standby Liquid Control System (SLCS). This system provides a diverse means of bringing the reactor to a subcritical condition and is used in the case where the control rods cannot be physically inserted.

6.101 The amount of neutron absorbent material injected to the RPV should be enough to insert sufficient negative reactivity into the core to ensure the reactor remains subcritical in the most reactive state with sufficient margin for uncertainties for all DBAs and AOOs.

6.102 The injection rate of the neutron absorbing material should at a minimum conform with the requirements of the licensing authority.

6.103 The ability to inject neutron absorbing material into the RPV should be possible even in the event that off-site power is unavailable.

7 SPECIFIC CONSIDERATIONS IN DESIGN OF PHWRS

REACTOR COOLANT SYSTEM (Primary Heat transport system)

The PHWR key process systems consist of primary heat transport system (including the shut-down cooling system (SDCS)) and the moderator system. The primary heat transport system circulates pressurized heavy water through the fuel channels to remove the heat produced in the fuel. This heat is transferred to ordinary light water in the steam generators located inside the reactor building. During shut-down periods, the SDCS is used in conjunction with the primary heat transport system for removing residual heat from the fuel.

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 comprises the primary coolant pumps, the primary side of the steam generators, the reactor inlet and outlet headers, the fuel channels, the pressurizer, the feeders and the piping up to and including the isolation devices; and the SDCS which comprises sets of pumps and heat exchangers.

The heavy water moderator is circulated through the calandria and cooled in a relatively low temperature, low pressure system. The system comprises pumps and heat exchangers. The heat exchangers remove the nuclear heat generated in the moderator and the heat transferred to the moderator from the fuel channels. Helium is used as a cover gas over the heavy water moderator in the calandria. Chemistry control of the moderator water is maintained by the moderator purification circuit.

CONNECTED SYSTEMS

The systems that are directly connected to the RCS perform the safety function of ensuring the integrity of the RCS during operational states and accident conditions. They include but are not limited to:

- The fuel handling, including the re-fuelling machines;
- The pressure control and inventory control system;
- The pump seal cooling system;
- The emergency core cooling system;
- The shut-down cooling system;
- The heavy water collection system.

ASSOCIATED SYSTEMS

The associated systems are those essential to the safe functioning of the RCS and connected systems. The associated systems in a PHWR include but are not limited to:

- The moderator and its cooling system;
- The shield cooling system;
- The steam and feed water system;
- The auxiliary feed water system.

7.1 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.

7.2 To preserve the integrity of its pressure boundary the following types of damage should be considered according to the relevant code requirements and limits:

- Excessive deformation and plastic instability;
- Elastic or elastic-plastic instability;
- Progressive deformation;
- Progressive cracking initiation (fatigue);
- Fast fracture.

7.3 Equipment of the RCS should be designed so that the stresses imposed upon it remain below the values defined for structural materials to prevent fast crack growth during normal operational conditions, anticipated operational occurrences, design basis accidents and accidents without significant core degradation.

7.4 At low operating temperature the ductility and pressure resistance of some materials may be significantly lower. Where such materials are used for the manufacturing, the allowable loadings at low operating temperatures should be defined, and the pressure and temperature ranges determined to prevent the risk of brittle fracture of the component.

7.5 The pressure boundary materials, the pressure-temperature limits and the integrity of the reactor pressure boundary, including embrittlement considerations, should all be taken into account in this information.

7.6 Groups 1 and 2 should be physically separated by distance or barriers to ensure that a single design basis event will not disable systems in both groups.

7.7 The layout of the RCS should be such that main RCS equipment is protected against the effects of internal hazards (e.g., high energy pipe break, missiles and heavy load drop).

7.8 In conjunction with an adequate consideration of loads in the design basis of RCS equipment, layout provisions should be implemented to avoid propagation of failures among RCS equipment.

7.9 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.

7.10 Adequate system(s) with appropriate accuracy, reliability and response time should be designed to detect a leak and make its quantification possible in operational conditions.

Fuel channel assemblies

7.11 The fuel channels 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 coolant around and through the fuel bundles.

7.12 The fuel channel assemblies should be designed to meet all applicable requirements for the specified design life.

7.13 The fuel channel design should permit continuous gas flow in the annulus between the pressure tube and the calandria tube to allow leak before break detection.

7.14 All materials used in the fuel channel assembly must withstand prolonged exposure to the following environments: radiation, high-purity heavy water and the cover gas (e.g., the gas between the pressure tubes and the calandria tubes).

7.15 The fuel channels design conditions should be taken as the most adverse combination of temperature and pressure anywhere along the length of the pressure tube.

7.16 The fuel channels should be designed and manufactured in accordance with established codes and standards taking into consideration available experience including operating experience.

7.17 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.

7.18 Rolled joints employed in RCS should be tested for pull-out strength. The axial pull out load should be at least three times the design condition total axial load when the test is performed at design temperature.

7.19 Non-inspectable welds should be limited to the extent possible and analyses should be performed to assess the consequences of the failure.

7.20 Fuel channels 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.

Steam generators

7.21 The main function of the steam generators is to transfer heat from the reactor coolant of the primary circuit to the secondary circuit and to provide steam to operate the turbines.

7.22 The steam generators should facilitate the natural circulation in primary circuit.

7.23 The steam generators are parts of the primary pressure boundary. The primary side should be assigned to the safety category1 and be designed to withstand SL2 seismic loads. The design and manufacturing codes should be specified.

7.24 The steam generators tubes and their internal structures should be designed for the maximum stresses at maximum temperatures and most severe fatigue conditions expected to occur in operational states and in accident conditions.

7.25 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.

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

7.27 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 secondary side of the steam generators;
- Addition of chemical additives to the feed water;
- Monitoring of the conductivity and for contamination of the sampled fluid;
- Draining.

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

7.29 The design provisions should be taken to address overfilling of the steam generators that may occur as a consequence of PIEs.

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

7.31 The design should include blow-down provisions to control, for the secondary sides of the steam generators, the amount of solids (sludge) that could accumulate in areas of stagnant flow.

