Western European Nuclear Regulators' Association
REACTOR HARMONIZATION WORKING GROUP

WENRA Reactor Safety Reference Levels

January 2007

Issue A: Safety Policy	
Document status: Final	Safety area: Safety Management

Reference levels

1. Issuing and communication of a safety policy

1.1 A written safety policy[1] shall be issued by the licensee.

1.2 The safety policy shall be clear about giving safety an overriding priority in all plant activities.

1.3 The safety policy shall include a commitment to continuously develop safety.

1.4 The safety policy shall be communicated to all site personnel with tasks important to safety, in such a way that the policy is understood and applied.

1.5 Key elements of the safety policy shall be communicated to contractors, in such a way that licensee's expectations and requirements are understood and applied in their activities.

2. Implementation of the safety policy and monitoring safety performance

2.1 The safety policy shall require directives for implementing the policy and monitoring safety performance.

2.2 The safety policy shall require safety objectives and targets, clearly formulated in such a way that they can be easily monitored and followed up by the plant management.

3. Evaluation of the safety policy

3.1 The adequacy and the implementation status of the safety policy shall be evaluated by the licensee on a regular basis, more frequent than the periodic safety reviews.

[1] A safety policy is understood as a documented commitment by the licensee to a high nuclear safety performance supported by clear safety objectives and targets and a commitment of necessary resources to achieve these targets. The safety policy is issued as separate safety management document or as a visible part of an integrated organisational policy.

Issue B: Operating Organisation	
Document status: Final	Safety area: Safety Management

Reference levels

1. Organisational structure

1.1 The organisational structure for safe and reliable operation of the plant, and for ensuring an appropriate response in emergencies, shall be justified[2] and documented.

1.2 The adequacy of the organisational structure, for its purposes according to 1.1, shall be assessed when organisational changes are made which might be significant for safety. Such changes shall be justified in advance, carefully planned, and evaluated[3] after implementation.

1.3 Responsibilities, authorities, and lines of communication shall be clearly defined and documented for all staff with duties important to safety.

2. Management of safety and quality

2.1 The licensee shall ensure that the plant is operated in a safe manner and in accordance with all applicable legal and regulatory requirements.

2.2 The licensee shall ensure that decisions on safety matters are preceded by appropriate investigation and consultation so that all relevant safety aspects are considered. Safety issues shall be subjected to appropriate safety review, by a suitably qualified independent review function.

2.3 The licensee shall ensure that the staff is provided with the necessary facilities and working conditions to carry out work in a safe manner.

2.4 The licensee shall ensure that safety performance is continuously monitored through an appropriate review system in order to ensure that safety is maintained and improved as needed.

2.5 The licensee shall ensure that relevant operating experience, international development of safety standards and new knowledge gained through R&D-projects are analysed in a systematic way and continuously used to improve the plant and the licensee's activities.

2.6 The licensee shall ensure that plant activities (processes) are controlled through a documented quality management system covering all activities, including relevant activities of vendors and contractors, which may affect the safe operation of the plant.

[2] The arguments shall be provided that the organisational structure supports safety and an appropriate response in emergencies.
[3] A verification that the implementation of the organisational change has accomplished its safety objectives.

3. Sufficiency and competency of staff

3.1 The required number of staff for safe operation[4], and their competence, shall be analysed in a systematic and documented way.

3.2 The sufficiency of staff for safe operation, their competence, and suitability for safety work shall be verified on a regular basis and documented.

3.3 A long-term staffing plan[5] shall exist for activities that are important to safety.

3.4 Changes to the number of staff, which might be significant for safety, shall be justified in advance, carefully planned and evaluated after implementation.

3.5 The licensee shall always have in house, sufficient, and competent staff and resources to understand the licensing basis of the plant (e.g. Safety Analysis Report or Safety Case and other documents based thereon), as well as to understand the actual design and operation of the plant in all plant states.

3.6 The licensee shall maintain, in house, sufficient and competent staff and resources to specify, set standards manage and evaluate safety work carried out by contractors.

[4] Operation is defined as all activities performed to achieve the purpose for which a nuclear power plant was constructed (according to the IAEA Glossary).

[5] Long term is understood as 3-5 years for detailed planning and at least 10 years for prediction of retirements etc.

Issue C: Quality Management	
Document status: Final	Safety area: Safety Management

Reference levels

1. Objectives

1.1 Throughout the life of a nuclear power plant the licensee shall develop, implement, and maintain a documented quality management system[6] that defines the required quality and safety objectives applicable to work that is important to safety and is carried out by any organization[7], unit, or individual who can affect nuclear safety.

1.2 The quality management system shall grade the requirements set out in it to reflect their relative importance to nuclear safety with respect to each item, service, or process covered.

1.3 The quality management system shall enable the licensee to evaluate compliance with applicable nuclear safety requirements and to identify potential safety improvements.

2. Scope

2.1 Nuclear safety shall be the overriding consideration in the identification of the items, services, and processes to which the quality management system applies.

2.2 The quality management system shall ensure that the organizational structure, functional responsibilities, levels of authority, and interfaces for all organizations[8], units, and individuals who can affect nuclear safety are clearly documented and assigned.

2.3 The quality management system shall ensure that any organizational change that may affect safety is evaluated, classified with regard to its importance to safety, and justified.

3. Implementation

3.1 The most senior person representing the licensee on site shall be responsible and accountable for ensuring that an effective quality management system is being

---

[6] In some IAEA Member States, the quality assurance programme is referred to as the quality assurance system or the quality system. A more recent term is "Quality Management System". IAEA is revising its main Reference SS document 50-C-SG-Q Code on QA for safety in NPPs etc to align it more with ISO 9001:2000. In Para 1.2 of the 4th draft of DS 338 it explains the new terminology it is proposing to adopt:

> *The term "Management System" has been adopted instead of "Quality Assurance". The term "Management System" reflects the evolution in the approach from the initial concept of "Quality Control" (controlling the quality of products) through "Quality Assurance" (the system to assure the quality of products) and "Quality Management" (the system to manage quality). The "Management System" is a set of interrelated or interacting elements (system) to establish policy and objectives and to achieve those objectives.*

In this Reference Level document, "quality management system" has been used in anticipation of that change whilst adhering largely to related standards from fully endorsed, rather than draft, IAEA standards.

[7] Such organizations include all those within the licensee's company as well as designers, vendors, contractors, suppliers, and service providers employed directly or indirectly on work for the licensee.

[8] Such organizations include all those within the licensee's company as well as designers, vendors, contractors, suppliers, and service providers employed directly or indirectly on work for the licensee.

implemented on site and that the senior management team is committed to and meeting its responsibility for reviewing and ensuring the success of the system.

3.2 The licensee shall establish and maintain sufficient resources and processes to define, achieve, analyse, and preserve the quality of items that are important to safety, and to take timely and effective corrective or preventive action to respond to deviations from required specifications.

3.3 The licensee shall ensure that procured items and services meet established requirements and perform as specified and that selected suppliers continue to provide acceptable items and services during the fulfilment of their procurement obligations. Licensees may delegate procurement activities to other organizations, but shall remain responsible for the overall effectiveness of these activities.

3.4 Products and processes that do not conform to specified requirements shall be identified and reported to an appropriate level of management within the organization. The safety implications of the non-conformances shall be evaluated and the actions taken shall be recorded, where appropriate.

3.5 The quality management system shall be implemented by management in collaboration[9] with those performing the work, and those assessing the work.

