

IAEA SAFETY STANDARDS

for protecting people and the environment

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

Step 11c

2017-11-28

Draft DS 481

DRAFT SAFETY GUIDE

:

At the beginning of the drafting, decision was made to separately draft the design recommendations for the main three technologies (PWR, BWR and PHWR) .At the latest CS meeting, with the participation of one expert for every Reactor technology, we came to the conclusion that merging recommendations for the design of the Reactor Coolant System was achievable, but not for the associated systems which are clearly reactor technology dependent. This merging led to create a new section (section 5) specific to the design of the RCS with a set of common recommendations for the 3 technologies.

FOREWORD

[Click here and type the body of your report]

CONTENTS

1. INTRODUCTION	1
BACKGROUND	1
OBJECTIVE.....	1
SCOPE.....	1
STRUCTURE.....	2
2. EXTENT OF THE RCS AND ASSOCIATED SYSTEMS.....	2
REACTOR COOLANT SYSTEM	3
SYSTEMS FOR HEAT REMOVAL IN SHUTDOWN CONDITIONS	3
SYSTEMS FOR COOLANT INVENTORY CONTROL IN OPERATIONAL STATES.....	4
SYSTEMS FOR CORE REACTIVITY CONTROL IN OPERATIONAL STATES.....	4
SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS	4
SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS	4
ULTIMATE HEAT SINK AND RESIDUAL HEAT TRANSFER SYSTEMS IN ALL PLANT STATES	4
3. DESIGN BASIS OF RCS AND ASSOCIATED SYSTEMS	5
GENERAL	5
SAFETY FUNCTIONS.....	6
POSTULATED INITIATING EVENTS.....	6
INTERNAL HAZARDS	7
EXTERNAL HAZARDS	7
ACCIDENT CONDITIONS	9
DESIGN BASIS ACCIDENTS.....	10
DESIGN EXTENSION CONDITIONS (WITHOUT SIGNIFICANT FUEL DEGRADATION)	10
DESIGN LIMITS AND ACCEPTANCE CRITERIA	11
RELIABILITY	12
SYSTEMS DESIGNED TO COPE WITH DESIGN BASIS ACCIDENTS	12
SAFETY FEATURES TO COPE WITH DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT FUEL DEGRADATION.....	13
DEFENCE IN DEPTH	14
SAFETY CLASSIFICATION.....	14
ENVIRONMENTAL QUALIFICATION.....	15
LOADS AND LOAD COMBINATIONS.....	16
MATERIALS	18
MATERIALS IN CONTACT WITH RADIOACTIVE FLUIDS	19
MATERIAL EXPOSED TO HIGH NEUTRON FLUX.....	19
MANUFACTURING AND INSTALLATION	20
CALIBRATION, TESTING, MAINTENANCE, REPAIR, REPLACEMENT, INSPECTION AND MONITORING.....	20

SPECIFIC RECOMMENDATIONS FOR PRE SERVICE AND IN-SERVICE INSPECTION OF THE REACTOR COOLANT SYSTEM.....	21
PRE-SERVICE INSPECTION AND TESTING.....	21
IN SERVICE INSPECTION (ISI) AND TESTING.....	22
SPECIFIC RECOMMENDATIONS FOR INSPECTION OF THE STEAM GENERATORS:.....	22
OVERPRESSURE PROTECTION.....	22
LAYOUT.....	23
RADIATION PROTECTION.....	23
COMBUSTIBLE GAS ACCUMULATION IN NORMAL OPERATION.....	24
VENTING AND DRAINING.....	24
INTERFACE.....	24
CONTAINMENT ISOLATION.....	25
INSTRUMENTATION.....	25
MULTI UNITS AT THE SITE.....	26
CODES AND STANDARDS.....	26
USE OF PROBABILISTIC ANALYSES IN DESIGN.....	27
4. ULTIMATE HEAT SINK AND RESIDUAL HEAT TRANSFER SYSTEMS.....	27
ULTIMATE HEAT SINK.....	27
RESIDUAL HEAT TRANSFER SYSTEMS.....	30
RESIDUAL HEAT TRANSFER IN OPERATIONAL STATES.....	31
RESIDUAL HEAT TRANSFER IN CASE OF DESIGN BASIS ACCIDENTS.....	33
RESIDUAL HEAT TRANSFER IN CASE OF DESIGN EXTENSION CONDITIONS.....	33
5. SPECIFIC CONSIDERATIONS IN DESIGN OF THE REACTOR COOLANT SYSTEM.....	34
REACTOR COOLANT SYSTEM.....	34
STRUCTURAL DESIGN OF THE REACTOR COOLANT SYSTEM.....	35
DESIGN BASIS LOADS AND LOAD COMBINATIONS.....	36
CONTROL OF COOLING CONDITIONS IN OPERATIONAL STATES.....	37
ISOLATION OF THE REACTOR COOLANT PRESSURE BOUNDARY.....	40
POSTULATED INITIATING EVENTS.....	42
INTERNAL HAZARDS.....	42
EXTERNAL HAZARDS.....	42
LAYOUT.....	43
DESIGN LIMITS.....	43
SAFETY CLASSIFICATION.....	44
ENVIRONMENTAL QUALIFICATION.....	44
PRESSURE TESTS.....	45
VENTING.....	45
SPECIFIC DESIGN ASPECTS.....	46
6. SPECIFIC CONSIDERATIONS IN DESIGN OF THE ASSOCIATED SYSTEMS FOR PWR TECHNOLOGY.....	52

SYSTEMS FOR COOLANT INVENTORY AND CORE REACTIVITY CONTROL IN OPERATIONAL STATES.....	52
CONTROL OF THE COOLANT INVENTORY.....	53
CORE REACTIVITY CONTROL.....	53
SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES.....	54
HEAT REMOVAL IN POWER OPERATION AND HOT SHUT-DOWN MODES.....	54
RESIDUAL HEAT REMOVAL IN RHR MODE.....	55
SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS.....	57
CORE COOLING IN ACCIDENT CONDITIONS.....	58
RESIDUAL HEAT REMOVAL IN HOT SHUT-DOWN MODES FOR DESIGN BASIS ACCIDENTS.....	60
RESIDUAL HEAT REMOVAL IN THE LONG TERM OF DESIGN BASIS ACCIDENTS.....	62
RESIDUAL HEAT REMOVAL IN HOT SHUT-DOWN MODES FOR DESIGN EXTENSION CONDITIONS WITHOUT SIGNIFICANT CORE DEGRADATION.....	63
RCS FAST DEPRESSURIZATION IN DESIGN EXTENSION CONDITIONS WITH CORE MELTING.....	63
SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS.....	64
SPECIFIC DESIGN ASPECTS.....	65
7. SPECIFIC CONSIDERATIONS IN DESIGN OF THE ASSOCIATED SYSTEMS FOR BWR TECHNOLOGY.....	65
SYSTEMS FOR COOLANT INVENTORY AND CORE REACTIVITY CONTROL IN OPERATIONAL STATES.....	65
REACTOR WATER CLEAN-UP (RWCU).....	65
SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES.....	66
ISOLATION CONDENSERS (IF INCLUDED IN DESIGN).....	66
SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS.....	67
CORE COOLING IN CASE OF DESIGN BASIS ACCIDENTS.....	67
RESIDUAL HEAT REMOVAL IN CASE OF DESIGN BASIS ACCIDENTS.....	68
CORE COOLING IN CASE OF DESIGN EXTENSION CONDITIONS.....	68
RCS FAST DEPRESSURIZATION IN DESIGN EXTENSION CONDITIONS WITH CORE MELTING.....	69
SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS.....	69
8. SPECIFIC CONSIDERATIONS IN DESIGN OF THE ASOCOATED SYSTEMS OF PHWR TECHNOLOGY.....	69
SYSTEMS FOR REACTIVITY CONTROL IN OPERATIONAL STATES.....	70
SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES.....	70
SYSTEMS FOR REACTIVITY CONTROL IN ACCIDENT CONDITIONS.....	74
SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS.....	75
ENHANCED EMERGENCY HEAT REMOVAL SYSTEM.....	78
RECOMMENDATIONS FOR HEAT TRANSFER FOR DEC.....	81

PROVISIONS FOR FAST DEPRESSURIZATION OF THE PRIMARY HEAT TRANSPORT SYSTEM (CRASH COOL-DOWN).....	82
LIST OF ABBREVIATIONS	84
REFERENCES.....	86
ANNEX I: PWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS.....	89
ANNEX II: BWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS....	90
ANNEX III: PHWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS	91
CONTRIBUTORS TO DRAFTING	92

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 [1], 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. [1] 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. This Safety Guide covers the RCSASs, including the ultimate heat sinks as defined in Section 4. It covers design considerations for the RCSASs that are common for various reactor types, limited as mentioned in para. 1.5. The scope does not extend to the detailed design of specific components.

1.8. 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.

1.9. 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

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

1.11. 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 that apply to RCSASs.

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

1.13. Sections 5 provide supplementary design recommendations which are specific to the Reactor Coolant systems for Pressurized water reactor, boiling reactor and pressurized heavy water reactor technologies.

1.14. Sections 6, 7 and 8 provide supplementary design recommendations which are specific to associated systems for PWR, BWR and PHWR technologies, respectively.

1.15. Annexes I, II and III provide diagrams of the reactor coolant system and the 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:-

- RCS provides a confinement barrier for the protection of plant workers, the public and the environment from radioactive material;
- 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 significant fuel damage in design basis accidents and to mitigate the consequences of design extension conditions to the extent practicable;
- 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;
- Limit RCS over pressures in operational conditions, design basis accidents and design extension conditions without significant core degradation;
- 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 power operation (pressure, temperature and coolant flow rate). However fuel elements and control rods for controlling the core reactivity and shutting down the reactor are not addressed in this Safety Guide but in Ref. [1].

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 6). 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 7). Specific features of PHWRs are provided in section 8.

SYSTEMS FOR HEAT REMOVAL IN SHUTDOWN CONDITIONS

2.5. Those systems are systems designed to remove residual heat from the reactor coolant system during shutdown conditions. They include systems designed to cool down RCS to cold shut-down condition including refuelling condition after shutdown for PWR and BWR.

SYSTEMS FOR COOLANT INVENTORY CONTROL IN OPERATIONAL STATES

2.6. Those systems are systems designed to compensate for leakages and to control the reactor coolant inventory in operational states.

SYSTEMS FOR CORE REACTIVITY CONTROL IN OPERATIONAL STATES

2.7. Those systems are systems designed to accommodate slow reactivity changes (including control the core power distribution) in power operation and to control margins to re-criticality in shut-down conditions.

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 until 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, 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 until the safe shut-down conditions are reached in accident conditions.

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

2.10. Ultimate 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 heat from the residual 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 conditions.

3. DESIGN BASIS OF RCS AND ASSOCIATED SYSTEMS

3.1. This section describes generic design 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 6 for PWR, in Section 7 for BWR and in Section 8 for PHWR.