7.32 The design should include provisions for sampling of fluids from relevant location of the secondary side.

7.33 The design of the steam generators should be such that the following safety parameters are adequate:

- Primary pressure drop;
- Heat transfer;
- Tube plugging allowance;
- Fouling allowance;
- Maximum allowable tube leakage;
- Cold and hot plenums separator (divider plates) should be strong enough to withstand a loss of coolant accident (LOCA);
- Provisions to avoid tube fretting.

7.34 Steam generators design should prevent consequential ruptures of heat exchange tubes induced by a single tube rupture.

7.35 Heat exchange tubes material, tube plate material and welding materials should withstand corrosion/erosion impact of primary/secondary coolant, including under-sludge corrosion.

7.36 Electro-chemical interaction of heat exchange tubes material and tube supports material should be prevented.

7.37 To ensure the integrity and reliability, provisions in the design and layout should be implemented to enable inspection of major components to be carried out during outages.

7.38 The heat transfer should be ensured in operational states and some postulated accident conditions. Ranges of power and other relevant parameters (e.g. temperature and pressure of the primary coolant) should be specified for each plant state.

7.39 Design provisions implemented to achieve and to preserve the integrity of the primary and secondary shells and of the tube should be designed to meet the acceptance criteria for integrity defined for the different plant states.

7.40 The layout of the piping and equipment should be such that flow induced vibration, flow accelerated corrosion (FAC), aging effects, acoustic excitation, and thermal-fatigue and the accumulation of radioactive material are minimized. Harmful consequences of accidental flooding should also be minimized.

7.41 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.

7.42 The layout of the piping and equipment should provide sufficient accessibility to allow periodic testing, maintenance and inspection, including maintenance and inspection for welds and piping supports, to be conducted.

7.43 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.

7.44 The design should be such that the risk of stress corrosion cracking (SCC) is minimized, for all operational conditions, wherever dis-similar metal welds are employed.

7.45 The choice of materials, for the piping of the RCS including feeders and headers should be corrosion-resistant, especially against FAC.

7.46 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 in design. A system should be provided to monitor for and to collect any leaks.

Reactor coolant pumps

7.47 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 met with sufficient margins in operational states.

7.48 The pumps in the RCS should have adequate flow coast-down characteristics in the event of a pump trip under normal operation or accident conditions to avoid undesirable thermal-hydraulic conditions of the reactor coolant with regard to the integrity of the fuel.

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

7.50 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.

7.51 The design of the pumps should be such that the following safety parameters are adequate:

- Pump performance characteristics, including head/flow characteristics, flow coast-down rate, single and two-phase pump performance;
- Pump operating parameters, e.g. speed, flow, head;
- Pump net positive suction head needed to avoid cavitation;
- Pump seal design and performance (including seal temperature limitations, if applicable);
- Vibration monitoring provisions.

7.52 The pumps should be designed to avoid any fuel-pressure tube fretting and fuel endplate cracking due to the pump vane passing frequency (acoustic excitation) during all operational and accident conditions.

Pressure and inventory control

7.53 The pressure and inventory control of the RCS should be designed to maintain the pressure within the limits specified for the operational states.

7.54 If the pressurizer can be isolated from the RCS in certain operating conditions (i.e. during warm-up or cool-down), 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 devices.

7.55 The pressurizer and the bleed condenser vessels should be designed to enable changes in primary coolant volume, arising from normal load changes and operational transients, to be accommodated without actuating the safety systems or the overpressure protection devices.

7.56 The pressurizer and the bleed condenser should be designed to maintain, in conjunction with the primary coolant make up system, the RCS water inventory within the limits specified for the operational states.

7.57 The RCS should include an overpressure protection system to preserve the structural integrity of the RCS boundary by keeping, in conjunction with the reactor shut-down system, the pressure below the design limits specified for the different categories of postulated initiating events.

7.58 The overpressure protection system should be designed to provide protection against unacceptable load combinations of high pressure and low temperature when the reactor coolant system is operated at low temperature (protection of RCS equipment with materials of less ductility at low temperature).

7.59 The configuration of the vessels, the layout of the spray lines and nozzles, the layout of the surge line should avoid or minimize the low and high cycle fatigue, thermal stratification, and accumulation of condensate.

7.60 The in-service inspection program defined for the reactor coolant pressure boundary should also be used for the vessel of the pressurizer and the bleed condenser.

7.61 Spray nozzles should be easily inspectable and replaceable.

7.62 Postulated initiating events leading to a pressure transient in normal operation including operation at low pressure should be identified and categorized according to their estimated frequency of occurrence. For each of them, SSCs designed to respond should be identified.

7.63 The safety class assigned to the reactor coolant pressure boundary is also assigned to individual items belonging to the reactor pressure boundary. The safety class assigned to the non-pressure retaining components is determined to be commensurate to their individual safety significance.

7.64 Items belonging to the reactor coolant pressure boundary should withstand the seismic loads and are therefore expected to be of seismic category 1.

7.65 Safety valves ensuring the overpressure protection of the RCS system at any temperature should be of seismic category 1.

7.66 The non-pressure retaining equipment should be of seismic category 2 so that their failure does not compromise seismic category 1 equipment.

7.67 The overpressure protection devices should be designed to be protected against the effects of internal hazards.

7.68 The pressure and inventory control including the overpressure protection devices should be designed to accomplish their intended functions in case of the loss of the off-site power.

7.69 The pressure and inventory control should be designed such that the safety valves do not need to open to control the pressure in operational states.

7.70 The control of pressure in operational states should not lead to release of coolant into the containment atmosphere.

7.71 The overpressure protection devices should have sufficient discharge capacity so that the RCS design limits established for the different overpressure transient categories are not exceeded. Limits given by proven industry codes and standard applicable to nuclear pressure vessel should be used.

7.72 The safety valves, including the relief valves, should be qualified for discharge of steam, water-steam mixture and water at the appropriate reactor condition.

7.73 The overpressure protection devices should include redundant safety valves. The setting of the safety valves should be such that safety valves open in sequence for different levels of pressure to avoid unnecessary discharge of coolant.