3.6 Work that is important to safety shall be controlled and performed using easily understood, approved current instructions, procedures, drawings, or other means, that have been appropriately validated before first use and are periodically reviewed to ensure adequacy and effectiveness.

3.7 Personnel shall be trained in requirements of the quality management system, so that they are competent to perform their assigned work and understand the safety consequences of their activities.

4. Assessment

4.1 The licensee shall assess the quality management system on a regular basis to ensure that it provides the required level of safety.

4.2 An organisational unit shall be established, or an outside agency assigned, that is responsible for independently assessing the adequacy of the quality management system and work performed. The organisational unit shall have sufficient authority and organisational freedom to carry out its responsibilities. People who conduct independent assessments shall not participate directly in the work being assessed[10].

4.3 All managers shall regularly carry out self-assessment by reviewing the processes for which they are responsible to determine their efficiency and effectiveness with establishing, promoting, and achieving nuclear safety objectives, and shall take any necessary corrective actions.

[9] Collaboration is taken to mean that all groups are involved in the process.

[10] However, it is important that the audit team is familiar with the work being assessed. The aim of this requirement is to avoid any conflict of interest on the part of the assessor.

Issue D: Training and Authorization of NPP staff (jobs with safety importance)	
Document status: Final	Safety area: Safety Management

Reference levels

1. Policy

1.1 The licensee shall establish an overall training policy and a comprehensive training plan on the basis of long-term competency needs and training goals that acknowledges the critical role of safety. The plan shall be kept up to date.

1.2 A systematic approach to training shall be used to provide a logical progression, from identification of the competences required for performing a job, to the development and implementation of training programmes including respective training materials for achieving these competences, and to the subsequent evaluation of this training.

2. Competence and qualification

2.1 Only qualified persons that have the necessary knowledge, skills, and safety attitudes shall be allowed to carry out tasks important to safety. The licensee shall ensure that all personnel performing safety-related duties including contractors have been adequately trained and qualified.

2.2 The Licensee shall define and document the necessary competence requirements for their staff.

2.3 Appropriate training records and records of assessments against competence requirements shall be established and maintained for each individual with tasks important to safety.

2.4 Staff qualifying for positions important to safety shall undergo a medical examination to ensure their fitness depending upon the duties and responsibilities assigned to them. The medical examination shall be repeated at specified intervals.

3. Training programmes and facilities

3.1 Performance based training programmes shall be established for all staff with tasks important to safety. The programmes shall cover basic training in order to qualify for a certain position and refresher training as needed.

3.2 All technical staff including on-site contractors shall have a basic understanding of nuclear safety, radiation safety, fire safety, the on-site emergency arrangements and industrial safety.

3.3 Representative simulator facilities shall be used for the training of control room operators to such an extent that the hands-on-training of normal and emergency operating procedures is effective. The simulator shall be equipped with software to cover

normal operation, anticipated operational occurrences, and a range of accident conditions[11].

3.4 For control room operators, initial and annual refresher training shall include training on a representative full-scope simulator. Annual refresher training shall include at least 5 days on the simulator.[12]

3.5 Refresher training for control room operators shall include especially the following items as appropriate:

- Plant operation in normal operational states, selected transients and accidents;
- Shift crew teamwork;
- Operational experiences and modifications of plant and procedures.

3.6 Maintenance and technical support staff including contractors shall have practical training on the required safety critical activities.

4. Authorization

4.1 Staff controlling changes in the operational status of the plant shall be required to hold a authorization valid for a specified time period. The licensee shall establish procedures for their staff to achieve this authorization. In the assessment of an individual's competence and suitability as a basis for the authorization, documented criteria shall be used.

4.2 If an authorised individual:

- Moves to another position for which an authorization is required;
- Has been absent from the authorised position during an extended time period;

Re-authorisation shall be conducted after necessary individual preparations.

4.3 Work on safety related structures, systems, or components carried out by contractor personnel shall be approved and monitored by a suitably competent member of licensee's staff.

[11] This type of simulator is known as a full-scope simulator.

[12] Time includes the necessary briefings.

Appendix E	Issue: Design Basis Envelope for Existing Reactors
Document status: Final	Safety area: Design

Reference levels:

1. Objective

1.1 The design basis[13] shall have as an objective the prevention or, if this fails, the mitigation of consequences resulting from anticipated operational occurrences and design basis accident conditions. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed prescribed limits and are as low as reasonably achievable.

2. Safety strategy

2.1 Defence-in-depth[14] shall be applied in order to prevent, or if prevention fails, to mitigate harmful radioactive releases. The design shall therefore provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment, and an adequate protection of the barriers.

2.2 The design shall prevent as far as practicable:

- challenges to the integrity of the barriers;
- failure of a barrier when challenged;
- failure of a barrier as consequence of failure of another barrier.

3. Safety functions

3.1 The plant shall be able to fulfil the following fundamental safety functions[15]:

- control of reactivity,
- removal of heat from the core and
- confinement of radioactive material,

[13] The design basis shall be reviewed and updated during the lifetime of the plant (see ref level 11.1).
[14] Defined in the IAEA Safety Requirements NS-R-1, 2.9- 2.11. Further information is provided in INSAG-10.
[15] Under the conditions specified in the following paras.

in the plant states: normal operation, anticipated operational occurrences and design basis accident conditions.

4. Establishment of the design basis

4.1 The design basis shall specify the capabilities of the plant to cope with a specified range of plant states[16] within the defined radiation protection requirements. Therefore, the design basis shall include the specification for normal operation and transients/accident conditions from Postulated Initiating Events (PIEs), the safety classification, important assumptions and, in some cases, the particular methods of analysis.

4.2 A list of PIEs shall be established to cover all events that could affect the safety of the plant. From this list, a set of design basis events shall be selected with deterministic or probabilistic methods or a combination of both, and used to set the boundary conditions according to which the structures, systems and components important to safety shall be designed, in order to demonstrate that the necessary safety functions are accomplished and the safety objectives met.

4.3 The design basis shall be systematically defined and documented to reflect the actual plant.

5. Set of design basis events

5.1 Internal events such as loss of coolant accidents, equipment failures, maloperation and hazards, and their consequential events, shall be taken into account in the design of the plant. The list of events shall be plant specific. (see Appendix for assessment of implementation)

5.2 The following types of natural and man made external events shall as a minimum be taken into account in the design of the plant according to site specific conditions:

- extreme[17] wind loading
- extreme outside temperatures
- extreme rainfall, snow conditions and site flooding
- extreme cooling water temperatures and icing
- earthquake
- airplane crash
- other nearby transportation, industrial activities and site area conditions which reasonably can cause fires, explosions or other threats to the safety of the nuclear power plant

[16] Normal operation, anticipated operational occurrences and design basis accident conditions.
[17] Definition of "extreme" is based on historical weather data for the site region

6. *Combination of events*

6.1 Credible combinations of individual events, including internal and external hazards, that could lead to anticipated operational occurrences or design basis accident conditions, shall be considered in the design. Engineering judgement and probabilistic methods can be used for the selection of the event combinations.

7. Definition and application of technical acceptance criteria

7.1 Initiating events shall be grouped into a limited number of categories that correspond to plant states[18], according to their probability of occurrence. Radiological and technical acceptance criteria shall be assigned to each plant state such that frequent initiating events shall have only minor or no radiological consequences and that events that may result in severe consequences shall be of very low probability.