GENERAL

3.2. 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 general design requirements.

3.3. The design of RCSASs should be conducted taking into account the recommendations of GS-G-3.1 [19] and GS-G-3.5 [22] to meet the requirements 1 to 3 of SSR-2/1 Rev.1 [1] and the requirements of GSR Part 2 [2].

3.4. The design of RCSASs should be conducted taking into account design recommendations for nuclear safety and nuclear security in an integrated manner in such way that nuclear safety and nuclear security measures do not compromise each other. Recommendations for nuclear security are detailed in [3].

3.5. RCSASs are required to be designed in compliance with requirements 47 to 53 of SSR-2/1 (Rev.1) [1], with account taken of all other requirements of SSR-2/1 (Rev.1) [1] 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;
- Practical elimination of early radioactive releases or large radioactive releases.

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

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

- The s function(s) to be performed by the structure, system or component;

- The postulated initiating events they have to cope with;
- loads and load combinations that the structure or component must withstand.
- The protection against the effects of internal hazards;
- The protection against the effects of external hazards;
- Design limits and acceptance criteria (applicable to the design of systems, structures and components)
- Reliability
- Provisions against common cause failures within a system and between systems belonging to different levels of defence in depth;
- The safety classification;
- Environmental conditions for qualification
- Monitoring and control capabilities;
- Materials;
- Provisions for testing, inspection, maintenance and decommissioning.

SAFETY FUNCTIONS

3.8. 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

3.9. Paragraphs 3.10 and 3.12 provide recommendations on meeting Requirement 16 of SSR-2/1 (Rev. 1) [1].

3.10. 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 on the basis of their estimated frequency of occurrence¹.

3.11. For each of the conditions caused by PIEs, the list of RCSASs necessary to bring the plant to safe and stable shut-down condition should be established.

¹ TECDOC 1791 provides recommendation for PIEs categorization

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

INTERNAL HAZARDS

3.13. Paragraphs 3.14–3.17 provide recommendations on meeting Requirements 17 and para.5.16 of SSR-2/1 (Rev. 1) [1] in relation to internal hazards. Recommendations provided in the draft Guide DS 494, Protection against Internal Hazards in the Design of Nuclear Power Plants [6] should be used to identify internal hazards to be considered in design RCSAS activities. .

3.14. The screening process used for identifying internal hazards should be documented in accordance with a management system process. SSCs important to safety 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 effects of the failures of non-protected SSCs on protected SSCs.

3.15. Layout and protection should be adequate to ensure that the response of the systems, as described in the analysis of the postulated initiating events, remains valid even considering the effects of the hazard.

3.16. Layout and protection of the redundancies 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.

3.17. Methods, design and construction codes and standards used should provide adequate margins to justify that cliff edge effects would be avoided in the event of an increase of the severity of the internal hazards.

EXTERNAL HAZARDS

3.18. Paragraphs 3.19–3.26 provide recommendations ~~on meeting~~ on meeting Requirement 17 and the paragraphs 5.17-5.21A of SSR-2/1 (Rev. 1) [1] in relation to external hazards. Recommendations provided in IAEA Safety Standards Series No. NS-G-1.5 [4], External Events Excluding Earthquakes in the Design of Nuclear Power Plants should also 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.

3.19. With regard to the effects of external hazards, protection should be applied to the extent possible to prevent damage to RCSASs important to safety (eg. systems to shut down the reactor and to mitigate consequences of accident conditions). Protection can rely on an adequate layout and protection measures of the buildings at the site. When protection measures are not effective, SSCs should be designed to withstand the hazard loads and their combinations.

3.20. 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 initiator of an accident.

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

3.22. Structures, systems and components of the RCSASs should be assigned to appropriate seismic categories in accordance with the recommendations and guidance given in *Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6* [5]. Components forming the RCPB, the secondary envelope of the steam generators (PWR and PHWR), and safety systems designed to mitigate the DBAs should be designed to withstand SL2 seismic loads.

3.23. 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.

3.24. RCSASs, structures and components ultimately necessary to prevent an early radioactive release or a large radioactive release (if any) should be identified. Integrity and operability (where relevant) of those items should be preserved in case of natural hazards causing loads exceeding those resulting from the site hazard evaluation. Boundary conditions for the design or assessment should be justified.

3.25. 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 systems available at the site (see Requirement 5.17 of SSR-2/1 (Rev. 1) [1]).

3.26. Capability for adequate core cooling should be such as to remain operational for longer than the time necessary prior to crediting off-site support services.

ACCIDENT CONDITIONS

3.27. 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.

3.28. 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);
- Reactor coolant leakages to the secondary side (PWR and PHWR);
- Main steam/SG feed water piping break (PWR and PHWR);
- Loss of residual heat removal in shutdown conditions;
- Reactivity and power distribution anomalies;

3.29. Paragraphs 3.30–3.32 provide recommendations on meeting Requirement 18 of SSR-2/1 (Rev. 1) [1].

3.30. Computer 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 management system. Users of the codes should be qualified and trained with respect to the domain of validation and application and to the assumptions made in the models of the codes.

3.31. 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.

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

Design basis accidents

3.33. Paragraphs 3.34–3.35 provide recommendations on meeting Requirements 19 and 25 of SSR-2/1 (Rev. 1) [1].

3.34. Design basis accident (DBA) conditions should be identified and calculated for the RCS in order to specify adequate performance of the safety systems.

3.35. 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 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)

3.36. Paragraphs 3.37–3.42 provide recommendations on meeting Requirement 20 of SSR-2/1 (Rev. 1) [1] [for conditions without core melting](#).

3.37. Relevant design extension conditions should be identified on the basis of engineering judgement as well as deterministic and probabilistic assessment.

3.38. As typical examples, the following three types of DECAs should be considered:

- Very unlikely events² 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.

3.39. 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

² The exceedance frequencies of a design basis defined for a safety system should be low.

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 sink should be conducted to identify relevant candidates for DEC.

3.40. Design extension conditions without significant fuel degradation 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. Examples of DEC that may apply include:

- 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.

3.41. For the performances of the RCSAs necessary in DEC, design extension conditions may be calculated with less conservative rules 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 which key parameters present uncertainties to be considered in design.

3.42. Mitigation of design extension conditions (DEC) should be accomplished by permanent systems to the extent possible. Short term actions should be implemented by permanent equipment.

DESIGN LIMITS AND ACCEPTANCE CRITERIA

3.43. Paragraphs 3.44–3.45 provide recommendations on meeting Requirements 15 and 28 of SSR-2/1 (Rev. 1) [1].

3.44. The performance of RCSAs should be defined and specified to fulfil a well-defined and accepted³ 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;

³ ‘Well defined and accepted’ generally means either widely accepted by Member State regulatory bodies or proposed by international organizations.

- 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.

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

RELIABILITY

3.46. The Paragraphs 3.47–3.56 provide recommendations on meeting Requirements 21, 22, 23, 24, 25, 26, 29 and 30 of SSR-2/1 (Rev. 1) [1].

3.47. The following factors should be considered to achieve the adequate reliability of the RCSAS necessary to control reactivity of the core, to maintain sufficient inventory in the reactor coolant system, to remove residual heat from the core 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;
- Aging,
- Maintenance;
- Use of equipment designed for fail-safe behavior.

Systems designed to cope with design basis accidents

3.48. 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.

3.49. 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 (either active or a passive failure, see SSR2/1 Rev.1, para. 5.40). If duly justified, some component failures could not be postulated (e.g. some passive failures if justified)

3.50. The on-site power source (Emergency Diesel Generator and/or batteries) 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 to the ultimate heat sink and maintaining the reactor in a safe state in the long term [7].

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

3.52. Recommendations related to the reliability of the system with regard to the effects of internal, external hazards and environmental conditions are addressed in paras 3.14–3.17, 3.19–3.26 and 3.78–3.75, respectively.

Safety features to cope with design extension conditions without significant fuel degradation

3.53. 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.

3.54. The more likely combinations of PIEs and common cause failure (CCF) between the redundancies of the safety systems should be analysed. 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 such events from escalating to accident with core melting. The additional features for residual heat removal and heat transfer to the ultimate heat sink should be designed and installed such that they should be unlikely to fail for the same cause.

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

3.56. Recommendations indicated in the paragraphs 3.48 - 3.52 should be applied, taking into account that meeting the single failure criterion is not required and that additional safety features for DEC are supplied by the Alternate AC power source. and batteries.

DEFENCE IN DEPTH

3.57. Paragraphs 3.58–3.61 provide recommendations on meeting Requirement 7 of SSR-2/1 (Rev. 1) [1].

3.58. Alternative means to shut down the reactor or to maintain sub criticality, or to accomplish residual heat removal and heat transfer to the ultimate heat sink in the different plant states should be implemented within the defence in depth approach.

3.59. Vulnerabilities for CCF between those means 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.

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

3.61. Instrumentation for actuation of RCSAS designed as safety systems and for monitoring of plant status should be independent to the extent practical.

SAFETY CLASSIFICATION

3.62. Paragraphs 3.63–66 provide recommendations on meeting Requirement 22 of SSR-2/1 (Rev. 1) [1]. Detailed recommendations provided in Safety Guide SSG-30 [8] should also be considered.

3.63. Consequences of a SSC failure should be considered both on the accomplishment of the function, and on the level of the radioactive release. For SSCs 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 SSCs 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.

3.64. The classification should be established in a consistent manner such that all systems necessary for the accomplishment of one safety function including the associated support service systems are assigned in the same class, or justification should be provided.

3.65. In accordance with Requirement 9 of SSR-2/1 (Rev. 1) [1], pressure retaining equipment that is safety classified is required to be designed and manufactured in accordance with proven codes and standards widely used by the nuclear industry (see, for example, Refs. [15-17]). The engineering design and manufacturing rules applicable to each individual component should be

selected with due account taken of the two effects resulting from its failure in terms of function not accomplished and radioactive release.

3.66. With regard to implementing the following recommendations, and in terms of the safety classification described in SSG-30 [8]:

- Systems designed not to exceed the dose limits accepted in the event of a design basis accident should be assigned in 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 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 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.

ENVIRONMENTAL QUALIFICATION

3.67. Paragraphs 3.68–3.75 provide recommendations on meeting Requirement 30 of SSR-2/1 (Rev. 1) [1]. Detailed recommendations provided in *Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants*, IAEA Safety Standard Series DS 485 [10] should also be considered.

3.68. 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.

3.69. The relevant environmental conditions that may prevail prior to, during and following an accident, the ageing of structures, systems and components throughout the lifetime of the plant should all be taken into consideration in the environmental qualification [10].

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

3.71. Environmental qualification should include the consideration of such factors as temperature, pressure, humidity, radiation levels. 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.

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

3.73. For components subject to the effects of ageing degradation 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 relevant accident conditions for their use.