7.74 No shut-off valve should be placed in the discharge line of a safety valve, nor between the item being protected and a safety valve. If exceptions are made to deal with the failure to close of some safety valves, the inadvertent closing of the shut-off valves should be reliably prevented.

7.75 Relief and safety valves should be equipped with a position indicator in the main control room (MCR).

7.76 Diverse ttechnologies should be used for pressure and inventory control, and the overpressure protection devices to reduce the likelihood of common cause failure.

7.77 The overpressure protection devices should be designed and qualified not to open spuriously when equipment is subjected to harsh ambient conditions and to keep its operability to ensure a permanent protection of the integrity of the reactor coolant system.

7.78 In case of overpressure due to design basis accident conditions, analysis should be performed to demonstrate that the acceptance criteria are met. The analysis should be performed with an adequate grade of conservatism to justify that margins provided by the design are appropriate to accommodate uncertainties and to prevent cliff-edge effects. The following elements should be considered:

- Analyses do not credit non-safety classified systems unless their operation can aggravate the consequences of the initiating event;
- Safety classified systems are assumed to operate at their less favourable performances regarding the criterion to be met;
- Discharge capacity of the safety valves is determined on the basis of the applicable standard;
- The total discharge capacity credited in the analysis is calculated taking into account the sequential opening of the safety valves and that one safety valve at least fails to open;
- Loss of the off-site power is combined if it can aggravate the consequences of the initiating event.

7.79 The effectiveness of the overpressure protection at low operating temperature should be demonstrated taking into account the specified ranges of pressure and temperature established for the plant normal operation.

Provisions for fast depressurization of the primary heat transport system (crash cool-down)

7.80 PHWRs should be equipped with a fast depressurization of the primary circuit by the crash cool-down of the steam generators secondary side (or equivalent) using the steam relief valves.

7.81 The design should demonstrate that during crash cool-down:

- The secondary side of the steam generators inventory should be sufficiently maintained to cool and depressurize the RCS;

- Water inventory in the RCS should be maintained;

- The heat transfer mechanism (e.g., thermo-syphoning or intermittent buoyancy induced flow (IBIF)) in the RCS should not be disrupted.

7.82 A crash cool-down or an RCS depressurization should not result in any reactivity or structural concerns.

SYSTEMS FOR OPERATIONAL STATES

This section presents the systems designed for maintaining the reactivity control and the cooling safety functions during operational states.

REACTIVITY CONTROL

This section presents the systems designed for the reactivity control function during operational conditions. It focusses only on the systems which involve injecting a liquid solution into the primary heat transport system or into the moderator system. The reactor regulating system (reactivity control system) is addressed in the Safety Guide [18].

7.83 The reactor regulating system includes liquid zone control units, control absorber units and adjusters that can be used to absorb neutrons and reduce reactor power if larger power reductions are required. The liquid zone control units consist of independently adjustable liquid zones that introduce light water in zirconium alloy tubes into the reactor. Light water is a stronger absorber of neutrons than heavy water. Controlling the amount of light water controls the power of the reactor. On-power refuelling and zone-control actions provide reactivity control.

HEAT REMOVAL SYSTEMS

This section presents the systems designed for maintaining the cooling safety function during operational states. In operational states, several systems could be credited for heat removal. These systems consist of the main steam and feed water system, the shut-down cooling system and the auxiliary feed water system.

Steam and feed water system

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

The steam and feed water system is composed of the main steam lines and the feed water supply to the steam generators. The main steam lines supply steam from the steam generators in the reactor building to the turbine through the steam balance header, located in the turbine building, at a constant pressure. The feed water system controls the flow to maintain the required steam generators level.

7.84 In normal operation, the steam and main feed water 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.

7.85 The feed water system should take hot, pressurized feed water from the feed water train in the turbine building and discharge it into the preheater section of the steam generators.

7.86 Provision should be made to control the system pressure and the coolant inventory in the steam generators during start-up.

7.87 The main steam and feed water system should have sufficient capacity to dissipate heat to the ultimate heat sink during the initial phase of plant cool-down.

7.88 The main steam and feed water system should have sufficient capacity to dissipate heat to the ultimate heat sink when the main condenser is not available.

7.89 Main steam isolation valves (MSIVs) should be provided to isolate the main steam supply to the turbine in the event of steam generators tubes leak, after the reactor is shut-down, the SDCS is placed in service and the primary heat transport system is depressurized.

7.90 The safety class of the piping from the steam generators up to and including the main steam isolation valves and the main feed water isolation valves should be the same as the safety class of the steam generators secondary side.

7.91 Heat removal redundancy should be provided to the extent necessary to permit controlled cool-down of the RCS when the ultimate heat sink is not available or the main steam line is isolated.

7.92 The main steam and feed water system should be provided with devices such as safety valves for the overpressure protection of the steam generators secondary side when the main steam and feed water isolation valves are closed.

7.93 The capacity of the safety valves should be adequate to limit the maximum steam generators secondary side pressure within the acceptance criteria.

7.94 The system that controls the steam generators pressure should use steam discharge valves. These relief valves should also provide overpressure protection of the steam generators secondary side in addition to the main steam safety valves (MSSVs).

7.95 The materials used in the main steam and feed water system should have fracture toughness properties that afford protection against brittle fracture under all modes of plant operation for plant lifetime and should be compatible with the chemistry of feed water

7.96 As a minimum, the following should be displayed and/or alarmed in the MCR: steam flow rates, steam generators pressure, steam generators level, steam header pressure, feed water flow rates, feed water header pressure, feed water temperature, radioactivity levels, and key chemical parameters.

7.97 Controls should be provided for the main steam isolation valves and bypass valves to allow remote manual operation and automatic operation.

7.98 Controls should be provided for the valves to dump steam to the atmosphere to allow remote manual and/or automatic operation.

7.99 The main steam (safety and/or relief valves) devices should be capable of dissipating heat from the steam generators when the main condenser is not available for heat removal.

7.100 The main steam and feed water system should provide capability to automatically and/or manually bypass the turbine and discharge steam directly to the condenser. The capacity of the bypass should be adequate to accommodate the load rejections.

7.101 Provisions should be made to ensure that the failure of one steam line will not cause blow-down of the unaffected steam generators.