7.2 Criteria for protection of the fuel rod integrity, including fuel temperature, DNB, and cladding temperature, shall be specified. In addition, criteria shall be specified for the maximum allowable fuel damage during any design basis event.

7.3 Criteria for the protection of the (primary) coolant pressure boundary shall be specified, including maximum pressure, maximum temperature, thermal- and pressure transients and stresses.

7.4 If applicable, criteria in 7.3 shall be specified as well for protection of the secondary coolant system.

7.5 Criteria shall be specified for protection of containment, including temperatures, pressures and leak rates.

8. Demonstration of reasonable conservatism and safety margins

8.1 The initial and boundary conditions shall be specified with conservatism.

8.2 The worst single failure[19] shall be assumed in the analyses of design basis events. However, it is not necessary to assume the failure of a passive component, provided it is justified that a failure of that component is very unlikely and it remains unaffected by the PIE.

8.3 Only safety systems shall be credited to carry out a safety function. Non-safety systems shall be assumed to operate only if they aggravate the effect of the initiating event[20].

8.4 A stuck control rod shall be considered as an additional aggravating failure in the analysis of design basis events[21].

8.5 The safety systems shall be assumed to operate at their performance level that is most penalising for the initiator.

---

[18] See footnote 16

[19] A failure and any consequential failure(s) shall be postulated to occur in any component of a safety function in connection with the initiating event or thereafter at the most unfavourable time and configuration.

[20] This means that non-safety systems are either supposed not to function after the initiator, either supposed to continue to function as before the initiator, depending on which of both cases is most penalising.

[21] This assumption is made to ensure the sufficiency of the shutdown margin. The stuck rod selected is the highest worth rod at Hot Zero Power and conservative values of reactor trip reactivity (conservative time delay and reactivity versus CR position dependence) are used. A stuck rod can be handled as single failure in the DBA-analysis if the stuck rod itself is the worst single failure.

8.6 Any failure, occurring as a consequence of a postulated initiating event, shall be regarded to be part of the original PIE.

8.7 The impact of uncertainties, which in specific cases are of importance for the results, shall be addressed in the analysis of design basis events.

9. Design of safety functions

General

9.1 The fail-safe principle shall be considered in the design of systems and components important to safety.

9.2 A failure in a system intended for normal operation shall not affect a safety function.

9.3 Activations and manoeuvring of the safety functions shall be automated or accomplished by passive means such that operator action is not necessary within 30 minutes after the initiating event. Any operator actions required by the design within 30 minutes after the initiating event shall be justified[22].

9.4 The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components[23], redundancy, diversity[24], physical and functional separation and isolation.

Reactor shutdown functions

9.5 The means for shutting down the reactor shall consist of at least two diverse systems.

9.6 At least one of the two systems shall, on its own, be capable of quickly[25] rendering the nuclear reactor sub critical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure.

Heat removal functions

9.7 Means for removing residual heat from the core after shutdown, and during and after anticipated operational occurrences and accident conditions, shall be provided taking into account the assumptions of a single failure and the loss of off-site power.

Confinement functions

9.8 A containment system shall be provided in order to ensure that any release of radioactive material to the environment in a design basis accident would be below prescribed limits. This system shall include:

- leaktight structures covering all essential parts of the primary system;
- associated systems for control of pressures and temperatures;
- features for isolation;

---

[22] The control room staff has to be given sufficient time to understand the situation and take the correct actions. Operator actions required by the design within 30 min after the initiating event have to be justified and supported by clear documented procedures that are regularly exercised in a full scope simulator.

[23] Proven by experience under similar conditions or adequately tested and qualified.

[24] The potential for common cause failure shall be considered to determine where diversity should be applied to achieve the necessary reliability.

[25] Within 4-6 seconds, i.e. scram system.

- features for the management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.

9.9 Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a design basis accident. These lines shall be fitted with at least two containment isolation valves arranged in series. Isolation valves shall be located as close to the containment as is practicable.

9.10 Each line that penetrates the containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve. This valve shall be outside the containment and located as close to the containment as practicable.

10. Instrumentation and control systems

10.1 Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment, and for obtaining any information on the plant necessary for its reliable and safe operation. Provision shall be made for automatic recording[26] of measurements of any derived parameters that are important to safety.

10.2 Instrumentation shall be adequate for measuring plant parameters and shall be environmentally qualified for the plant states concerned.

Control room

10.3 A control room shall be provided from which the plant can be safely operated in all its operational states, and from which measures can be taken to maintain the plant in a safe state or to bring it back into such a state after the onset of anticipated operational occurrences and design basis accidents.

10.4 Devices shall be provided to give in an efficient way visual and, if appropriate also audible indications of operational states and processes that have deviated from normal and could affect safety. Ergonomic factors shall be taken into account in the design of the control room. Appropriate information shall be available to the operator to monitor the effects of the automatic actions.

10.5 Special attention shall be given to identifying those events, both internal and external to the control room, which may pose a direct threat to its continued operation, and the design shall provide for reasonably practicable measures to minimize the effects of such events.

[26] By computer sampling and/or print outs.

10.6 For times when the main control room is not available, there shall be sufficient instrumentation and control equipment available, at a single location that is physically and electrically separated from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and the essential plant parameters can be monitored.

Protection system

10.7 Redundancy and independence designed into the protection system shall be sufficient at least to ensure that:

- no single failure results in loss of protection function; and
- the removal from service of any component or channel does not result in loss of the necessary minimum redundancy.

10.8 The design shall permit all aspects of functionality of the protection system, from the sensor to the input signal to the final actuator, to be tested in operation. Exceptions shall be justified.

10.9 The design of the reactor protection system shall minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operation and anticipated operational occurrences. Furthermore, the reactor protection system shall not prevent operators from taking correct actions if necessary in design basis accidents.

10.10 Computer based systems used in a protection system, shall fulfil the following requirements:

- the highest quality of and best practices for hardware and software shall be used;
- the whole development process, including control, testing and commissioning of design changes, shall be systematically documented and reviewed;
- in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken; and
- where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.

Emergency power

10.11 It shall be ensured that the emergency power supply is able to supply the necessary power to systems and components important to safety, in any operational state or in a design basis accident, on the assumption of a single failure and the coincidental loss of off-site power.

11. *Review of the design basis*

11.1 The actual design basis shall regularly[27], and when relevant as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach to identify needs and opportunities for improvement. Reasonably practicable measures shall be taken with respect to backfitting or other measures justified from a safety point of view.

Appendix

Interpretation of the reference level 5.1, for the purpose of benchmarking of implementation, in terms of types of internal events to be included in the safety analysis as a minimum:

The list mainly applies on PWR and BWR. For the other designs: AGR, CANDU and RBMK used in single WENRA countries, the list has to be adapted to the reactor type and implementation checked as self-assessment by the concerned country. The final list will in all cases be plant type specific.

Initiating events

- small, medium and large LOCA (break of the largest diameter piping of the Reactor Coolant Pressure Boundary)
- breaks in the main steam and main feed water systems
- forced decrease of reactor coolant flow
- forced increase or decrease of main feed water flow
- forced increase or decrease of main steam flow
- inadvertent opening of valves at the pressurizer (PWR)
- inadvertent operation of the emergency core cooling system ECCS
- inadvertent opening of valves at the steam generators (PWR)
- inadvertent opening of main steam relief/safety valves (BWR)
- inadvertent closure of main steam isolation valves
- steam generator tube rupture (PWR)
- uncontrolled movement of control rods
- uncontrolled withdrawal/ejection of control rod
- core instability (BWR)
- chemical and volume control system (CVCS) malfunction (PWR)
- pipe breaks or heat exchanger tube leaks in systems connected to the RCS and located partially outside containment (Interfacing System LOCA)
- fuel handling accidents

[27] Regularly is understood as an ongoing activity to analyse the plant and identify opportunities for improvement. The periodic safety reviews are complementary tools to verify and follow up on this activity in a longer perspective. Significant new safety information is understood as new insights gained from e.g. safety analyses and the development of safety standards and practices.