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

3.75. Evidence of environmental qualification, the applicable parameters and the established qualification needs should be contained in or referenced by applicable design documentation in an auditable form for the lifetime of the plant.

LOADS AND LOAD COMBINATIONS

3.76. The design basis of each component and structure of the RCSASs should include, for each plant state and service condition, the loads and load combinations imposed by the construction, lifting, operational states and accident conditions, environmental conditions inside the buildings, internal and external hazards for which stability, integrity, functionality and operability is required.

3.77. Loading conditions, loads and stresses should be calculated applying adequate accepted methodologies and rules to establish confidence in the robustness of the design, and to provide adequate 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;

3.78. 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 coincidentally).

3.79. Design basis loading conditions, including internal and external hazard loads, should be assigned in different categories in accordance with plants states and/or service conditions (e.g. normal conditions, upset conditions, emergency conditions, faulted conditions) according to their estimated frequency of occurrence⁴ or according to requirements of accepted codes and regulations.

3.80. Appropriate acceptance criteria (e.g. design pressure and temperature, stress limits) to be met for ensuring integrity should be defined and be appropriate to each load combination with account taken of the load combination category.

3.81. The stress levels may be different for the different modes of failure (e.g. progressive deformation and fatigue or excessive deformation and plastic instability). Protection against brittle fracture should be ensured, and the critical buckling stress should be considered if relevant for the component.

Meeting the criteria given by internationally recognized codes and standards provides reasonable assurance that structures and components are capable of performing their intended functions. When operability needs to be demonstrated, additional analyses or tests should be conducted..

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

3.83. 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).

⁴ • Normal service conditions: loading conditions to which the equipment may be subjected during 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

3.84. 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.

3.85. SSCs designed to accomplish their functions in plant conditions categorized as “emergency conditions” or “faulted conditions” should be designed to meet adequate⁵ 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

3.86. Paragraphs 3.87–3.91 provide recommendations on meeting Requirement 47 of SSR-2/1 (Rev. 1) [1].

3.87. The materials used for the pressure retaining boundary of the RCSASs should be specified with regard to chemical composition, microstructure, mechanical/thermal properties, heat treatment, and manufacturing requirements and activation of materials, as applicable. The materials should be homogeneous and 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.

3.88. The specifications on welding materials used for manufacturing or repair of components also should be established so that the welds have sufficient strength and toughness.

3.89. 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 including resistance to stress corrosion cracking;
- Resistance to effects of irradiation;
- Resistance to thermal embrittlement;
- Resistance to hydrogen embrittlement;

⁵ Meeting the stress limit proposed by codes for emergency or faulted conditions is generally not considered as adequate by Regulatory Bodies.

- Ductility characteristics;
- Fracture toughness characteristics (including both brittle and ductile);
- Ease of fabrication (including weldability).

3.90. Sensitivity of the used materials for activation under neutron irradiation should be minimized to the extent practical.

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

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

3.93. Materials used should enable efficient decontamination.

Material exposed to high neutron flux

3.94. The materials used in this application should take into consideration:

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

3.95. With regard to the risk of embrittlement of the RPV, a surveillance programme should be established on the basis of tests conducted on samples of materials used for the RPV manufacturing. These samples are installed in the RPV and removed on a scheduled basis. These samples when removed are subject to mechanical testing, including tensile strength and charpy impact or fracture toughness testing.

Other samples are analysed to measure the irradiation fluence that the RPV wall and the samples are being exposed to.

Acceptance criteria should be specified for all the tests performed.

MANUFACTURING AND INSTALLATION

3.96. Paragraph 3.97 provides recommendation on meeting Requirement 11 of SSR-2/1 (Rev. 1) [1].

3.97. Pressure retaining components, should be manufactured and installed in accordance with established processes that ensure the achievement of the design specifications. The management system should be established for manufacturing process including identification and traceability of materials, welding, handling, and storage of manufactured components. More detailed recommendations are provided by the codes and standards selected for the manufacturing.

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

3.98. Paragraphs 3.99–3.114 provide recommendations on meeting Requirement 29 of SSR-2/1 (Rev. 1) [1].

3.99. Provisions are required to be taken to ensure that SSCs important to safety will keep their capability to perform their intended function as designed over their lifetime. Inspection and or periodic testing are good practices to meet this requirement.

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

3.101. The design should incorporate provisions to facilitate examination, testing, in service inspection, maintenance, repair and modifications to be carried out during the construction, commissioning and operation phases [11].

3.102. 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.

3.103. The development of strategies and programs to address examination, testing, in-service inspection, maintenance and monitoring is a necessary aspect of RCSAS design. The strategies and programs to be implemented should take into account Human Factors Engineering criteria in order to facilitate efficient conduct of activities and minimize the contribution of human error.

3.104. 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.

3.105. Non-destructive examination should be defined and conducted on welds and weld claddings to ensure their acceptability for structural integrity, on the basis of pre-defined acceptance criteria for each type of non-destructive method. The personnel, equipment and procedures should be qualified prior to performing the non-destructive examination.

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

3.106. The components of the RCPB should be designed, manufactured and installed in a manner that permits adequate inspections and tests of the boundary, support structures and components throughout the lifetime of the plant.

3.107. The design should allow access to any part of the RCS that has to be inspected during the plant life time, in particular welds. Specific areas subject to cyclic loads and neutron irradiation should be identified at design stage and specifically monitored in order to confirm that no damage occurs due to ageing effects, thermal fatigue and neutron irradiation.

3.108. Methods and criteria provided by relevant national and international codes and standards may be used for Pre service inspection and for in service inspection.

Pre-service inspection and testing

3.109. Prior to the start of operation, a Pre-Service-Inspection (PSI) program should be developed and performed.

3.110. The RPV and RCPB should be subject to examinations, inspections and 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 RCPB welds and other representative areas 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 inspection results;
- Hydrostatic test (according to design and manufacturing code) of the RPV and RCS once installation is complete;
- 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 such cases, adequate provisions should be made for the inspection of those areas to the extent reasonably practicable.

In service inspection (ISI) and testing

3.111. The RPV and RCPB should permit volumetric examination of the entire volume of the welds as well as surface examination. For example, ultrasonic, eddy current or magnetic flux methods could be used for such examinations.

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

3.113. The following issues should be considered in deriving the inspection criteria:

- The minimum detectable indication in non-destructive examinations;
- The expected crack growth and fracture toughness in operational states and in accident conditions;
- Sourcing of RPV welded and base metal coupons representing relevant inspection areas of the RPV and other major components subject to recurrent ultrasonic testing (e.g. welded joints and base metal with cladding, bimetallic welds, nozzle areas) should be stored to produce 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;
- All controls during manufacturing process should be referenced and traceable for the operational lifetime;

Specific recommendations for inspection of the steam generators:

3.114. 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

3.115. Paragraphs 3.116–3.119 provide recommendations on meeting Requirement 48 of SSR-2/1 (Rev. 1) [1].

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

3.117. Over pressure protection devices should be installed as close as practicable to the component to be protected.

3.118. The discharge capacity should be sufficient to limit the pressure such that the stress limits for the service condition are met for each of the components of the system to be protected.

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

LAYOUT

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

- Radiological protection of site personnel;
- Protection against the consequences of pipe failure; (depressurization wave, 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 seismic events,
- Provisions to minimize stresses in the piping also considering thermal expansion;
- Provisions to facilitate testing, inspection, repair and replacement.

RADIATION PROTECTION

3.121. Paragraphs 3.122–3.125 provide recommendations on meeting Requirement 81 of SSR-2/1 (Rev. 1) [1]. Detailed recommendations for design measures for radiological protection are given in Ref. [12] should also be considered.

3.122. The design of the layout of RCSASs should allow for the inspection, maintenance, repair and replacement of components in consideration of ALARA principle.

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

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

3.125. Content of cobalt, antimony, silver and other easily activated nuclides 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 nuclides like cobalt 60, antimony 124, and silver 110.

COMBUSTIBLE GAS ACCUMULATION IN NORMAL OPERATION

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

VENTING AND DRAINING

3.127. Provision should be made for venting and draining RCSASs.

3.128. Provisions should also be implemented for collecting and managing inventories from leakages during normal operation. Leakages can occur from, among others, valve stems, valve seats, pump seals and gaskets during reactor operation.

INTERFACE

3.129. Appropriate isolation devices should be provided for connections between systems or components belonging to different safety classes [8]. These devices should prevent situation where failure of a system or a 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. The isolation device should have the same safety classification as the system or component with the higher safety classification to which it is connected.

3.130. Structures interfacing with the RCSASs should be considered as SSCs important to safety and should be designed accordingly in order not to affect their integrity and performances. Such structures include:

- Snubbers and their anchors;
- Pipe whip restraints;
- Building penetrations;
- Protective structures (e.g. barriers, shields, etc).;

CONTAINMENT ISOLATION

3.131. Paragraph 3.132 provides recommendations on meeting Requirement 56 of SSR-2/1 (Rev. 1) [1].

3.132. Piping that penetrates the primary containment wall(s) should be provided with adequate isolation devices and the piping run between isolation valves should be designed according to [13].

INSTRUMENTATION

3.133. 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 main control room and the technical support center with appropriate and reliable information for the accident management.
- Periodic testing of systems and components;
- Supporting an understanding of maintenance state of SSCs.

3.134. Consequences of sharing of sensors for different purposes should be assessed in order to preserve adequate independence of the different levels of defence in depth. The 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.

3.135. Instrument sensing lines should be designed such that characteristics of measurement (e.g. magnitude, frequency, response time, chemical characteristics) are not distorted.

3.136. Potential leakage of radioactive materials into RCSASs should be monitored [14].

MULTI UNITS AT THE SITE

3.137. As stated in Requirement 33 of SSR-2/1 (Rev. 1) [1]:

“Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.”

CODES AND STANDARDS

3.138. Paragraphs 3.140–3.141 provide recommendations on meeting Requirement 9 of SSR-2/1 (Rev. 1) [1].

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

3.140. Codes and standards have been developed by various national and international organizations, covering areas such as:

- Materials;
- Manufacturing (e.g. welding) and construction;
- Civil structures;
- Pressure vessels and pipes;
- Instrumentation and control;
- Environmental and seismic qualification;
- Pre-service and in-service inspection and testing;
- Management system;
- Fire protection.

USE OF PROBABILISTIC ANALYSES IN DESIGN

3.141. Paragraphs 3.1413-3.144 provides recommendations on meeting Requirement 5.76 of SSR-2/1 (Rev. 1) [1].

3.142. 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 DEC's.

3.143. 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

4.1. This section addresses guidance and the main recommendations for the design of the systems designed to transfer residual heat from the different decay heat removal systems to the Ultimate heat sink (UHS) on meeting the Requirement 53 of SSR-2/1 (Rev. 1) [1].