7.102 Steam lines and feed water piping should be routed, protected and restrained to prevent multiple accidents in the event of the rupture of a steam line, a feed water line or any other pipe.

Shut-down cooling system (residual heat removal system)

The SDCS consists of pumps and heat exchangers connected between the inlet and outlet headers of each primary heat transport system (PHTS) loop. The system is normally full of heavy water and is normally isolated from the PHTS by two valves in series.

The function of the SDCS, as the name implies, is to provide fuel cooling after a reactor shut-down, for an indefinite period of time. It is also designed to provide the cooling function with the primary heat transport system drained to the reactor headers to permit maintenance of the steam generators and the PHTS pump internals.

7.103 The SDCS should preferably be located inside the containment.

7.104 The SDCS should have the capability to control the heavy water level in the PHTS headers in the drained state.

7.105 The SDCS should have the capability to cool-down the PHTS where heat removal via the steam generators is suddenly not possible,

7.106 The SDCS should be designed also to remove residual heat when the reactor is shut-down following an accident by functioning as an alternative heat removal to the steam generators.

7.107 The shut-down heat exchangers should be designed to handle extreme temperature shocks.

7.108 The SDCS 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. The SDCS should have the capability to be used for draining of the PHTS when cold and depressurized.

7.109 The SDCS should have sufficient flow adjustment capability.

7.110 To ensure the integrity and reliability, provisions in the design and layout should be implemented to enable inspection of major components to be carried out during outages.

7.111 The heat transfer should be ensured in operational states and some postulated accident conditions. Ranges of relevant parameters (e.g. temperature and pressure of the primary coolant) should be specified for each plant state.

Auxiliary feed water system

The feed water could be composed of the following systems:

- A main feed water system;
- An auxiliary feed water system;
- An emergency feed water system.

7.112 An auxiliary feed water system or equivalent should be designed to maintain the heat removal capability of the plant in the events where main feed water system becomes unavailable. The capability for heat removal of the auxiliary feed water system may be used to reduce the pressure in the RCS when necessary.

7.113 An auxiliary feed water system or equivalent should be designed to maintain the plant in a hot standby condition for an extended period. It can also have to be used to bring the plant to a cold shut-down. The auxiliary feed water system should provide sufficient capacity to fulfil these functions efficiently.

7.114 The design of the auxiliary feed water system should include connection lines to supply water into steam generators from the reserve water tank (also called the containment water tank or the dousing reservoir). Means for recording the amount of water supplied into the steam generators should be provided.

7.115 The design of the auxiliary feed water system should include connection lines to supply water into steam generators from the fire engines or mobile diesel-pumps. Means for recording the amount of water supplied into the steam generators should be provided.

SYSTEMS FOR ACCIDENT CONDITIONS

This section presents the systems designed for maintaining the reactivity control and the cooling safety functions during accident conditions, including DBAs and DECs without significant core degradation.

Reactivity control

This section addresses recommendations for systems designed for the reactivity control safety function during accident conditions, including DBAs and DECs without significant core degradation.

Reactor Shut-down System 2

Reactor shut-down system 2 (SDS2) provides a fast injection of the concentrated gadolinium nitrate solution into the bulk moderator through a number of horizontally distributed nozzles. Holes along the length of the injection nozzles within the calandria vessel form several rows of jets (up, down, and to each side) for the injected solution. SDS2 employs an independent triplicated logic system which senses the requirement for this emergency shut-down and opens fast-acting helium pressure valves to inject the gadolinium poison into the moderator.

7.116 The reactor shut-down systems 1 and 2 should be passive, fast acting, fully capable, diverse physically and functionally independent of each other.

7.117 For SDS2, chemistry-related issues (e.g.: avoiding precipitation) should be addressed.

7.118 SDS2 should be designed to meet the derived acceptance criteria for the reactor trip parameter effectiveness for all AOOs and DBAs.

7.119 In the poised state (i.e., capable of adding a sufficient negative reactivity to shut-down the reactor), provisions should be taken in SDS2 design to:

- Hold outside the reactor core a sufficient amount of neutron absorbing liquid (gadolinium nitrate) of the appropriate concentration, chemical composition and absorbing properties, ready to be injected into the moderator for shutting down the reactor;
- Provide means of verifying the amount of poison held and its concentration, correct chemical composition and absorbing properties;
- Provide means of injecting, as efficiently and effectively as possible, the poison into the moderator following an SDS2 reactor trip signal;
- Provide means of back-flushing the injection lines in which the poison concentration is excessive as a consequence of poison migration.

7.120 In the tripped state (i.e., the poison has been injected into the moderator to shut down the reactor and to maintain it sub-critical), provisions should be taken in SDS2 design to:

- Upon receipt of a Reactor Trip signal, SDS2 should quickly add sufficient negative reactivity to stop the sustained nuclear chain reaction and to shut down the reactor;

- In conjunction with the SDS2 Trip Logic Sub-system, SDS2 should be capable of maintaining the reactor sub-critical following an SDS2 Reactor Trip;

- SDS2 design should allow arresting the injection if the SDS2 Trip Logic Subsystem clears an unsealed-in Reactor Trip state.

7.121 The reliability should include sensing the need for shut-down, initiation of shut-down, and insertion of negative reactivity. All elements necessary to complete the shut-down function should be included.

Residual heat removal system

This section presents the systems designed for maintaining the cooling safety function during accident conditions, including DBAs and DECs without significant core degradation.

Systems designed for maintaining the cooling safety function for the DBAs include the emergency core cooling systems and the enhanced emergency heat removal system.

7.122 Systems in the RCSASs that are provided to mitigate the consequences of DBAs should be considered safety systems and be designed according to the rules established for these systems.

7.123 Systems that are provided to mitigate the consequences of DECs should be considered as design features for DECs and be designed according to the rules established for these features. The systems could be designed with appropriate redundancy within systems to achieve the required reliability.

Emergency core cooling system

The emergency core cooling system (ECCS) includes in general a combination of active and passive injection means (pumps, piping and valves) with different delivery pressures, depending on the designs, and also passive injection tanks (accumulators). The system may also include heat exchangers.