- loss of off-site power
- load drop by failure of lifting devices

Initiating events as well as consequential events (could be both types)

- fire
- explosion
- flooding

Consequential events

- missile generation, including turbine missiles
- release of fluid (oil etc) from failed systems
- vibration
- pipe whip
- jet impact

Appendix F	Issue: Design Extension of Existing Reactors
Document status: Final	Safety area: Design

Reference levels:

1. Objective

1.1 The design extension[28] analysis shall examine the performance of the plant in specified accidents beyond the design basis, including selected severe accidents, in order to minimise as far as reasonably practicable radioactive releases harmful to the public and the environment in cases of events with very low probability of occurrence.

2. Selection and analysis of Beyond Design Basis Events

2.1 Beyond design basis events shall be selected[29] and considered in the safety analysis to determine those sequences for which reasonable practicable preventive or mitigative measures can be identified and implemented (see Appendix for assessment of implementation).

2.2 Realistic assumptions and modified[30] acceptance criteria may be used for the analysis of the beyond design basis events.

3. Instrumentation for the management of beyond design basis accident conditions

3.1 Adequate instrumentation shall exist which can be used in severe accident environmental conditions in order to manage such accidents according to guidelines/procedures for severe accidents.

3.2 Necessary information from instruments shall be relayed to the control room as well as to a separately located supplementary control room/post and be presented in such a way

[28] Design extension is understood as measures taken to cope with additional events or combination of events, not foreseen in the design of the plant. Such measures need not involve application of conservative engineering practices but could be based on realistic, probabilistic or best estimate assumptions, methods and analytical criteria.

[29] Based on a combination of deterministic and probabilistic assessments as well as engineering judgement.

[30] Modified in relation to the conservative criteria used in the analysis of the design basis events.

to enable a timely assessment of the plant status and critical safety functions in severe accident conditions.

4. Protection of the containment against selected beyond design basis accidents[31]

4.1 Isolation of the containment shall be possible in a beyond design basis accident.[32] However, if an event leads to bypass of the containment, consequences shall be mitigated.

4.2 The leaktightness of the containment shall not degrade significantly for a reasonable time after a severe accident.

4.3 Pressure and temperature in the containment shall be managed in a severe accident.

4.4 Combustible gases shall be managed in a severe accident.

4.5 The containment shall be protected from overpressure in a severe accident[33].

4.6 High pressure core melt scenarios shall be prevented.

4.7 Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.

Appendix

Interpretation of the reference level 2.1, for the purpose of benchmarking of implementation, in terms of types events to be analysed for design extension as a minimum, if not already considered in the design basis:

- anticipated transient without scram (ATWS)
- station black out
- total loss of feed water
- LOCA together with the complete loss of one emergency core cooling system[34]
- uncontrolled level drop during mid-loop operation (PWR) or during refuelling
- total loss of the component cooling water system
- loss of core cooling in the residual heat removal mode
- loss of fuel pool cooling
- loss of ultimate heat sink function
- uncontrolled boron dilution (PWR)
- multiple steam generator tube ruptures (PWR, PHWR)
- loss of required safety systems in the long term after a Postulated Initiating Event

---

[31] These reference levels aim at providing protection at the level 4 of the defence-in-depth. Such protection could be provided by existing equipment that has been assessed, and if needed modified, to perform the relevant function in a severe accident condition or additional equipment on a best estimate basis.

[32] Special attention needs to be given for certain reactor types to the analysis of severe accident conditions with an open containment during certain shutdown states. Should such an accident occur, it should be possible to achieve timely containment isolation or implement equally effective compensatory measures. Therefore consideration has to be given to the time needed for the restoration of containment isolation and effective leaktightness, taking into account factors such as the progression of the accident sequences.

[33] This reference level could be seen as a special case of reference level 4.3. However, it is kept for clarity as a separate reference level since it might call for specific measures to protect against fast as well as slow containment overpressurization.

[34] Either the high pressure or the low pressure emergency core cooling system

Issue G: Safety Classification of Structures, Systems and Components	
Document status: Final	Safety area: Design

Reference levels

1. Objective

1.1 All SSCs[35] important for safety shall be identified and classified on the basis of their importance for safety.

2. Classification process

2.1 The classification of SSCs shall be primarily based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment.

2.2 The classification shall identify for each safety class:

- The appropriate codes and standards in design, manufacturing, construction and inspection;
- Need for emergency power supply, qualification to environmental conditions;
- The availability or unavailability status of systems serving the safety functions to be considered in deterministic safety analysis;
- The quality management provisions.

3. Ensuring reliability

3.1 SSCs important to safety shall be designed, constructed and maintained such that their quality and reliability is commensurate with their classification.

3.2 The failure of a SSC in one safety class shall not cause the failure of other SSCs in a higher safety class. Auxiliary systems supporting equipment important to safety shall be classified accordingly.

4. Selection of materials and qualification of equipment

4.1 The design of SSCs important to safety and the materials used shall consider the effects of operational conditions over the plant lifetime and the effects of design basis accidents on their characteristics and performance.

[35] SSCs include software for I&C.

4.2 A qualification procedure shall be adopted to confirm that SSCs important to safety meet throughout their design operational lives the demands for performing their function, taking into account environmental conditions[36] over the lifetime of the plant and when required in anticipated operational occurrences and accident conditions.

[36] Environmental conditions include as appropriate vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity, and combinations thereof.

Issue H: Operational limits and conditions	
Document status: Final	Safety area: Operation

Reference levels

1. Purpose

1.1 OLCs shall be developed to ensure that plants are operated in accordance with design assumptions and intentions as documented in the SAR.

1.2 The OLCs shall define the conditions that must be met to prevent situations that might lead to accidents or to mitigate the consequences of accidents should they occur.

2. Establishment and review of OLCs

2.1 Each established OLC shall be justified based on plant design, safety analysis and commissioning tests.

2.2 OLCs shall be kept updated and reviewed in the light of experience, developments in science and technology, and every time modifications in the plant or in the safety analysis warrant it, and changed if necessary.

2.3 The process for making modifications or temporary modifications of OLCs shall be defined. Such modifications shall be adequately justified by safety analysis and independent safety review.

3. Use of OLCs

3.1 The OLCs shall be readily accessible to control room personnel.

3.2 Control room operators shall be highly knowledgeable of the OLCs and their technical basis. Relevant operational decision makers shall be aware of their significance for the safety of the plant.

4. Scope of OLCs

4.1 OLCs shall cover all operational plant states including power operation, shutdown and refuelling, any intermediate conditions between these states and temporary situations arising due to maintenance & testing.

5. Safety limits, safety systems settings and operational limits

5.1 Adequate margins shall be ensured between operational limits and the established safety systems settings, to avoid undesirably frequent actuation of safety systems.

5.2 Safety limits shall be established using a conservative approach to take uncertainties in the safety analyses into account.