ULTIMATE HEAT SINK

4.2. UHS is defined as the medium into which residual heat is discharged in the different plant states after shut down of the reactor, and it normally takes one or both of a large body of water or the atmosphere. The body of water can be the sea, a river, a lake, a reservoir, ground water or combinations of these, but in general, access to natural, inexhaustible supplies of water is preferable to limited capacities. For UHS relying on the atmosphere, cooling towers or spray ponds with their associated structures and systems are usual equipment designed to transfer heat to the atmosphere. Some passive reactor plant designs also rely more exclusively on the atmosphere for dissipating reactor decay heat immediately following plant transients and accident conditions. The medium used as a recipient for the decay heat can also be used as a source of cooling for turbine condensers during power operation but the associated transport systems are out of scope of this Safety Guide.

4.3. For a site with multiple units, equipment important to safety designed as interfaces with UHS medium should be specific to each unit.

4.4. UHS capacity should be adequate to absorb decay heat from the different reactors and spent fuel pools at the site. This capacity should be designed considering that several or even all units could be in accident conditions simultaneously.

4.5. UHS reliability and capacity should be ensured for the short and long term taking into account all the relevant heat loads generated during normal shutdown modes, AOOs and accident conditions, the rates of heat rejection during those conditions and relevant regulations pertaining to environmental protection.

4.6. Short and long term capacity of the UHS should be preferably achieved by the use of the inexhaustible natural bodies of water, or the atmosphere. Where access to an inexhaustible supply of water or the atmosphere at the site is not available:

- UHS capacity should be ensured by an adequate amount of water always available at the site. This capacity should be adequate to absorb all heat loads generated at the site until the heat sink can be replenished⁶. In such a demonstration account should be taken of factors that could delay the replenishment process. Such factors include evaporation, human induced events, natural hazards, plant accident conditions, availability of interconnections and the complexity of the procedures for replenishment.
- A minimum amount of water, including a margin for uncertainties should be immediately available to bring reactors to the safe shutdown state in the event of any PIEs. For each unit, this minimum quantity⁷ should be already stored in the basins of the cooling towers/ spray ponds dedicated to the unit.
- -Beyond this minimum capacity the amount of water required prior to replenishment could be stored in on site reservoir with a possibility to transfer this water from on-site reservoir to UHS. This transfer system should be considered as a support system to achieve the required safety function of UHS and should be safety classified accordingly.
- For long term capacity of the UHS the make-up systems to provide replenishment of on-site reservoirs should be permanently installed and should be designed with an adequate rate for the long term heat removal capacity.

4.7. To fulfil the design objectives in terms of capacity and reliability and to comply with the Defence in depth concept (Requirement 53, item 6.19A), different UHS and different accesses to the UHS may be necessary.

4.8. Structures associated to UHS should be designed to withstand the loads caused by the site hazards derived from the site hazard evaluation. Recommendations and guidance on the consideration of external events in the design of the structures (extreme temperatures and

⁶ The minimum capacity should not be less than 7 days, in some States the acceptable capacity of water is 30 days.

⁷ In some States the acceptable minimum capacity of water is 3 days.

conditions, floods, tsunamis, high winds, biological phenomena, collision with floating bodies, etc.) are provided in [4].

4.9. 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.

4.10. In determining the necessary capacity of the UHS, design basis environmental parameters should be defined with consideration of time periods during which those conditions are assumed to exist Ref. [4].

4.11. The effectiveness of the ultimate heat sink should not be over sensitive to short term variations of the environmental parameters.

4.12. These parameters should 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.

4.13. Capability for heat loads rejection should be assured following any interruption of power generation or loss of operability of normal heat removal systems.

4.14. UHS capability should be designed for absorbing the relevant heat loads at the maximum peak heat rejection rate for the different plant states with consideration of the time dependent behaviour of the individual heat loads.

4.15. 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.

4.16. 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:

- Residual heat of the reactor coolant system(s);
- Decay heat of the spent fuel with the storage(s) at maximum capacity;
- Heat generated by the operation of SSCs important to safety to achieve and maintain a safe plant shut down, or to mitigate -accident conditions. (if heat produced by components is transported by the residual heat transfer chain);

- Heat from other accident related heat sources (e.g. chemical reactions).

4.17. In establishing the residual heat loads of the reactor (including decay heat, heat due to shut-down fission and energy stored in RCS and other operated heat removal systems or structures), 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.

4.18. 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.

4.19. 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 TRANSFER SYSTEMS

4.20. 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 from residual heat removal 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.

Paragraphs 4.21–4.26 provide recommendations on meeting Requirements 7 and 53 of SSR-2/1 (Rev. 1) [1].

4.21. All residual heat sources at the nuclear power plant should be considered for the design of the heat transfer systems⁸.

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

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

4.23. 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 on the heat transfer chain.

4.24. To ensure effectiveness of the defence in depth strategy the different means provided should be independent to the extent practicable, in particular a different and independent heat transfer chain should be implemented for accidents with core melting [13].

4.25. Heat transfer chain(s) and its various systems and components should be designed and manufactured applying the design recommendations derived from its safety classification established on the basis of its safety significance.

4.26. 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

4.27. Paragraphs 4.28–4.39 provide recommendations on meeting the Requirement 51 of SSR-2/1 (Rev. 1) [1] and supplement the generic recommendations indicated in section 3.

4.28. 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.

4.29. Heat transfer should be tolerant to one failure postulated at any component necessary for transferring residual heat to the ultimate heat sink.

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

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

4.32. 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.

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

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

4.35. 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 case of DBAs). In that case, a failure on equipment operated only during operational states -should not propagate to equipment required to operate during design basis accident conditions.

Specific Design aspects

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

4.37. The intermediate cooling system should be protected against over pressure caused by leakages occurring in 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 leakages outside of the containment.

4.38. 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 or foreign parts.

4.39. 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

4.40. 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.

4.41. 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.

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

4.43. The heat transfer chain should have capabilities designed to simultaneously 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.

Residual heat transfer in case of design extension conditions

4.44. Conditions requiring additional needs (safety features for DEC) 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).

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 THE REACTOR COOLANT SYSTEM

REACTOR COOLANT SYSTEM

5.1. 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 (PWR and PHWR or directly to the turbine generator). 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. The RCS includes the reactor pressure vessel, the pressurizer (PWR and PHWR), piping and pumps for the circulation of the coolant and the steam generators for (PWR and PHWR).

For PHWR technology:

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 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.

Structural design of the reactor coolant system

5.2. Paragraphs 5.3–5.14 provide recommendations on meeting the Requirement 47 of SSR-2/1 (Rev. 1) [1].

5.3. Technical specifications should be established for the design and manufacturing of the Reactor Coolant Pressure Boundary (RCPB), and of the Secondary Side Pressure Boundary (SSPB) for PWR and PHWR, in order to achieve a high reliability of those components. Those specifications should be established in accordance with the latest edition of proven codes and standards taking into consideration of regulatory requirements and available experience, and should include specifications for :

- An analysis of the relevant potential damage modes and a selection of appropriate materials having proven structural characteristics;
- A comprehensive identification of loads and load combinations and appropriate margins regarding the failure criteria;
- Manufacturing and inspection or controls on the basis of proven and qualified industrial practices;
- An in-service inspection programme proving that the original quality of equipment is maintained during its lifetime, in particular that cracks or defects of significance to safety do not exist.

5.4. High confidence in the design and manufacturing of the large components of RCS should be provided to justify their failure may not be retained as a PIE for the plant design (consequences of such failure cannot be reasonably mitigated).

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

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

5.6. 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 corrosion, stratification, aging, etc.).

5.7. 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 fuel degradation.

5.8. The 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 occurrences should be assigned to each of them according to the usage factor assessment of each component.

5.9. 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.

Design basis loads and load combinations

5.10. Structural design of the Reactor Coolant Pressure Boundary, and also the Secondary Side Pressure Boundary for PWR and PHWR, should be established on the basis of a limited number of loads and load combinations defined as envelopes of loads to which the equipment could be subjected over its lifetime taking into account the normal plant operation, conditions caused by the postulated plant events, and the site hazards considered in the design basis of the equipment. At low operating temperature the ductility and fracture resistance of some materials may be significantly lower. Where such materials are used for 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 (e.g. the over pressure protection system) should be implemented to prevent the risk of brittle fracture of the component, taking into account the specified ranges of pressure and temperature established for the plant normal operation.

5.11. Stresses caused by normal service and upset conditions should be less than the stress limits specified for those loading conditions categories. The design temperature should not be exceeded, and a good practice is not to exceed the design pressure. The cumulative usage factor should be less than 1.

5.12. 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 in magnitude and time (e.g. does not exceed 110% of the design pressure).

5.13. 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. (e.g. should not exceed 130% of the design pressure).

5.14. The thermal hydraulic conditions in the RCS should be monitored throughout the plant life time in order to identify and record the situations that may cause fatigue to RCS equipment. This monitoring should prove that the number of occurrences allowed for each plant situation is not exceeded during the plant life time, as specified in 5.8, and there is minimal risk of cracking induced by fatigue.

Control of cooling conditions in operational states

5.15. Paragraphs 5.16–5.17 provide recommendations on meeting the Requirement 49 of SSR-2/1 (Rev. 1) [1].

5.16. Design provisions should be implemented for monitoring, display and control of the key RCS parameters (RCS pressure and temperature, RCS water inventory, steam and feed water flow (for BWR), SG pressure and water levels (for PWR and PHWR), 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.

5.17. SSCs to maintain adequate cooling conditions of the fuel should be classified SSCs important to safety and be designed and manufactured accordingly (see section 3, safety classification).

Pressure control and overpressure protection

5.18. Provisions and design recommendations given by paragraphs 5.19–5.25 should be considered for the design of the pressure control of the Reactor Coolant System and for the Secondary Side (for PWR and PHWR).

5.19. 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.

5.20. The diversity principle should be applied in the design between the pressure control system and the over pressure protection system to reduce the likelihood of common cause failures.

5.21. If the pressurizer can be isolated from the RCS in certain operating conditions (i.e. PHWR 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.

5.22. Systems intended for the control of pressure should be designed to prevent, in normal operation and AOOs, the operation of the safety valves (respectively safety relief valves for BWR). The release of primary coolant should be minimized and not discharged into the containment.

5.23. Setting and system performances of systems designed to control operational conditions should be determined on the basis of realistic response of the plant.

5.24. 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 (for PWR and PHWR).

5.25. Pressure control in RCS and Secondary Side circuit (for PWR and PHWR) should be ensured even in the event of a loss of off-site power.

5.26. Paragraphs 5.27–5.39 provide recommendations on meeting the Requirement 48 of SSR-2/1 (Rev. 1) [1], but also apply to the over pressure protection system of the Secondary Side for PWR and PHWR.

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

5.28. An overpressure protection system should be implemented to preserve the structural integrity of the Reactor coolant pressure 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.

5.29. For PWR/PHWR, an overpressure protection system should be implemented to preserve the structural integrity of the SSPB 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.