7.124 ECCS 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.

7.125 ECCS should be designed to cool the core adequately in the event of a double ended guillotine break of a header.

7.126 The emergency core cooling system injection capacity should ensure core re flooding in case of design basis LOCA, according to the applicable acceptance criteria (e.g.: maximum fuel sheath temperature).

7.127 The ECCS should be capable of maintaining the core in a coolable geometry and removing residual heat.

7.128 ECCS injection pressure may be lower than the steam generators relief devices opening pressure in order to limit the releases from the active steam generators in case of design basis steam generators tube rupture. Especially this pressure should be lower than the steam generators safety valves opening pressure in order to limit the risk that they open and fail to close.

7.129 ECCS injection pressure should limit the risk of causing an RCS overpressure.

7.130 Injection of a large volume of cold water may cause pressurized thermal shock to the reactor coolant pressure boundary or distortion of reactor internals, especially in cold shut-down states. The design should demonstrate that thermal shock has been addressed, in terms of calculating transient fluid conditions at key locations, resulting metal temperature and the corresponding stresses.

7.131 ECCS may ensure residual heat transfer to the heat exchanger by cooling the sumps in the event of DBAs, especially large break LOCA. The heat exchanger capability should allow limiting sump heat–up in a range compatible with the qualification conditions inside reactor building and with the qualification of ECCS pumps.

7.132 As the emergency core cooling system is connected to the RCS, it should be equipped with isolation devices, as required for reactor coolant pressure boundary (see RCS). These valves should be closed in normal operation and should open quickly in case injection is required. It should be possible to reclose them if the injection is stopped in the long term of an accident, especially if there is a leak suspicion on a train.

7.133 As the emergency core cooling system is partly located outside the containment, it should be equipped with containment isolation devices, as required by Requirement 56 of [2]. It should be possible to close the suction valves from the sumps at any time if a leak is detected on the system part located outside the containment, in order to prevent the drainage of the sump. Such isolation should be performed with a high level of confidence as its failure would lead to a severe accident with total depletion of the water reserves.

7.134 All the components of the emergency core cooling system that belong to the reactor coolant pressure boundary (injection nozzles) should be designed considering the same quality and the same loads as the RCS pipes.

7.135 Unplanned drainage of the emergency core cooling system water reserve should be prevented (e.g. specifically in case of external hazard). The containment penetrations of the ECCS pumps suction and the isolation valves should be adequately protected.

7.136 The ECCS pumps should be qualified to operate with active water loaded with particles, according to the filtration system capability. Qualification specification should consider the actual activity and debris release to be assumed in DBAs and DECs without significant core degradation (LOCA and secondary breaks).

7.137 Possible leaks in the parts of the emergency core cooling system that are located outside the containment should be monitored in order to be able to isolate the system before it causes the drainage of the water reserves and before it causes environmental conditions in the building that would preclude the isolation valves operation.

7.138 The ECCS isolation devices located outside the containment should be qualified to remain operable is spite of a possible leak from the ECCS.

7.139 Natural circulation flows, where credited, should be capable of providing sufficient flows and should not be impaired by such effects as accumulation of non-condensable gas or adverse temperature distributions.

7.140 In case of LOCA, local effect of the break (jet impingement, pipe whip) should be so limited that no more than one ECCS train is made unavailable.

Specific design aspects

7.141 The recirculation pumps of the ECCS should be located outside the containment in order to limit the severity of the environmental conditions for which they should be qualified to and also to facilitate maintenance and repair.

7.142 The ECCS provides an extension of the containment (3^{rd} barrier) when circulating water outside containment in the event of DBAs. This water may be highly radioactive, in case of fuel damage; therefore the structural design recommendations on component design should allow precluding radiological releases with a high confidence (see recommendations given in [15]).

7.143 The ECCS pumps may require motor and room cooling for proper operation. These support functions should be performed with a reliability level commensurate with their importance: if their failure may lead to the pump failure in a short time duration that precludes any set up of an alternative cooling, then the design recommendations on these systems should be consistent with those of the emergency core cooling system, according to [20].

7.144 The cooling of ECCS pumps by diversified means could be considered if their injection function is required in DECs where a common cause failure on cooling means is assumed.

Enhanced emergency heat removal system

The enhanced emergency heat removal system (EHRS) is to feed water to the steam generators in order to maintain heat removal capability.

7.145 The EHRS design should ensure that there is adequate long-term heat transfer available for the residual heat removal following a loss of the normal heat removal systems for the reactor (main and auxiliary feed water).

7.146 The EHRS should have independent passive (back-up emergency feed water) and active (emergency feed water) trains. Each of the active and passive trains alone of the EHRS should have sufficient capability to maintain sufficient water inventory in the secondary side of the steam generators.

7.147 The active train of the EHRS and its supporting SSCs should be designed to operate under the postulated initiating events considered as DBAs and resulting in the loss of normal heat removal systems.

7.148 The design of the active train of the EHRS that is provided to mitigate the consequences of DBAs should meet the safety systems design requirements.

7.149 The passive train of the EHRS and its supporting SSCs should be designed to operate under the DECs without significant core degradation.

7.150 The active train (emergency feed water) of the EHRS could have pumps taking suction from a source of on-site fresh water that is in a separate location from the main plant service water system intake. This active EHRS should have an automated emergency power supply (EPS) start-up and the connection lines to supply water to the secondary side of the steam generators.

7.151 The passive (back-up emergency feed water) train of the EHRS represents the reserve water tank (also called the containment water tank or the dousing reservoir) and connection lines (including valves and piping) to supply water to the secondary side of the steam generators.

7.152 The reserve water system is a backup water system and hence could be designed to be non-operational.

7.153 The reserve water tank should be designed to provide a gravity-driven passive light water make-up since no external power is needed to transfer its inventory to the various potential users once the isolation valves are opened.

7.154 The reserve water tank should be located at a high elevation in the reactor building.

7.155 The reserve water tank should have sufficient capacity to provide an emergency source of water by gravity to the steam generators (back-up emergency feed water), to the containment cooling spray, to the moderator system, to the shield cooling system and to the primary heat transport system if required.