6. Unavailability limits

6.1 Limits and conditions for normal operation shall include limits on operating parameters, stipulation for minimum amount of operable equipment, actions to be taken by the operating staff in the event of deviations from the OLCs and time allowed to complete these actions.

6.2 Where operability requirements cannot be met, the actions to bring the plant to a safer state shall be specified, and the time allowed to complete the action shall be stated.

6.3 Operability requirements shall state for the various modes of normal operation the number of systems or components important to safety that should be in operating condition or standby condition.

7. Unconditional requirements

7.1 If operating personnel cannot ascertain that the power plant is operating within operating limits, or the plant behaves in an unexpected way, measures shall be taken without delay to bring the plant to a safe and stable state.

7.2 Plant shall not be returned to service following unplanned shutdown until it has been shown to be safe to do so.

8. Staffing levels

8.1 Minimum staffing levels for shift staff shall be stated in the OLCs.

9. Surveillance

9.1 The licensee shall ensure that an appropriate surveillance[37] program is established and implemented to ensure compliance with OLCs and shall ensure that results are evaluated and retained.

10. Non-compliance

10.1 In cases of non-compliance, remedial actions shall be taken immediately to re-establish OLC requirements.

10.2 Reports of non-compliance shall be investigated and corrective action shall be implemented in order to help prevent such non-compliance[38] in future.

---

[37] The objectives of the surveillance programme are: to maintain and improve equipment availability, to confirm compliance with operational limits and conditions, and to detect and correct any abnormal condition before it can give rise to significant consequences for safety. The abnormal conditions which are of relevance to the surveillance programme include not only deficiencies in SSCs and software performance, procedural errors and human errors, but also trends within the accepted limits, an analysis of which may indicate that the plant is deviating from the design intent. *(NS-G-2.6 Para 2.11)*

[38] If the actions taken to correct a deviation from OLCs are not as prescribed, including those times when they have not been completed successfully in the allowable outage time, plant shall be deemed to have operated in non-compliance with OLCs.

Issue I: Ageing Management	
Document status: Final	Safety area: Operation

Reference levels

1. Objective

1.1. The operating organisation shall have an Ageing Management Programme[39] to identify all ageing mechanisms important to safety related structures, systems and components (SSCs), determine their possible consequences, and determine necessary activities in order to maintain the operability and reliability of these SSCs.

2. Technical requirements, methods and procedures

2.1 The licensee shall assess structures, systems and components important to safety taking into account of relevant ageing and wear-out mechanisms and potential age related degradations in order to ensure the capability of the plant to perform the necessary safety functions throughout its planned life, under design basis conditions.

2.2 The licensee shall provide monitoring, testing, sampling and inspection activities to assess ageing effects to identify unexpected behaviour or degradation during service.

2.3. The Periodic Safety Reviews shall be used to confirm whether ageing and wear-out mechanisms have been correctly taken into account and to detect unexpected issues.

2.4. In its AMP, the licensee shall take account of environmental conditions, process conditions, duty cycles, maintenance schedules, service life, testing schedules and replacement strategy.

2.5. The AMP shall be reviewed and updated as a minimum with the PSR, in order to incorporate new information as it becomes available, to address new issues as they arise, to use more sophisticated tools and methods as they become accessible and to assess the performance of maintenance practices considered over the life of the plant.

3. Major structures and components

3.1. Ageing management of the reactor pressure vessel[40] and its welds shall take all relevant factors including embrittlement, thermal ageing, and fatigue into account to compare their performance with prediction, throughout plant life.

3.2. Surveillance of major structures and components shall be carried out to timely detect the inception of ageing effects and to allow for preventive and remedial actions.

---

[39] **Ageing** is considered as a process by which the physical characteristics of a structure, system or component (SSC) change with time (ageing) or use (wear-out).
An Ageing Management Programme (AMP) should be understood as an integrated approach to identifying, analysing, monitoring and taking corrective actions and document the ageing degradation of structures, systems and components.

[40] Or its functional equivalent in other designs

Issue J: System for Investigation of Events and Operational Experience Feedback	
Document status: Final	Safety area: Operation

Reference levels

1. Programmes and Responsibilities

1.1 The licensee shall establish and conduct a programme to collect, screen, analyse, and document operating experience and events at the plant in a systematic way. Relevant operational experience and events reported by other plants shall also be considered.

1.2 Operating experience at the plant shall be evaluated to identify any latent safety relevant failures or potential precursors and possible tendencies towards degraded safety performance or reduction in safety margin.

1.3 The licensee shall designate staff for carrying out these programmes, for the dissemination of findings important to safety and – where appropriate – for recommendations on actions to be taken. Significant findings and trends shall be reported to the licensee's top management.

1.4 Staff responsible for evaluation of operational experience and investigation into events shall receive adequate training, resources, and support from the line management.

1.5 The licensee shall ensure that results are obtained, that conclusions are drawn, measures are taken, good practices are considered and that timely and appropriate corrective actions are implemented to prevent recurrence and to counteract developments adverse to safety.

2. Collection and storage of information

2.1 The information relevant to experience from normal and abnormal operation and other important safety-related information shall be organized, documented, and stored in such a way that it can be easily retrieved and systematically searched, screened and assessed by the designated staff.

3. Reporting and dissemination of safety significant information

3.1 The licensee shall report incidents and abnormal events of significance to safety in accordance with established procedures and criteria.

3.2 Plant personnel shall be required to report abnormal events and be encouraged to report internally near misses relevant to the safety of the plant.

3.3 Information resulting from the operational experience shall be disseminated to relevant staff and shared with relevant national and international bodies.

3.4 A process shall be put in place to ensure that operating experience of events at the plant concerned as well as of relevant events at other plants is appropriately considered in the training programme for staff with tasks related to safety.

4. Assessment and investigation of events

4.1 An initial assessment of events important to safety shall be performed without delay to determine whether urgent actions are necessary.

4.2 The licensee shall have procedures specifying appropriate investigation methods, including methods of human performance analysis.

4.3 Event investigation shall be conducted on a time schedule consistent with the event significance. The investigation shall:

- Establish the complete event sequence;
- Determine the deviation;
- Include direct and root cause analysis;
- Assess the safety significance including potential consequences; and
- Identify corrective actions.

4.4 The operating organisation shall maintain liaison as appropriate with the organizations (manufacturer, research organization, designer) involved in design and construction, with the aims of feeding back information on operating experience and obtaining advice, if necessary, in case of equipment failures or abnormal events.

4.5 As a result of the analysis, timely corrective actions shall be taken such as technical modifications, administrative measures or personnel training to restore safety, to avoid event recurrence and where appropriate to improve safety.

5. Review and continuous improvement of the OEF process

5.1 Periodic reviews of the effectiveness of the OEF process based on performance criteria shall be undertaken and documented either within a self-assessment programme by the licensee or by a peer review team.

Issue K: Maintenance, in-service inspection and functional testing	
Document status: Final	Safety area: Operation

Reference levels

1. Scope and objectives

1.1 The licensee shall prepare and implement documented programmes of maintenance, testing, surveillance, and inspection of SSCs important to safety to ensure that their availability, reliability, and functionality remain in accordance with the design over the lifetime of the plant. They shall take into account operational limits and conditions and be re-evaluated in the light of experience.

1.2 The programmes shall include periodic inspections and tests of SSCs important to safety in order to determine whether they are acceptable for continued safe operation of the plant or whether any remedial measures are necessary.