5.30. The discharge capacity of the overpressure protection system 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 at least fails to open (or more for systems with more safety valves). This independent failure may not be considered in the analysis of over pressure transients initiated by multiple failures
- Loss of the off-site power is combined if it can aggravate the consequences of the initiating event.

5.31. The over pressure protection devices should be designed in such a way to keep the water hammer effects as low as possible.

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

5.33. No shut-off valves should be placed in the discharge line of a safety valve (safety relief valves for BWR), nor between the item being protected and a safety valve (safety relief valves for BWR). When a relief valve is used for pressure control, its reliable closing should be secured by means of a relief line shut-off valve.

5.34. The safety valve, safety relief valves and relief valves should be provided with a position indicator that is independent of the control equipment.

5.35. The outlet of the SRVs should be instrumented in order to detect leakages.

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

5.37. The valves used for the overpressure protection and the associated piping should be designed to discharge steam as well as a steam-water mixture and water.

5.38. Spurious opening of a safety valve (safety relief valve for BWR) should be prevented and its frequency should not be higher than the frequency considered for loss of coolant accidents.

5.39. Components that can increase pressure in the primary circuit (e.g. pressurizer heaters or make up pumps for PWR and PHWR) should be equipped with a system that stops the operation of the component to prevent inadvertent pressure increase.

5.40. Paragraph 5.41 provides recommendations on meeting the Requirement 20 of SSR-2/1 (Rev. 1)[1].

5.41. 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, if relevant.

Isolation of the Reactor Coolant Pressure Boundary

5.42. RCPB comprises pressure retaining components of the RCS that cannot be isolated from the reactor. The limits of the RCPB are:

- The outermost containment isolation valve in RCS piping which penetrates primary reactor containment, if relevant;
- The reactor coolant system safety or safety relief valves;
- The second of two isolation valves for piping connected to RCS and whose failure would result in a leakage non-compensable by the normal water make-up system;
- The first isolation valve, for piping connected to RCS whose failure would result in a leakage compensable by the normal water make-up system, if relevant;
- The second isolation valve as seen from the reactor side in the main steam and feed water piping (BWR).

5.43. Paragraphs 5.44–5.51 provide recommendations on meeting the Requirement 6.13 of SSR-2/1 (Rev. 1) [1].

5.44. Isolation devices between the RCPB and connected piping or component whose failure would result in a leakage non compensable by the normal make up system should be designed to close quickly and reliably in order to limit the loss of coolant. The loss of coolant caused by such a failure should not necessitate the operation of the emergency core cooling system.

5.45. 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 without the need for off-site electrical power. The response time and closure time should be in accordance with the acceptance criteria defined for postulated initiating events.]In particular, to keep the full efficiency of the emergency core cooling system, all the systems connected to the RCPB should be automatically isolated in a timely manner unless necessary to meet the requirements applicable to a LOCA accident.

5.46. RCPB isolation should be designed according to the single failure criterion when the loss of coolant resulting from the break of the connected piping is not compensable by the normal make up system. .

5.47. RCPB isolation should be ensured even in the event of a loss of off-site power and preferably supplied by the uninterruptible power source.

5.48. RCPB isolation valves should be designed to return to a safe position in case of the loss of the power or air supply.

5.49. Adequate means should be provided in connected systems operating at lower pressures to prevent the over pressurization of such systems and possible loss of coolant accidents outside the containment.

5.50. Isolation devices should be designed and manufactured in compliance with the requirements and recommendations that apply to RCS components.

5.51. Provisions for testing leak tightness of the RCPB isolation valves should be implemented.

Postulated Initiating events

5.52. 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 categorized on the basis of their estimated frequency of occurrence. Typical examples are:

- Loss of off site power sources ;
- Malfunctioning of RCS control systems (pressure), (RPV water level, RCS recirculation flow, feed water heating for BWR), (PZR and SG level for PWR and PHWR), etc,
- Loss of the main condenser vacuum;
- Piping breaks;
- Spurious opening of a relief/safety valve;
- Loss of forced coolant circulation;
- Reactor Coolant Pump failure;
- Positive core reactivity insertion.

Internal Hazards

5.53. 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. Typical examples are:

- A break of a reactor coolant leg should neither propagate to neighbouring RCS leg or to main steam /feed water piping (for PWR and PHWR);
- A break of a main steam/feed water piping should neither propagate to neighbouring main steam/feed water piping or to reactor coolant loops;
- A break of pressurizer piping should not propagate to neighbouring pressurizer piping (PWR and PHWR).

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

External Hazards

5.55. The integrity of the RCPB should be maintained in the event of earthquake (SL2).

5.56. RCS components which are not part of the RCPB 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.

5.57. 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.

5.58. 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

5.59. The arrangement of piping and the location of equipment should facilitate establishment of natural circulation allowing the core decay heat removal.

5.60. 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. The layout of the piping should also be such as to prevent the accumulation of combustible gases.

5.61. 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.

Design limits

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

- Pressure and temperature;
- Max cooling rate, max heating rate for normal operation;
- Delta T max between hot leg and pressurizer (for PWR);
- Delta P max Primary/Secondary (for PWR);
- Max RCS leak rate;
- Max RCS/SG leak rate (for PWR and PHWR);
- Limits regarding the brittle fracture of RPV (for PWR);

- Component parameters (e.g. Delta P for reactor coolant pump seals, T seals).

General recommendations given in [15] should also be considered when relevant.

Safety classification

5.63. 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).

5.64. 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 [8] supplemented by the TECDOC 1787 [9].

Environmental qualification

5.65. 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. Typically equipment necessary for the accomplishment of the following

- 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);
- RCS Components designed to depressurize the RCS allowing the use of the low pressure pumps in accident conditions;
- RCS Components designed to depressurize the RCS in order to prevent Direct Containment Heating loads caused by the RPV failure at high pressure (for operability).

5.66. The selection of materials to be used for gasket and seals should be based on their suitability to maintain their capability when exposed to operating and accident conditions.

Pressure tests

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

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

Venting

For PWR

5.69. 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.

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

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

For BWR

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

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

5.74. Venting should be effective despite a single failure.

5.75. RCS components necessary for the venting should be qualified for accident conditions relevant for their intended.

5.76. Venting operation should be possible from the main control room.

For PHWR

Provisions should be implemented to limit the concentration of non-condensable gases in the primary coolant in normal operation.

Specific design aspects

Reactor pressure vessel

5.77. 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 limits as well as allowable heating and cooling rates as a function of temperature should be established for the pressure vessel. Changes of the brittle-ductile transition temperature of the beltline material due to neutron irradiation and thermal embrittlement should be accounted for.
- The vessel 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 at an acceptable level;
- The design of the pressure vessel should be such that it can withstand pressurized thermal shocks without losing its integrity;
- 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.

5.78. If advanced materials were to be used in the reactor pressure vessel, samples of these materials should be subjected to a fast neutron flux with high lead factor compared to the vessel wall and exposed to the environment of the pressure vessel. They should be examined periodically throughout the plant lifetime to monitor changes in mechanical properties (in particular ductility and toughness), and to enable predictions to be made of the behaviour of the material in due time allowing for corrective measures if necessary.

5.79. 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 (for PWR and BWR)

5.80. 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.

5.81. Pressure vessel internals should be designed to withstand loads associated to operational and accident conditions without significant core degradation and should keep capability to:

- support the core and permit the cooling of the fuel elements;
- insert of the control rods in the core to shut down the reactor.

5.82. Pressure vessel internals should be designed to:

- Properly channel the coolant flow through the vessel and fuel;
- Prevent unacceptable flow induced vibration;
- Minimize the susceptibility to stress corrosion cracking;
- Accommodate asymmetric blow-down loads caused by pipe ruptures;
- Ensure that fuel design limits are not exceeded in normal operation or anticipated operational occurrences.

Fuel channel assemblies (for PHWR)

5.83. 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.

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

5.85. 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.

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

5.87. 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.

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

5.89. Prototype 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.

5.90. 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.

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

5.92. The design should provide a mean for allowing reliable detection of fuel defects in the core during normal operation.

Reactor Coolant Pumps (PWR/PHWR) or Reactor Recirculation Pumps (BWR)

5.93. The design of reactor coolant pumps should be such that the following safety parameters 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.

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

5.95. The RCS pumps should be such as to provide an adequate flow of coolant with suitable hydraulic parameters to ensure that the applicable structural limits for the fuel and the RCS equipment including RPV internal are not exceeded in operational states and accident conditions without significant core degradation.

5.96. RCS pumps should have adequate flow coast-down characteristics in the event of a pump trip under AOO and plant states without significant core degradation to avoid undesirable thermal-hydraulic conditions of the reactor coolant with regard to the integrity of the fuel.

5.97. 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 SSCs important to safety from any such missiles.

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

5.99. RCP seal leakage should be controlled by maintaining adequate cooling of seal system in any plant states without significant core degradation. 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 to the seal system.

Relief and Safety Valves (PWR and PHWR) or Safety Relief Valves (BWR)

5.100. If compressed air is needed to operate relief valves, dedicated pneumatic accumulators should be associated to the valves to ensure a minimum and specified number of openings and closures. The number of times that each valve must be opened utilizing the pneumatic accumulators without recharging should be defined.

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

5.102. Where the over pressure protection is ensured by pilot operated safety valves (BWR and PWR), no shut-off valve should be installed in the pilot line required for opening the 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.

Steam generators (PWR and PHWR)

5.103. Steam generators tubes belong to the RCPB and hence should be designed with the same recommendations.

5.104. 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 accident conditions without significant core damage (e.g. should be designed to withstand loads from a 2A LOCA and a main steam line break).

5.105. 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.

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

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

5.108. Loadings such as those due to water hammer, over filling and thermal and/or hydraulic stratification should be addressed for the operating modes in which they may occur.

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

5.110. The design should include provisions for sampling water and steam from relevant locations of the secondary side.

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

5.112. 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;

5.113. Allowance for fouling, tube plugging, maximum allowable tube leakage should be specified for the plant operation.

5.114. Design provisions to prevent tube fretting should be implemented.

5.115. Design provisions to perform SG sampling should be implemented.

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

5.117. Electro-chemical interaction of SG tubes material and tube supports material should be prevented.

Piping system

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

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

5.120. 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.

5.121. Flow restrictors should be included in the main steam lines for BWR or SG outlet for PWR/PHWR, to limit the rate of loss of coolant following a main steam line break inside or outside the containment. For BWR, it should ensure that the core remains fully covered by water before the closing of the MSIVs.

Leak before break or break preclusion piping

5.122. If a leak before break or break preclusion concept is claimed for piping, the specific requirements to be met for design, manufacturing and operation should be defined.

5.123. Leak detection systems should be implemented with performances consistency with the demonstration of the leak before break assumptions..

5.124. 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:

- Core cooling capacity;
- Pressure build up inside the Primary Containment;
- Environmental qualification of equipment.