7.156 The active and passive EHRS are required to be functional during and after a seismic event and therefore should be designed to meet the seismic requirements.

7.157 The design should demonstrate that emergency heat removal capability is provided for all operating and accident conditions.

7.158 For all means of emergency heat removal, all equipment should be appropriately designed to function in the class of accidents for which they are credited.

7.159 The design should provide provisions to allow in-service inspection of safety-related components and equipment; and allow operational functional testing of safety-related systems and components

7.160 These systems should be capable of removing the heat loads from safety-related SSCs under DBAs and DECs without significant core degradation.

7.161 The application of the single failure criteria is not explicitly required by [2] for all design safety features for DECs.

7.162 The appropriate emergency power supply (AC or DC) should be provided as necessary to components that are needed for actuation or operation of safety features for DECs.

7.163 The safety features for DECs should be qualified such that they will function for the most severe environmental conditions (including seismic conditions) under which they would be expected to operate.

7.164 Manual actuation of the safety features for DECs should be possible from the MCR and if appropriate from the SCR.

7.165 Process information and control capability should be provided in the MCR and in the SCR to enable the passive and active EHRS to be operated and to achieve adequate reactor residual heat removal on a long term basis.

7.166 To ensure the integrity and reliability, provisions in the design and layout should be implemented to enable inspection of major components to be carried out during outages.

7.167 Natural circulation systems require a demonstration of capability over the full range of applicable operating conditions.

7.168 The need for automatic actuation of safety features for DECs without significant core degradation should be evaluated in the safety analysis case by case.

7.169 In the cases where the active EHRS is credited for DBAs, analysis should be performed to demonstrate that the acceptance criteria are met. The analysis should be done with adequate conservatism to justify that the margins provided in the design are appropriate to accommodate uncertainties and to prevent cliff-edge effects.

7.170 In the cases where crediting the passive EHRS for DECs without significant core degradation, analysis should be performed to demonstrate that the acceptance criteria are met. The best estimate analysis methodology is acceptable.

Recommendations for heat transfer for DEC

The complementary design feature is to have the capability to transfer residual heat from the core to an ultimate heat sink.

7.171 The feature should be independent, to the extent practicable, of those used in more frequent accidents; be capable of performing in the environmental conditions pertaining to these DECs; and have reliability commensurate with the function that they are required to fulfil.

7.172 The design principles for design features to deal with DECs do not necessarily need to incorporate the same degree of conservatism as those applied to the design up to and including DBAs. However, there should be reasonable assurance that design features will function as designed when called upon.

7.173 The design rules for complementary design features should be clearly described and should include operating experience, latest results from R&D safety research and up to date design practices.

The moderator system can be operated as an emergency heat removal for DECs without significant core degradation.

The moderator system of the PHWR reactor is a low-pressure and low-temperature system. It is independent of the primary heat transport system. The moderator system consists of pumps and heat exchangers that circulate the heavy water moderator through the calandria and remove the heat that is generated during reactor operation. For normal operation and DBAs, the heavy water acts as both the moderator and reflector for the neutron flux in the reactor core.

7.174 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.

7.175 The moderator system fulfils a safety function that is unique to PHWR. The moderator system should be designed to act as an emergency heat removal for DECs without significant core degradation under the postulated accident condition of large loss of coolant accident coincident with the loss of the emergency core cooling system.

Moderator system can be operated as specific design aspects for DECs without significant core degradation.

7.176 The design of the moderator system should consider all configurations when credited as an emergency heat removal for DECs without significant core degradation.

7.177 Each configuration, independently, should have adequate load capacity to transfer the heat to the ultimate heat sink and to prevent calandria tubes' failure.

7.178 The heat load capability of the moderator system configuration for DECs without significant core degradation should be demonstrated by means of tests and analyses.

7.179 The moderator system should be designed such that forced convection and natural convection flows are in the same direction.

7.180 The moderator system components should be designed and built to higher standards than otherwise required in order to minimize the possibility of heavy water loss and maximize reliability.

7.181 The moderator pumps should be designed to retain their pressure integrity during and following a site design earthquake.

7.182 The moderator system should be designed for overpressure protection from the pressure transients arising in the calandria from the burst of pressure tube and calandria tube.

7.183 The calandria vessel should be equipped with overpressure protection devices such as rupture disks or equivalent devices.

7.184 The relief capacity should be sufficient to avoid over-pressurization limits of the SSCs credited for DECs without significant core degradation. Limits given by proven industry codes and standard applicable to nuclear pressure vessel should be used.

LIST OF ABBREVIATIONS

AC/DC: Alternative current / direct current

AOO: Anticipated Operational Occurrence

ATWS: Anticipated transient without Scram

BWR: Boiling water reactor

CCF: Common cause failure

DBA: Design basis accident

DEC: Design extension condition

ECCS: Emergency core cooling system

EFWS: Emergency feed water system

EHRS: Emergency heat removal system

FAC: Flow accelerated corrosion

LOCA: Loss of coolant accident

MCR: Main control room

MSIV: Main steam isolation valves

MSSV: Main steam safety valves

PHTS: Primary heat transport system

PHWR: Pressurized heavy water reactor

PIE: Postulated initiating event

PWR: Pressurized water reactor

RCS: Reactor coolant system

RCSAS: Reactor coolant system and associated systems

RCPB: Reactor coolant pressure boundary

RHR: Residual heat removal

RPV: Reactor pressure vessel

SCC: Stress corrosion cracking

SCR: Supplementary control room

SDCS: Shut-down cooling system

SDS2: Shut-down system number 2 (liquid poison)

SRV: Steam relief valves

SSC: Structures, systems and components

UHS: Ultimate Heat Sink

REFERENCES

[1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 Rev.1, IAEA, Vienna (2016).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal hazards in the Design of Nuclear Power Plants (DS494).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants (DS485).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.6, IAEA, Vienna (2002).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.13, IAEA, Vienna (2005).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, IAEA Safety Standards Series No. DS 482 (under revision).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Core for Nuclear Power Plants, IAEA Safety Standards Series No. DS 488 (under revision).