2. Programme establishment and review

2.1 The extent and frequency of preventive maintenance, testing, surveillance and inspection of SSCs shall be determined through a systematic approach on the basis of:

Their importance to safety;
Their inherent reliability;
Their potential for degradation (based on operating experience, research and vendor recommendation);
Operational and other relevant experience and results of condition monitoring.

2.2 In-service inspections of nuclear power plants shall be carried out at intervals whose length shall be chosen in order to ensure that any deterioration of the most exposed component is detected before it can lead to failure.

2.3 Data on maintenance, testing, surveillance, and inspection of SSCs shall be recorded, stored and analysed. Such records shall be reviewed to look for evidence of incipient and recurring failures, to initiate corrective maintenance and review the preventive maintenance programme accordingly.

2.4 The maintenance programme shall be periodically reviewed[41] in light of operating experience, and any proposed changes to the programme shall be assessed to analyse their effects on system availability, their impact on plant safety, and their conformance with applicable requirements.

2.5 The potential impact of maintenance upon plant safety shall be assessed.

[41] It is anticipated that such reviews are carried out more frequently than the 10-yearly Periodic Safety Reviews.

3. Implementation

3.1 SSCs important to safety shall be designed to be tested, maintained, repaired and inspected or monitored periodically in terms of integrity and functional capability over the lifetime of the plant, without undue risk to workers and significant reduction in system availability. Where such provisions cannot be attained, proven alternative or indirect methods shall be specified and adequate safety precautions taken to compensate for potential undiscovered failures.

3.2 Procedures shall be established, reviewed, and validated for maintenance, testing, surveillance and inspection tasks.

3.3 A comprehensive work planning and control system shall be implemented to ensure that maintenance, testing, surveillance and inspection work is properly authorized and carried out according to the procedures.

3.4 Before equipment is removed from or returned to service, full consideration and approval of the proposed reconfiguration shall be ensured, followed by a documented confirmation of its correct configuration and, where appropriate, functional testing.

3.5 The actions to be taken in response to deviations from the acceptance criteria in the maintenance, testing, surveillance and inspection tasks, shall be defined in the procedures.

3.6 Repairs to SSCs shall be devised, authorized, and carried out as promptly as practicable. Priorities shall be established with account taken first of the relative importance to safety of the defective structure, system, or component.

3.7 Following any abnormal event due to which the safety functions and functional integrity of any component or system may have been challenged, the licensee shall identify and revalidate the safety functions and carry out any necessary remedial actions, including inspection, testing, maintenance, and repair, as appropriate.

3.8 The reactor coolant pressure boundary shall be subject to a system leakage test before resuming operation after a reactor outage in the course of which its leak-tightness may been affected.

3.9 The reactor coolant pressure boundary shall be subject to a system pressure test at or near the end of each major inspection interval.

3.10 All items of equipment used for examinations and tests together with their accessories shall be qualified and calibrated before they are used. All equipment shall be properly identified in the calibration records, and the validity of the calibration shall be regularly verified by the licensee in accordance with the quality management system.

3.11 Any in-service inspection process shall be qualified[42], in terms of required inspection area(s), method(s) of non-destructive testing, defects being sought and required effectiveness of inspections.

3.12 When a detected flaw that exceeds the acceptance criteria is found in a sample, additional examinations shall be performed to investigate the specific problem area in the analysis of additional analogous components (or areas). The extent of further examinations shall

[42] The ISI system qualification means to demonstrate that the combination of equipment, inspection procedure and personnel is appropriate for testing of a given inspection area according to a technical specification. It is recommended to uses as reference documents, eg the European Regulators Common Position on NDT Qualification, ENIQ methodology and/or IAEA – EBP-VVER-11 documents.

be decided with due regard for the nature of the flaw and degree to which it affects the nuclear safety assessments for the plant or component and the potential consequences.

3.13 Surveillance measures to verify the containment integrity shall include: a) leak rate tests; b) tests of penetration seals and closure devices such as air locks and valves that are part of the boundaries, to demonstrate their leak-tightness and, where appropriate, their operability; c) inspections for structural integrity (such as those performed on liner and pre-stressing tendons).

Issue LM: Emergency Operating Procedures and Severe Accident Management Guidelines	
Document status: Final	Safety area: Operation

Reference levels

1. Objectives

1.1 A comprehensive set of emergency operating procedures (EOPs) for design basis accidents (DBAs) and beyond design basis accidents (BDBAs), and also guidelines for severe accident management (SAMG) shall be provided.

2. Scope

2.1 EOPs shall be provided to cover Design Basis Accidents. These EOPs shall provide instructions for recovering the plant state to a safe condition.

2.2 EOPs shall be provided to cover Beyond Design Basis Accidents up to, but not including, the onset of core damage. The aim shall be to re-establish or compensate for lost safety functions and to set out actions to prevent core damage.

2.3 SAMGs shall be provided to mitigate the consequences of severe accidents for the cases where the measures provided by EOPs have not been successful in the prevention of core damage.

2.4 EOPs for Design Basis Accidents shall be symptom-based or a combination of symptom based and event based[43] procedures. EOPs for Beyond Design Basis Accidents shall be only symptom based.

3. Format and Content of Procedures and Guidelines

3.1 EOPs shall be developed in a systematic way and shall be supported by realistic and plant specific analysis performed for this purpose. EOPs shall be consistent with other operational procedures, such as alarm response procedures and severe accident management guidelines.

3.2 EOPs shall enable the operator to recognise quickly the accident condition to which it applies. Entry and exit conditions shall be defined in the EOPs to enable operators to select the appropriate EOP, to navigate among EOPs and to proceed from EOPs to SAMGs.

---

[43] Event-based EOPs enable the operator to identify the specific event and encompass:
- Information from significant plant parameters,
- Automatic actions that will probably be taken as a result of the event,
- Subsequent operator actions directed to returning the reactor to a normal condition or to provide for safe, extended and stable shutdown conditions.

Symptom-based EOPs enable the operator to respond to situations for which there are no procedures to identify accurately the event that has occurred. The decisions for measures to respond to such situations are specified in the procedures with respect to the symptoms and the state of systems of the plant (such as the values of safety parameters and critical safety functions).

3.3 SAMGs shall be developed in a systematic way using a plant specific approach. SAMGs shall address strategies to cope with scenarios identified by the severe accident analyses[44].

4. Verification and validation

4.1 EOPs and SAMGs shall be verified and validated in the form in which they will be used in the field, so far as practicable, to ensure that they are administratively and technically correct for the plant and are compatible with the environment in which they will be used.

4.2 The approach used for plant-specific validation and verification shall be documented. The effectiveness of incorporating human factors engineering principles in procedures and guidelines shall be judged when validating them. The validation of EOPs shall be based on representative simulations, using a simulator, where appropriate.

5. Review and updating of EOPs and SAMGs

5.1 EOPs and SAMGs shall be kept updated to ensure that they remain fit for their purpose.

6. Training

6.1 Shift personnel and on-site technical support shall be regularly trained and exercised, using simulators for the EOPs and, where practicable, for the SAMGs.

6.2 The transition from EOPs to SAMGs for management of severe accidents shall be exercised.

6.3 Interventions called for in SAMGs and needed to restore necessary safety functions shall be planned for and regularly exercised.

[44] Analysis aimed at identifying the plant vulnerabilities to severe accident phenomena, assessment of plant capabilities and development of accident management measures, including for containment protection as defined in Issue F (Design Extension of Existing Reactors) in RLs 4.1 to 4.7. It is understood that for these accident conditions also SAMGs shall be developed.