Leak detection system

5.125. Provisions should be made for the detection of any leakage of reactor coolant, and to the extent practicable for the identification of the location of the leak. Provisions should also be made to quantify and collect RCS leakages. These provisions should be adequately complemented by indicators and alarms in the main control room.

Insulation materials

5.126. Insulation material used inside the Primary containment should be selected in order to prevent clogging of the sump strainers and filters in case of high energy pipe breaks. Reflective metallic insulation should be used to the extent reasonably achievable.

5.127. For design relying on In Vessel Retention (IVR) strategy relying on 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 contacting 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.

6. SPECIFIC CONSIDERATIONS IN DESIGN OF THE ASSOCIATED SYSTEMS FOR PWR TECHNOLOGY

SYSTEMS FOR COOLANT INVENTORY AND CORE REACTIVITY CONTROL IN OPERATIONAL STATES

6.1. 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 performed by CVCS are:

- Control of the reactor coolant inventory;
- Control of the RCS pressure in shut-down modes with RCPs unavailable;
- 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.

6.2. 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.

Control of the coolant inventory

6.3. 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.

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

6.5. 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.

Core reactivity control

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

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

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

6.9. CVCS should have capabilities to prevent or to limit uncontrolled dilution of the RCS.

SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES

Heat removal in power operation and hot shut-down modes

6.10. 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.

6.11. 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.

6.12. 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 Residual Heat Removal System (RHRS).

6.13. 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.

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

6.15. Main feed water injection should be automatically stopped after a reactor trip in order to prevent an excessive cooling of the core.

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

6.17. In 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.

6.18. Each SG should be able to be independently and reliably isolated.

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

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

6.21. 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.

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

6.23. 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).

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

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

6.26. Systems operated to remove residual heat in hot shutdown mode should be designed to keep their operability in the event of a SL2 earthquake.

Residual heat removal in RHR mode

6.27. 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.

Paragraphs 6.28–6.38 provide recommendations on meeting the Requirement 51 of SSR-2/1 (Rev. 1) [1] and supplement the generic recommendations indicated in section 3.

6.28. 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).

6.29. 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.

6.30. 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.

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

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

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

6.34. 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

6.35. 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 operating conditions for the fuel and the reactor coolant pressure boundary.

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

6.37. 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.

6.38. Adequate instrumentation and isolation capability should be provided to detect leakages 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.

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

SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS

6.40. 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 not 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 4.

6.41. Paragraphs 6.41–6.46 provide recommendations on meeting the Requirements 7, 19 and 29 of SSR-2/1 (Rev. 1) [1] and supplement the recommendations indicated in section 3.

6.42. 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.

6.43. Systems designed for cooling the core in accident conditions (DBAs or DEC conditions 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.

6.44. The design of systems necessary in DBA conditions or in DEC conditions without significant core damage 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.

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

6.46. 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.

6.47. Performances of safety features for DEC conditions 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 applied 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 DEC conditions and to avoid cliff edge effects, key parameters should be identified and provisions for covering uncertainties should be taken.

Core cooling in accident conditions

6.48. The RCS water inventory control in accident conditions is performed by the Emergency Core Cooling System (ECCS) in conjunction with a depressurization of the RCS by the secondary side when necessary. The emergency core cooling 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.⁹

6.49. 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 availability of RCS feed & bleed.

6.50. Paragraphs 6.51–6.67 provide recommendations on meeting the Requirement 52 of SSR-2/1 (Rev. 1) [1] 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:

6.51. 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.

6.52. 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).

⁹ Specifications concerning the sump filtration system are given in [13].

6.53. 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.

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

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

6.56. 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);

6.57. The emergency core cooling system injection capacity should prevent boron crystallization in the core.

6.58. In some design, the emergency cooling system includes capabilities to remove core decay heat in the long term when RCS integrity is not assured. Those capabilities should be considered as part of the safety system.

6.59. 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 account the installed capacity for RCS bleeding.

Specific Design aspects

6.60. 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)¹⁰.

6.61. 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 designed to open quickly and without external service (e.g. check valves are widely used). Leak-tightness of the RCS isolation should be designed to be periodically tested. Moreover, ECCS should be

¹⁰ 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 SNC1 or similar standards),

protected against over pressurization caused by leakages. Adequate measurement should be installed (pressure, temperature) for warning about leakages through isolation valves.

6.62. 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.

6.63. 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).

6.64. Provisions should be implemented for an early detection of leakages 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.

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

6.66. The ECCS should be qualified to operate with active water loaded with particles, according to the filtration system capability.

6.67. 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 limiting phenomena such as vortex, air entrainment and accumulation of debris at the surface of the sump filters. Accounting for internal containment pressure build-up should be specifically justified if such practice is possibility arises from national regulatory provisions.

6.68. 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

6.69. 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.

6.70. Paragraphs 6.70–6.79 provide recommendations on meeting the Requirement 51 of SSR-2/1 (Rev. 1) [1] in DBA conditions, and to supplement recommendations indicated in section 3 relevant for safety systems.

6.71. Emergency Feed Water (EFW) and steam dump to atmosphere systems should have adequate performances to reliably accomplish residual heat removal and RCS cooling without exceeding limits defined for fuel, for the RCPB and structures important to safety defined for in accident conditions without significant core degradation.

6.72. EFW capacity and autonomy should be appropriate to reach RCS conditions compatible with RHR operation with adequate margins (24 hour autonomy is generally considered 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

6.73. 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.

6.74. 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 when the main condenser is not available or the main steam isolation valves are closed

Specific Design aspects

6.75. 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 accomplished¹¹).

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

6.77. 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.

¹¹ 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 SNC1, or similar standards).

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

6.79. Isolation of EFW to 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.

6.80. Isolation of main steam relief 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

6.81. 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.

6.82. Such a system includes several redundant safety divisions, each of which includes a pump and a heat exchanger with the intermediate cooling system; it takes suction from RCS and injects back water into RCS after being 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.

6.83. Paragraphs 6.83–6.85 provide recommendations on meeting the Requirement 51 of SSR-2/1 (Rev. 1) [1] in DBAs.

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

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

Specific Design aspects

6.86. 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)¹².

6.87. Recommendations 3.48 to 3.52 should also be considered.

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

6.88. Paragraphs 6.88–6.89 provide recommendations on meeting the Requirement 51 of SSR-2/1 (Rev. 1) [1] in DEC without significant core degradation.

6.89. Although needs for DEC 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 not 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;
- Remove decay heat from the core by operating a primary feed and bleed strategy;
- Implementation of a Passive Residual Heat Removal system.

6.90. 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, (e.g. the fire engines or mobile diesel-pumps).

RCS fast depressurization in design extension conditions with core melting

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

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

¹²As 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, or code JSME SNC1 or similar standards.

Specific design aspects

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

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

6.95. 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.

6.96. While 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.

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

6.98. The RCS fast depressurization shall be possible in case of station black-out.

SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS

6.99. Paragraphs 6.99–6.104 provide recommendations on meeting the Requirement 46, paras. 6.10 and 6.11 of SSR-2/1 (Rev. 1) [1] in accident conditions without significant core degradation. The following recommendations are for the design of the system relying on an adequate injection of water with high boric acid concentration. Recommendations for the shut-down system relying on the drop of solid absorbers are provided in [16].

6.100. 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.

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

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

6.103. ~~Acid-B~~boric acid concentration should be sufficient to compensate for the moderator effect variation during the RCS cooling.

Specific Design aspects

6.104. 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 accomplished¹³).

6.105. 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.

7. SPECIFIC CONSIDERATIONS IN DESIGN OF THE ASSOCIATED SYSTEMS FOR BWR TECHNOLOGY

SYSTEMS FOR COOLANT INVENTORY AND CORE REACTIVITY CONTROL IN OPERATIONAL STATES

Core reactivity control by moving control rods and by controlling of the recirculation coolant flow rate are addressed in [16].

Reactor water clean-up (RWCU)

7.1. 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.

7.2. 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.

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

¹³ 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 SNC1, or similar standards),

SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES

The following recommendations provide guidance to fulfil Requirement 51 of [1] and supplement the generic recommendations indicated in section 3.

7.4. 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 refuelling).

7.5. 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 refuelling operation in a reasonably short period.

7.6. 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.

7.7. 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.

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

7.9. 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)

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

7.11. 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.

7.12. 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.

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

7.14. 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

7.15. Emergency Core Cooling Systems (ECCS) should be designed and implemented to fulfil Requirement 52 of [1] 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).

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

7.17. Instrumentation should be provided to control temperature and water level of the suppression pool in accident conditions.

Residual heat removal in case of design basis accidents

7.18. 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

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

7.20. 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.

7.21. A reliable RCS depressurization system should be implemented to permit the injection of coolant to the RPV in the event that the high pressure core cooling injection is unable to keep RPV water level high enough.

7.22. 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.

7.23. Operability of the valve of turbine driven water supply system such as RCIC by using compressed air, DC power or human power should be ensured in case of Station Blackout (Loss of all AC power).

RCS fast depressurization in design extension conditions with core melting

7.24. A RCS depressurization should be implemented to prevent direct containment heating loads caused by the RPV failure at high pressure. This function should be accomplished with a different and dedicated set of SRVs which should be designed to remain open after the depressurization.

SYSTEMS FOR CORE REACTIVITY CONTROL IN ACCIDENT CONDITIONS

The Control Rod system is not discussed in the context of this guide (see [16]).

7.25. 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.

7.26. SLCS should have capability to shut down the core and to maintain sub criticality in the most reactive operational state with adequate margin for.

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

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

8. SPECIFIC CONSIDERATIONS IN DESIGN OF THE ASOCOATED SYSTEMS OF PHWR TECHNOLOGY

8.1. 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 fuel handling, including the re-fuelling machines;
- The pressure control and inventory control system;
- The pump seal cooling system;

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

SYSTEMS FOR REACTIVITY CONTROL IN OPERATIONAL STATES

8.2. This section presents the systems designed for the reactivity control function during operational conditions. Control devices used in the reactor control system include mechanical absorbers, adjusters and light-water zone compartments.

8.3. Under normal operating conditions, the reactor control system should control reactor power and, where applicable, flux spatial distribution, within operating limits for all operational mode. The operational limits may include maximum reactor power, maximum fuel channel or bundle power and maximum flux tilts.

8.4. Under AOO conditions, the reactor control system should respond to deviations from normal operation to keep all essential reactor parameters within specified limits and to prevent AOOs from escalating to accident conditions. The responses could be setback or stepbackstep back which reduces the power at different rates to appropriate levels

SYSTEMS FOR HEAT REMOVAL IN OPERATIONAL STATES

8.5. 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

8.6. 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.

8.7. 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.

8.8. 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.

8.9. The feed water system should take hot, pressurized feed water from the feed water train in the turbine building and supply it to the steam generator secondary side.