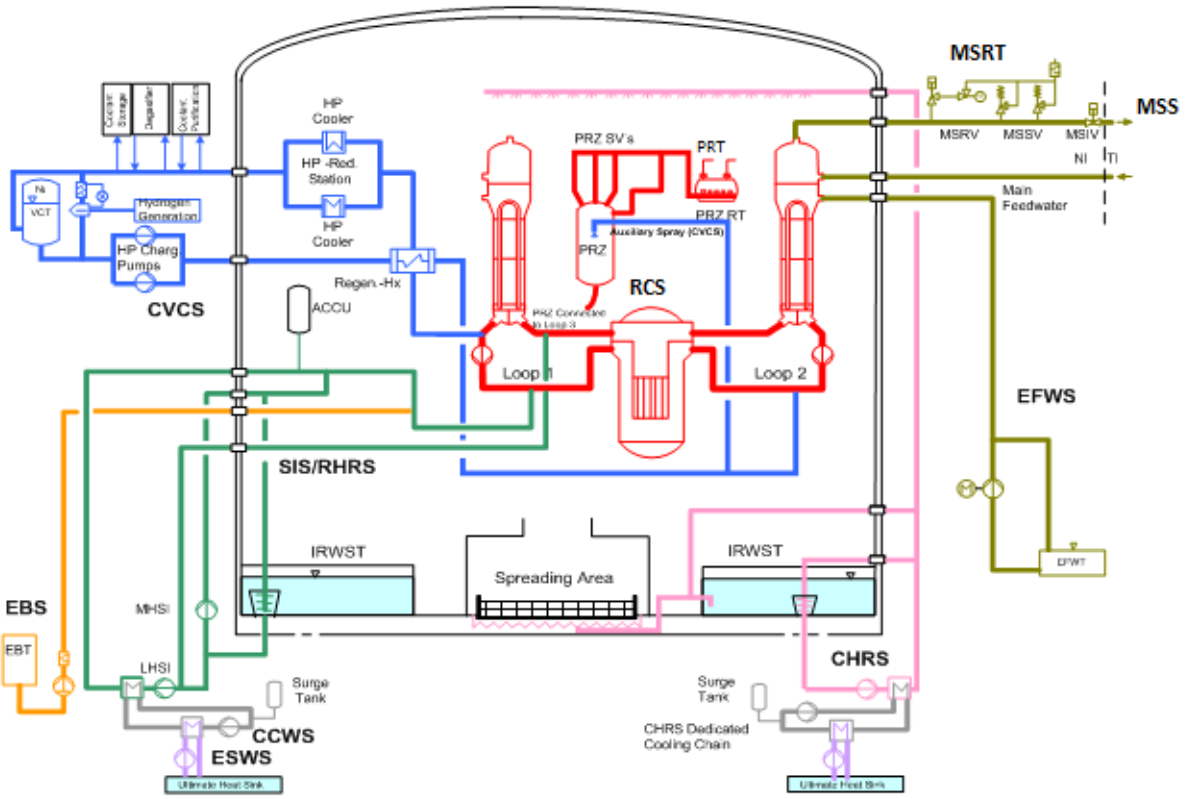
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Design of Fuel Handling and Storage Systems for Nuclear Power Plants, IAEA Safety Standards Series No.DS 487 (under revision).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Auxiliary and support systems for Nuclear Power Plants, IAEA Safety Standards Series No DS 440.