Issue N: Contents and updating of Safety Analysis Report (SAR)	
Document status: Final	Safety area: Safety Verification

Reference levels

1. Objective

1.1 The Licensee shall provide a SAR[45] and use it as a basis for continuous support of safe operation.

1.2 The Licensee shall use the SAR as a basis for assessing the safety implications of changes to the plant or to operating practices.

2. Content of the SAR

2.1 The SAR shall describe the site, the plant layout and normal operation; and demonstrate how safety is achieved.

2.2 The SAR shall contain detailed descriptions of the safety functions; all safety systems and safety-related structures, systems and components; their design basis and functioning in all operational states, including shut down and accident conditions.

2.3 The SAR shall identify applicable regulations codes and standards.

2.4 The SAR shall describe the relevant aspects of the plant organization and the management of safety.

2.5 The SAR shall contain the evaluation of the safety aspects related to the site.

2.6 The SAR shall outline the general design concept and the approach adopted to meet the fundamental safety objectives.

2.7 The SAR shall describe the safety analyses performed to assess the safety of the plant in response to postulated initiating events against safety criteria and radiological release limits.

2.8 The SAR shall describe the emergency operation procedures and accident management guidelines, the inspection and testing provisions, the qualification, and training of personnel, the operational experience feedback programme, and the management of ageing.

2.9 The SAR shall contain the technical bases for the operational limits and conditions.

2.10 The SAR shall describe the policy, strategy, methods, and provisions for radiation protection.

2.11 The SAR shall describe the on-site emergency preparedness arrangements and the liaison and co-ordination with off-site organizations involved in the response to an emergency.

[45] A consistent safety document or integrated set of documents constituting the licensing basis of the plant and updated under control of the regulatory body

2.12 The SAR shall describe the on-site radioactive waste management provisions.

2.13 The SAR shall describe how the relevant decommissioning and end-of-life aspects are taken into account during operation.[46]

3. Review and update of the SAR

3.1 The licensee shall update the SAR to reflect modifications, new regulatory requirements, and relevant standards, as soon as practicable after the new information is available and applicable.

[46] Guidance on the specific aspects that need to be addressed in the SAR is given in Chapter XV of the IAEA Safety Guide GS-G-4.1.

Issue O: Probabilistic Safety Analysis (PSA)	
Document status: Final	Safety area: Safety Verification

Reference levels

1. Scope and content of PSA

1.1 For each plant design, a specific PSA shall be developed for level 1 and level 2 including all modes of operation and all relevant initiating events including internal fire and flooding. Severe weather conditions and seismic events shall be addressed[47].

1.2 PSA shall include relevant dependencies[48].

1.3 The basic Level 1 and Level 2 PSAs shall contain uncertainty and sensitivity analyses.

1.4 PSA shall be based on a realistic modelling of plant response, using data relevant for the design, and taking into account human action to the extent assumed in operating and accident procedures.

1.5 Human reliability analysis shall be performed, taking into account the factors which can influence the performance of the operators in all plant states.

2. Quality of PSA

2.1 PSA shall be performed, documented, and maintained according to the quality management system of the licensee.

2.2 PSA shall be performed according to an up to date proven methodology, taking into account international experience currently available.

3. Use of PSA

3.1 PSA shall be used to support safety management. The role of PSA in the decision making process shall be defined.

3.2 PSA shall be used[49] to identify the need for modifications to the plant and its procedures, including for severe accident management measures, in order to reduce the risk from the plant.

3.3 PSA shall be used to assess the overall risk from the plant, to demonstrate that a balanced design has been achieved, and to provide confidence that there are no "cliff-edge effects"[50].

---

[47] This means that these two hazards shall be included in the PSA, except if a justification is provided for not including them, based on site-specific arguments on these hazards or on sufficient conservative coverage through deterministic analyses in the design, so that their omission from the PSA does not weaken the overall risk assessment of the plant.

[48] Such as functional dependencies, area dependencies (based on the physical location of the components) and other common cause failures

[49] It is intended that such analyses will be done on a continuous basis, not just every ten years during the Periodic Safety Review.

3.4 PSA shall be used to assess the adequacy of plant modifications, changes to operational limits and conditions and procedures and to assess the significance of operational occurrences.

3.5 Insights from PSA shall be used as input to development and validation of the safety significant training programmes of the licensee, including simulator training of control room operators.

3.6 The results of PSA shall be used to ensure that the items are included in the verification and test programmes if they contribute significantly to risk.

4. Demands and conditions on the use of PSA

4.1 The limitations of PSA shall be understood, recognized and taken into account in all its use. The adequacy of a particular PSA application shall always be checked with respect to these limitations.

4.2 When PSA is used, for evaluating or changing the requirements on periodic testing and allowed outage time for a system or a component, all relevant items, including states of systems and components and safety functions they participate in, shall be included in the analysis.

4.3 The operability of components that have been found by PSA to be important to safety shall be ensured and their role shall be recorded in the SAR.

[50] Small deviations in the plant parameters that could give rise to severely abnormal plant behaviour.

Issue P: Periodic Safety Review (PSR)	
Document status: Final	Safety area: Safety Verification

Reference levels

1. Objective of the periodic safety review

1.1 The licensee shall have the prime responsibility for performing the Periodic Safety Review.

1.2 The review shall confirm the compliance of the plant with its licensing basis and any deviations shall be resolved.

1.3 The review shall identify and evaluate the safety significance of deviations from applicable current safety standards and internationally recognised good practices currently available.

1.4 All reasonably practicable improvement measures shall be taken by the licensee as a result of the review.

1.5 An overall assessment of the safety of the plant shall be provided, and adequate confidence in plant safety for continued operation demonstrated, based on the results of the review in each area.

2. Scope of the periodic safety review

2.1 The review shall be made periodically, at least every ten years.

2.2 The scope of the review shall be clearly defined and justified. The scope shall be as comprehensive as reasonably practical with regard to significant safety aspects of an operating plant and, as a minimum the following areas shall be covered by the review:

- Plant design as built and actual condition of systems, structures and components;
- Safety analyses and their use;
- Operating experience during the review period and the effectiveness of the system used for experience feed-back;
- Organisational arrangements;
- Staffing and qualification of staff;
- Emergency preparedness; and
- Radiological impact on the environment.

3. Methodology of the periodic safety review

3.1 The review shall use an up to date, systematic, and documented methodology, taking into account deterministic as well as probabilistic assessments.

3.2 Each area shall be reviewed and the findings compared to the licensing requirements as well as to current safety standards and practices.

Issue Q: Plant modifications	
Document status: Final	Safety area: Operation

Reference levels

1. Purpose and scope

1.1 The licensee shall ensure that no modification to a nuclear power plant, whatever the reason for it, degrades the plant's ability to be operated safely.[51]

1.2 The licensee shall control plant modifications using a graded approach with appropriate criteria for categorization according to their safety significance[52].

2. Procedure for dealing with plant modifications

2.1 The licensee shall establish a process to ensure that all permanent and temporary modifications are properly designed, reviewed, controlled, and implemented, and that all relevant safety requirements are met.

2.2 For modifications to SSC, this process shall include the following:

- Reason and justification for modification;
- Design;
- Safety assessment;
- Updating plant documentation and training;
- Fabrication, installation and testing; and
- Commissioning the modification.