8.10. Provision should be made to control the steam pressure and the water inventory in the steam generators during start-up.

8.11. 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.

8.12. 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.

8.13. 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.

8.14. 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.

8.15. Redundant heat removal systems 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.

8.16. 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.

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

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

8.19. 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.

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

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

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

8.23. 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.

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

8.25. 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)

8.26. 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.

8.27. 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.

8.28. The SDCS should preferably be located inside the containment.

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

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

8.31. 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.

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

8.33. 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.

8.34. The SDCS should have sufficient flow adjustment capability.

8.35. 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.

8.36. 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 heat removal system.

8.37. 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.

8.38. An auxiliary feed water system or equivalent should be designed to maintain the plant in a hot standby condition for an extended period. The auxiliary feed water system should provide

sufficient capacity to fulfil this function efficiently. Where a connection to the Reserve feed water or to the deaerator is not possible, an alternate means to supply the auxiliary feed water to steam generators should be provided in the design

8.39. 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) and also 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 REACTIVITY CONTROL IN ACCIDENT CONDITIONS

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

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

Reactor Shut-down System 2

8.42. A PHWR reactor is equipped with two physically independent shutdown systems. These shutdown systems are designed to be both functionally different and geometrically separate. The functional difference is achieved by the use of shutoff rods for the first shut-down system (SDS1) and liquid poison injection for the second shut-down system (SDS2). Both shut-down systems are designed to be independently capable of quickly rendering the reactor subcritical from all AOOs and DBAs by an adequate margin.

The Second reactor shut-down system 2 (SDS2) provides a fast injection of a concentrated gadolinium nitrate solution (liquid neutron absorber) 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 injecting the poison solution. SDS2 employs an independent —multiple reactor trip logics which senses the parameters required for the shut-down and opens fast-acting helium pressure valves to inject the gadolinium poison into the moderator.

8.43. The first and second reactor shut-down systems (SDS1 and SDS2) should be passive, fast acting, fully capable, diverse and functionally independent of each other.

8.44. SDS2 should be designed to avoid chemistry-related issues (e.g. avoiding precipitation).

8.45. SDS2 should be designed to meet the acceptance criteria for the reactor trip parameter effectiveness for all AOOs and accident conditions without significant core damage.

8.46. 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 poison with an 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 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.

8.47. 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:

- Be capable of maintaining the reactor sub-critical following an SDS2 Reactor Trip;
- Allow arresting the injection if the SDS2 Trip Logic clears an unsealed-in Reactor Trip state.

8.48. 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.

SYSTEMS FOR CORE COOLING AND RESIDUAL HEAT REMOVAL IN ACCIDENT CONDITIONS

8.49. This section presents the systems designed for maintaining the cooling safety function during accident conditions, including DBAs and DECAs 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.

8.50. Systems in the RCSAs 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..

8.51. Systems that are provided to mitigate the consequences of DECAs should be considered as design features for DECAs 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

8.52. 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.

8.53. 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.

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

8.55. The emergency core cooling system injection capacity should ensure core re flooding in case of design basis LOCA, according to the applicable acceptance criteria.

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

8.57. 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.

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

8.59. 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.

8.60. 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.

8.61. 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. 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.

8.62. 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 [1]. 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.

8.63. 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.

8.64. 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.

8.65. 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 DECAs without significant core degradation (LOCA and secondary breaks).

8.66. Possible leakages 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.

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

8.68. 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.

8.69. 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.

8.70. 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.

8.71. The ECCS provides an extension of the containment (3rd 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 [13]).

8.72. 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 [18].

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

Enhanced emergency heat removal system

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

8.75. 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).

8.76. 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.

8.77. 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.

8.78. 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.

8.79. The passive train of the EHRS and its supporting SSCs should be designed to operate under the DEC's without significant core degradation.

8.80. 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.

8.81. 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.

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

8.83. 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.

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

8.85. 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.

8.86. 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.

8.87. The design should demonstrate that emergency heat removal capability is provided for all operating and accident conditions.

- 8.88. 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.
- 8.89. 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
- 8.90. These systems should be capable of removing the heat loads from safety-related SSCs under DBAs and DECAs without significant core degradation.
- 8.91. The application of the single failure criteria is not explicitly required by [1] for all design safety features for DECAs.
- 8.92. 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 DECAs.
- 8.93. The safety features for DECAs 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.
- 8.94. Manual actuation of the safety features for DECAs should be possible from the MCR and if appropriate from the SCR.
- 8.95. 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.
- 8.96. 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.
- 8.97. Natural circulation systems require a demonstration of capability over the full range of applicable operating conditions.
- 8.98. The need for automatic actuation of safety features for DECAs without significant core degradation should be evaluated in the safety analysis case by case.
- 8.99. 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.

8.100. In the cases where crediting the passive EHRS for DEC 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

8.101. The complementary design feature is to have the capability to transfer residual heat from the core to an ultimate heat sink.

8.102. 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 DEC; and have reliability commensurate with the function that they are required to fulfil.

8.103. The design principles for design features to deal with DEC 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.

8.104. 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.

Moderator system for DEC without significant core degradation

The moderator system can be operated as an emergency heat removal for DEC 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.

8.105. 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.

8.106. 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 DEC 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 DEC without significant core degradation.

8.107. The design of the moderator system should consider all configurations when credited as an emergency heat removal for DEC's without significant core degradation.

8.108. Each configuration, independently, should have adequate load capacity to transfer the heat to the ultimate heat sink and to prevent calandria tubes' failure.

8.109. The heat load capability of the moderator system configuration for DEC's without significant core degradation should be demonstrated by means of tests and analyses.

8.110. The moderator system should be designed such that forced convection and natural convection flows are in the same direction.

8.111. 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.

8.112. The moderator pumps should be designed to retain their pressure integrity during and following a site design basis earthquake.

8.113. 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.

8.114. The calandria vessel should be equipped with overpressure protection devices such as rupture disks or equivalent devices.

8.115. The relief capacity should be sufficient to avoid over-pressurization limits of the SSCs credited for DEC's without significant core degradation. Limits given by proven industry codes and standard applicable to nuclear pressure vessel should be used.

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

8.116. 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.

8.117. 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.

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

LIST OF ABBREVIATIONS

AC/DC: Alternative current / direct current

AOO: Anticipated operational occurrence

ATWS: Anticipated transient without ~~s~~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

EHR: 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

RCP: Reactor coolant pump

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)

SG: Steam generator

SGTR: Steam generator tube rupture

SRV: Steam relief valves

SSC: Structures, systems and components

SSPB: Secondary side Pressure Boundary

TSC: Technical support centre

UHS: Ultimate heat sink

REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 Rev.1, IAEA, Vienna (2016).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).
- [3] 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).
- [4] 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).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal hazards in the Design of Nuclear Power Plants (DS 494).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016).
- [8] 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).

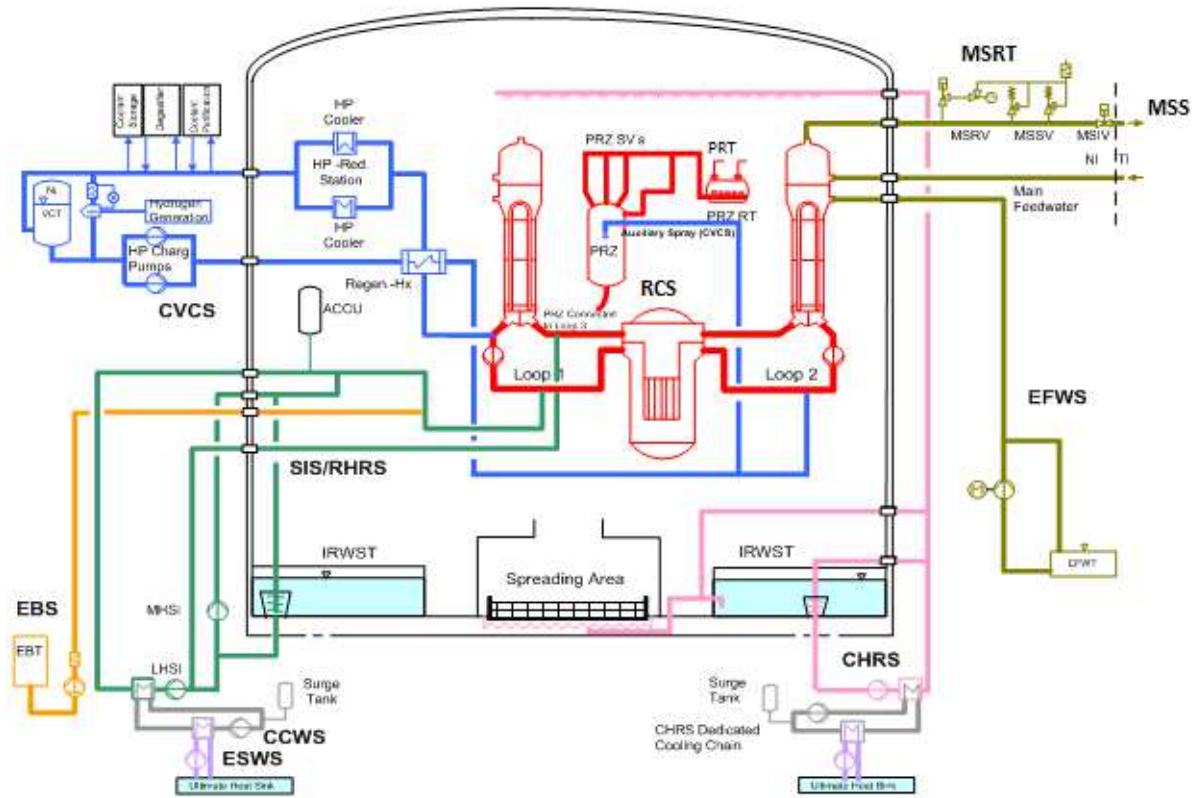
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA TECDOC Series 1787 (2016)
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants (DS 485).
- [11] 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).
- [12] 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).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, IAEA Safety Standards Series No. DS 482 (under revision).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).
- [15] 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).
- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Core for Nuclear Power Plants, IAEA Safety Standards Series No. DS 488 (under revision).
- [17] 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).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Auxiliary and support systems for Nuclear Power Plants, IAEA Safety Standards Series No DS 440.

[19] 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).