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

ANNEX I: PWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS



CCWS: Component Cooling System

CHRS: Containment Heat Removal System

CVCS: Chemical and

EBS: Emergency Borating System

EFWS: Emergency Feed Water System

ESWS: Essential Service Water System

IRWST: In Containment Reactor Water Storage tank

MSRT: Main Steam Relief Train

MSS: Main Steam System

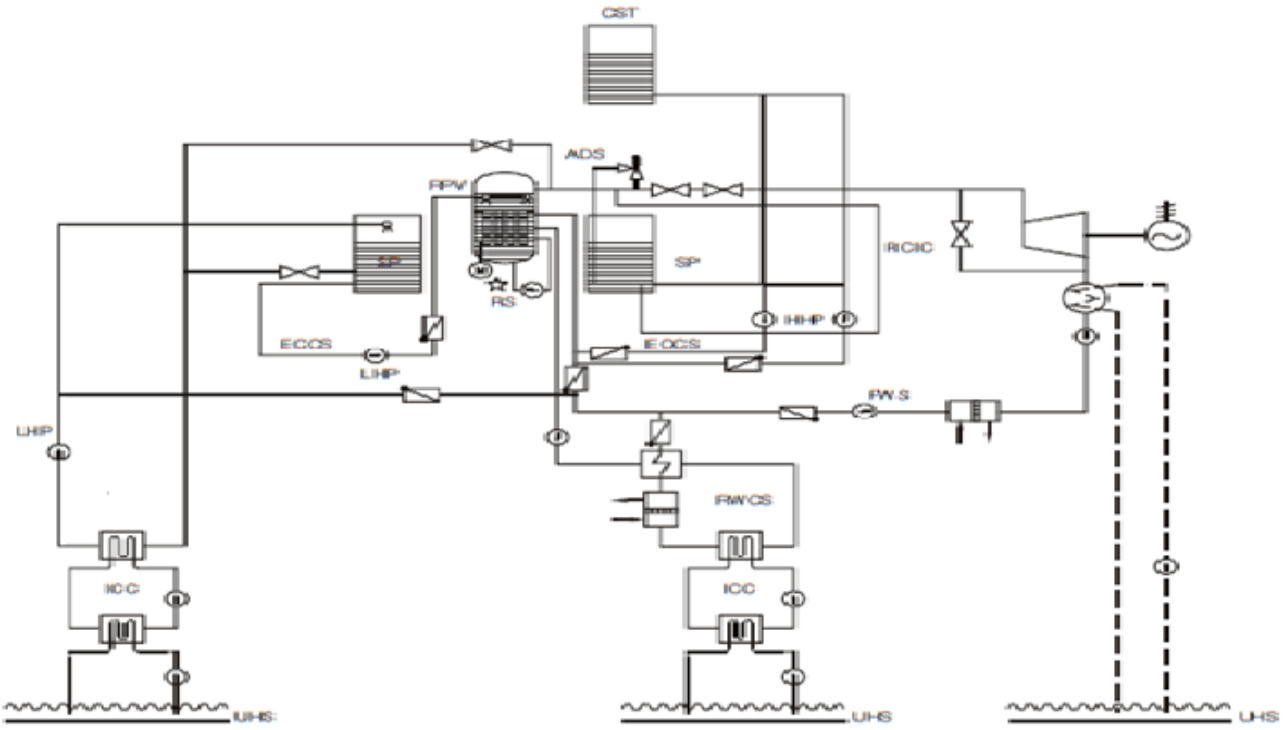
PRT: Pressurizer Relief Tank

RCS: Reactor Cooling System

RHRS: Reactor Heat Removal System

SIS: Safety Injection System

ANNEX II: BWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS



ADS: Component Cooling System

CST: Condensate Storage tank

ECCS: Emergency Core Cooling System

FWS: Feed Water System

HPP: High head Injection Pump

ICC: Intermediate Cooling Circuit

LHP: Low Head injection Pump

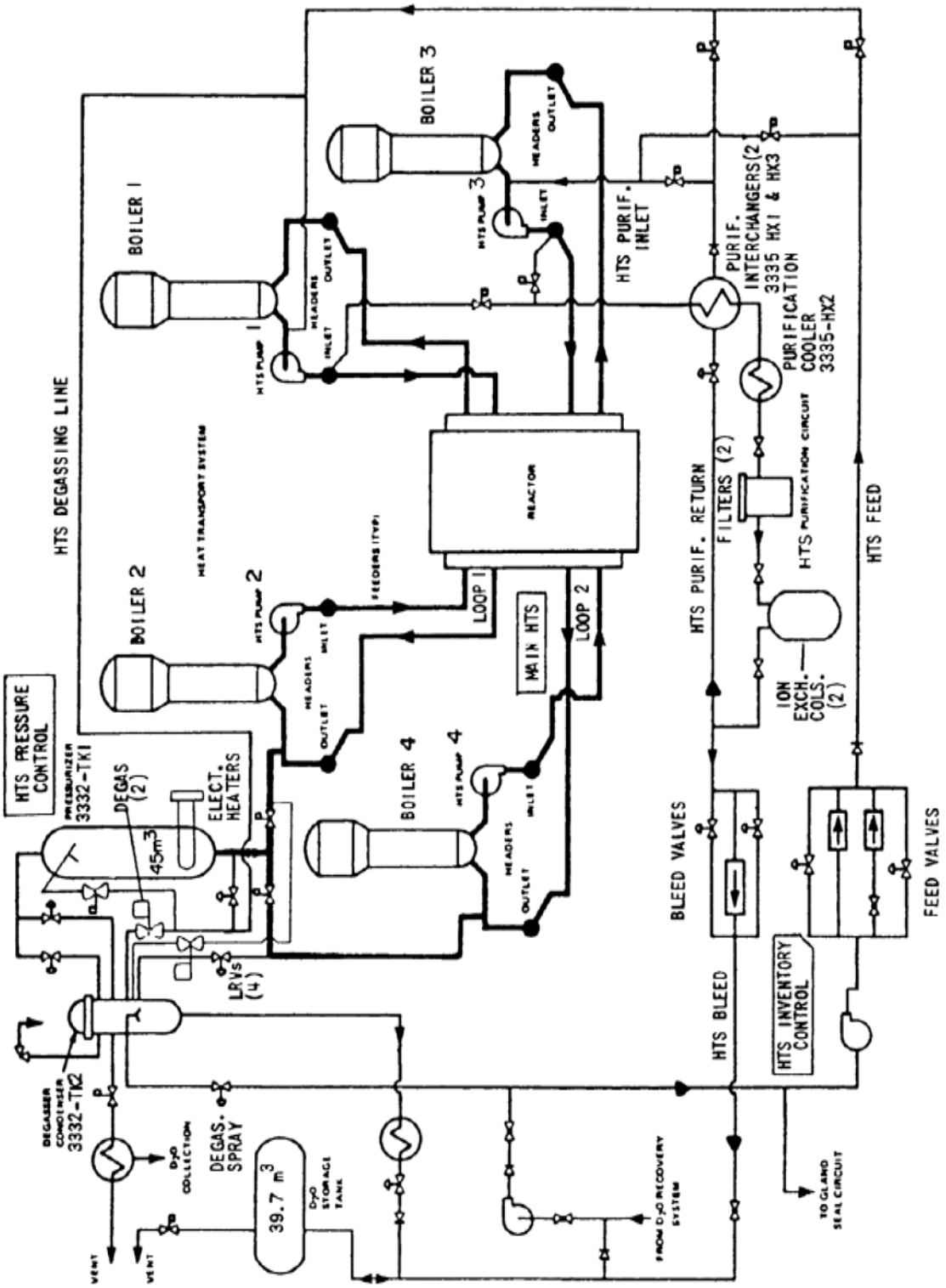
RCIC: Reactor Core Isolation Cooling

RPV: Reactor Pressure Vessel

SP: Suppression pool

UHS: Ultimate Heat Sink

ANNEX III: PHWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS



CONTRIBUTORS TO DRAFTING AND REVIEWS

3.1 Baik, S.J. KEPCO-E&C, South Korea

3.2 Beard, James GE- Hitachi Nuclear Energy Ltd, USA

3.3 Courtin, E. AREVA, France

3.4 Fil, N. Consultant, Russian Federation

3.5 Gasparini, M. Consultant. Italy

3.6 Jackson, C. US Nuclear Regulatory Commission, USA

3.7 Mesmous, N. Canadian Nuclear Safety Commission, Canada

3.8 Poulat, B. International Atomic Energy Agency

3.9 Taniguchi, Atsushi Tokyo Electric Power Company Holdings, inc.

3.10 Yamazaki, H. Toshiba Corporation, Japan

3.11 Yllera, J. International Atomic Energy Agency

3.12 Yoshikawa, K. Hitachi-GE Nuclear Energy Ltd, Japan