[20] 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 Water System

PRT: Pressurizer Relief Tank

CHRS: Containment Heat Removal System

RCS: Reactor Cooling System

CVCS: Chemical and Volume Control System

RHRS: Reactor Heat Removal System

EBS: Emergency Borating System

SIS: Safety Injection System

EFWS: Emergency Feed Water System

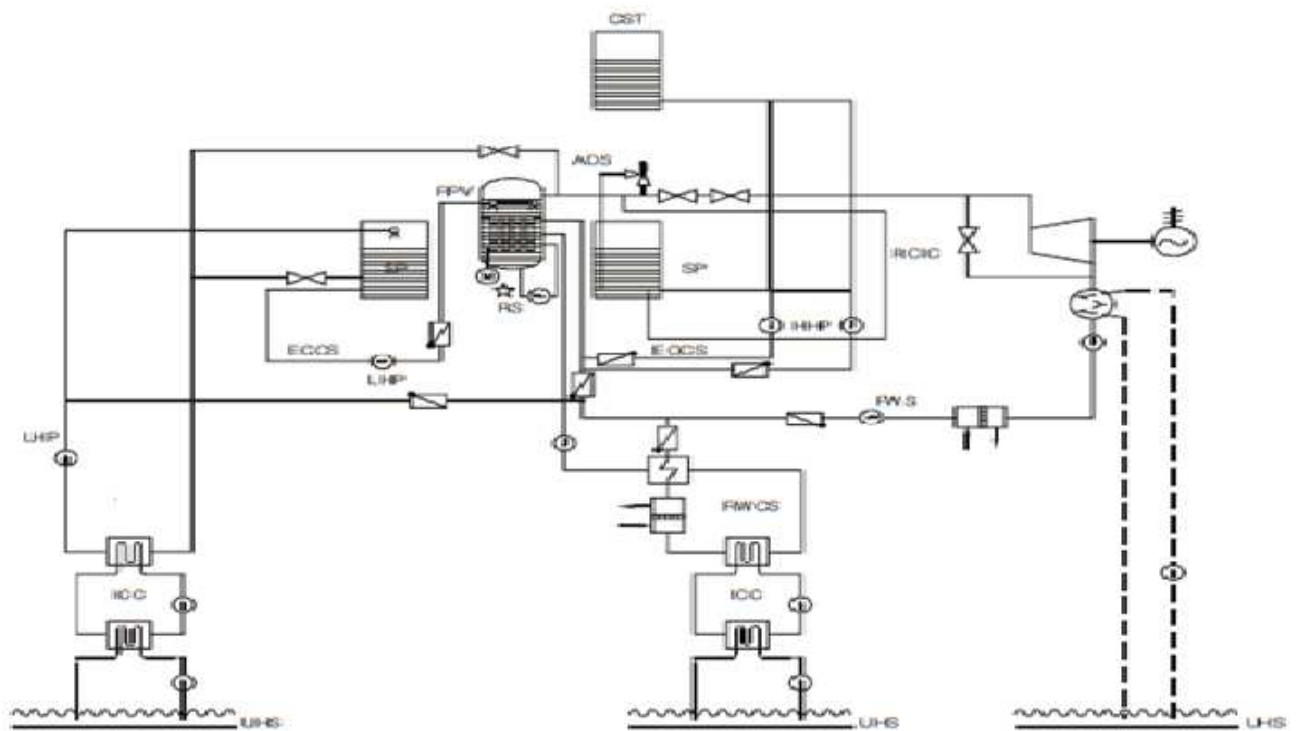
ESWS: Essential Service Water System

IRWST: In Containment Reactor Water Storage tank

MSRT: Main Steam Relief Train

MSS: Main Steam System

ANNEX II: BWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS



ADS: Automatic Depressurization System

CST: Condensate Storage tank

ECCS: Emergency Core Cooling System

FWS: Feed Water System

HHIP: High Head Injection Pump

ICC: Intermediate Cooling Circuit

LHP: Low Head injection Pump

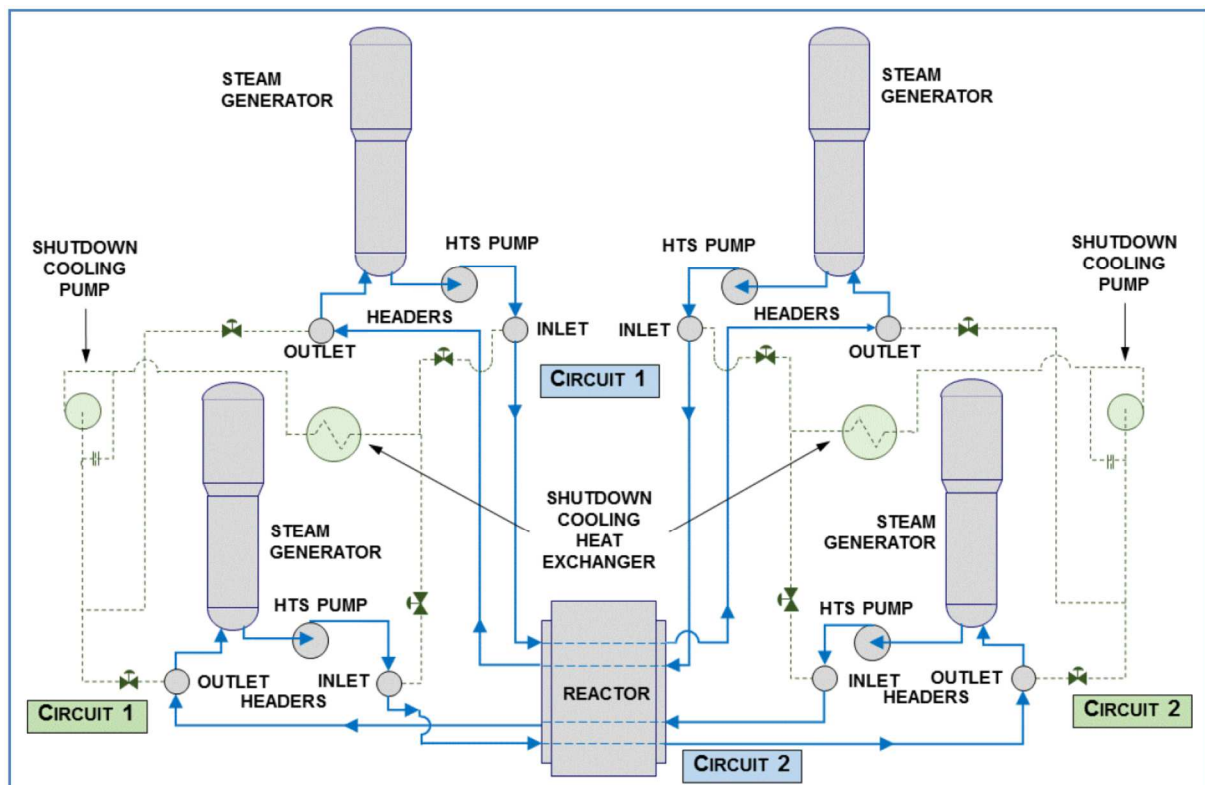
RCIC: Reactor Core Isolation Cooling

RPV: Reactor Pressure Vessel

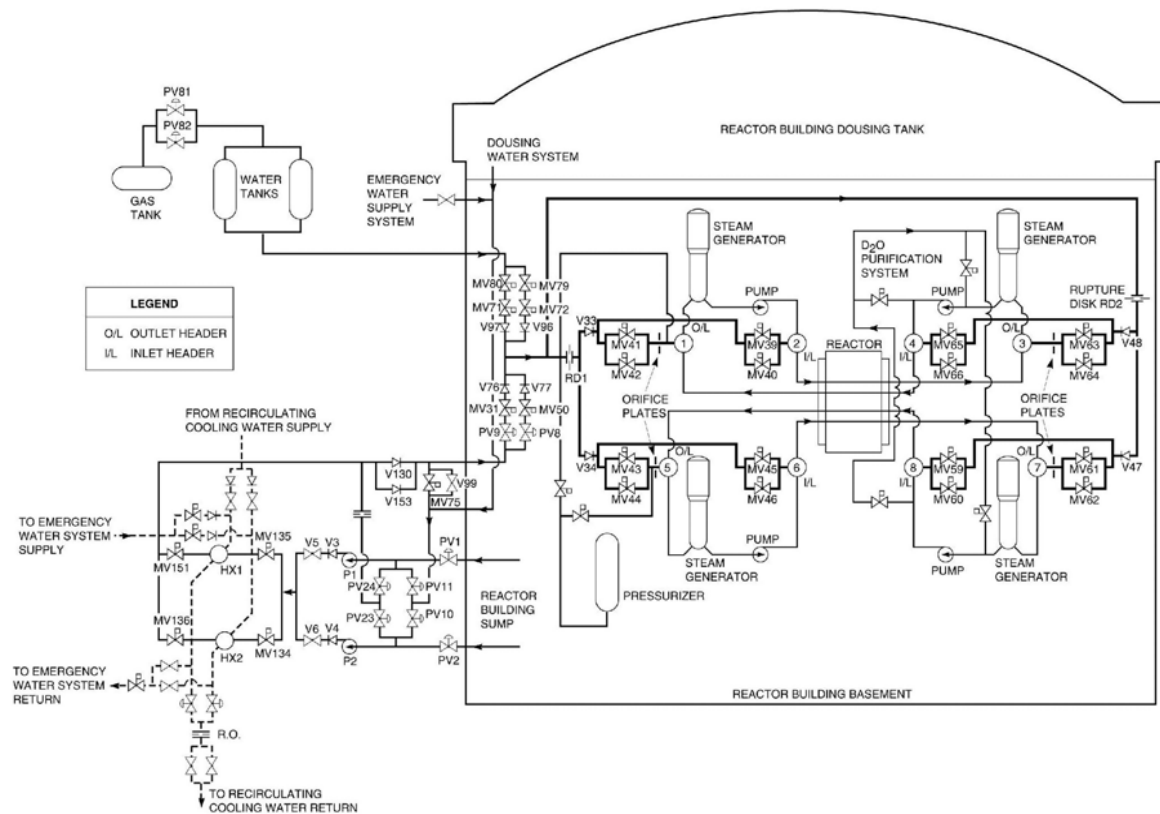
SP: Suppression pool

UHS: Ultimate Heat Sink

ANNEX III: PHWR DIAGRAMS OF THE RCS AND ASSOCIATED SYSTEMS



Typical Reactor Coolant System (Primary Heat Transport System) and Shutdown Cooling System for PHWR



Typical Emergency Core cooling System for PHWR

CONTRIBUTORS TO DRAFTING

Baik, S.J. KEPCO-E&C, South Korea

Beard, James GE- Hitachi Nuclear Energy Ltd, USA

Courtin, E. AREVA, France

Fil, N. Consultant, Russian Federation

Gasparini, M. Consultant. Italy

Jackson, C. US Nuclear Regulatory Commission, USA

Mesmous, N. Canadian Nuclear Safety Commission, Canada

Myeong-Yong Ohn Canadian Nuclear Safety Commission, Canada

Nakajima T. Nuclear Regulation Authority, Japan

Poulat, B. International Atomic Energy Agency

Taniguchi, A. Tokyo Electric Power Company Holdings, inc.

Yamazaki, H. Toshiba Corporation, Japan

Yllera, J. International Atomic Energy Agency

Yoshikawa, K. Hitachi-GE Nuclear Energy Ltd, Japan