3. Requirements on safety assessment and review of modifications

3.1 An initial safety assessment shall be carried out to determine any consequences for safety[53].

3.2 A detailed, comprehensive safety assessment shall be undertaken, unless the results of the initial safety assessment show that the scope of this assessment can be reduced.

3.3 Comprehensive safety assessments shall demonstrate all applicable safety aspects are considered and that the system specifications and the relevant safety requirements are met.

---

[51] RL 2.2 specifically addresses modifications to SSCs, all other reference levels relate to all type of modifications in the sense of IAEA NS-R-2, Para 7.1

[52] Para 4.5 of IAEA Guide NS-G-2.3 contains information about possible categories.

[53] This assessment is performed for the purpose of categorizing the intended modification according to its safety significance.

3.4 The scope, safety implications, and consequences of proposed modifications shall be reviewed by personnel not immediately involved in their design or implementation.

4. Implementation of modifications

4.1 Implementation and testing of plant modifications shall be performed in accordance with the applicable work control and plant testing procedures.

4.2 The impact upon procedures, training, and provisions for plant simulators shall be assessed and any appropriate revisions incorporated.

4.3 Before commissioning modified plant or putting plant back into operation after modification, personnel shall have been trained, as appropriate, and all relevant documents necessary for plant operation shall have been updated.

5. Temporary modifications[54]

5.1 All temporary modifications shall be clearly identified at the point of application and at any relevant control position[55]. Operating personnel shall be clearly informed of these modifications and of their consequences for the operation of the plant.

5.2 Temporary modifications shall be managed according to specific plant procedures.

5.3 The number of simultaneous temporary modifications shall be kept to a minimum. The duration of a temporary modification shall be limited.

5.4 The licensee shall periodically review outstanding temporary modifications to determine whether they are still needed.

---

[54] Examples of temporary modifications are temporary bypass lines, electrical jumpers, lifted electrical leads, temporary trip point settings, temporary blank flanges and temporary defeats of interlocks. This category of modifications also includes temporary constructions and installations used for maintenance of the design basis configuration of the plant in emergencies or other unanticipated situations. Temporary modifications in some cases may be made as an intermediate stage in making permanent modifications. IAEA Guide NS-G-2.3, Para 6.1

[55] By relevant control position it is meant any control point important for the modified system and also any administrative aspect related to the system in which the temporary modification has been implemented.

Issue R: On-site Emergency Preparedness	
Document status: Final	Safety area: Emergency Preparedness

Reference levels

1. Objective

1.1 The licensee shall provide arrangements for responding effectively to events requiring protective measures at the scene for:

(a) Regaining control of any emergency arising at their site, including events related to combinations of non-nuclear and nuclear hazards;

(b) Preventing or mitigating the consequences at the scene of any such emergency: and

(c) Co-operating with external emergency response organizations in preventing adverse health effects in workers and the public.

2. Emergency Preparedness and Response Plan

2.1 The licensee shall prepare an on-site emergency plan and establish the necessary organizational structure for clear allocation of responsibilities, authorities, and arrangements for co-ordinating plant activities and co-operating with external response agencies throughout all phases of an emergency.

2.2 The licensee shall provide for:

(a) Prompt recognition and classification of emergencies;

(b) Timely notification and alerting of response personnel;

(c) Ensuring the safety of all persons present on the site, including the protection of the emergency workers;

(d) Informing the authorities and the public, including timely notification and subsequent provision of information as required;

(e) Performing assessments of the situation on the technical, & radiological points of view (on and off site);

(f) Monitoring radioactive releases;

(g) Treatment and first aid of a limited number of contaminated and/or overexposed workers/persons on site; and

(h) Plant management and damage control[56].

2.3 The site emergency plan shall be based upon an assessment of reasonably foreseeable events and situations that may require protective measures on- or off-site. The plan shall

[56] Understood as urgent mitigatory repairs, controls, and other actions that are carried out, primarily at the site, while the emergency is still in progress.

also be co-ordinated with all other involved bodies and capable of extension should more improbable, severe events occur.

3. Organization

3.1 The licensee shall have people on-site at all times with the authority and responsibilities to classify and declare an emergency and, upon classification, to initiate promptly the appropriate on-site response[57].

3.2 Sufficient numbers of qualified personnel shall be available at all times for staffing appropriate positions promptly following the declaration and notification of an emergency.

3.3 Arrangements shall be made to provide technical assistance to operational staff. Teams for mitigating the consequences of an emergency (e.g. radiation protection, damage control, fire fighting, etc) shall be available.

3.4 Arrangements shall be made to alert off-site responsible authorities promptly.

3.5 The licensee shall identify those who are authorized to carry out the response functions assigned in the emergency plan.

4. Facilities and equipment

4.1 Appropriate emergency facilities shall be designated for responding to events on site and that will provide co-ordination of off-site monitoring and assessment throughout different phases of an emergency response.

4.2 An "On-site Emergency Control Centre", separated from the plant control room, shall be provided for on-site emergency management staff. Important information shall be available in the control centre about the plant and radiological conditions on and around the site. The centre shall have means of communicating with the control room, any supplementary control room, other important points on site, and with the on-site and off-site emergency response organizations[58].

4.3 Emergency facilities shall be suitably located and protected to enable the exposure of emergency workers to be controlled. Appropriate measures shall be taken to protect those occupying emergency facilities for a protracted time from hazards resulting from accidents[59].

4.4 Instruments, tools, equipment, documentation, and communication systems for use in emergencies shall be kept available and tested sufficiently frequently to demonstrate that they are in good working condition where they are unlikely to be affected by postulated accidents.

---

[57] The on duty shift supervisor could be among those authorised to declare an emergency and to initiate the appropriate on-site response.

[58] The *On-site Emergency Control Centre* is the office accommodation and associated office services set aside on or near to the site for staff who are brought together to provide technical support the Operations staff during an emergency. It may have plant information systems available, but is not expected to have any plant controls.

[59] This refers, primarily, to ensuring that the *On-site Emergency Control Centre* and other locations where staff are expected to spend a significant time are located somewhere that the staff can reach and work throughout an extended emergency with minimum risk to health. This will require location away from areas that are likely to be damaged of affected by radiation fields and, where appropriate, this will include provision of recirculatory air conditioning and continuous radiation monitoring systems.

5. Training, drills and exercises

5.1 Arrangements shall be made to identify the knowledge, skills, and abilities needed for personnel to perform their assigned response functions.

5.2 Arrangements shall be made to inform all employees and all other persons present on the site of the actions to be taken in the event of an emergency.

5.3 Training arrangements shall include basic emergency training and ongoing refresher training on an appropriate schedule and shall ensure that emergency response personnel meet the training obligations.

5.4 The site emergency plan shall be exercised at least annually. Some exercises shall be integrated to include as many as possible of the off-site organizations concerned.

5.5 Emergency exercises shall be evaluated systematically, and the emergency preparedness arrangements and the plan shall be subject to review and updating in the light of experience gained.

Issue S: Protection against internal fires	
Document status: Final	Safety area: Emergency Preparedness

Reference levels

1. Fire safety objectives

1.1 The licensee shall implement the defence in depth principle to fire protection, providing measures to prevent fires from starting, to detect and extinguish quickly any fires that do start and to prevent the spread of fires and their effects in or to any area that may affect safety[60].

2. Basic design principles

2.1 SSCs important to safety shall be designed and located so as to minimize the frequency and the effects of fire and to maintain capability for shutdown, residual heat removal, confinement of radioactive material and monitoring of plant state during and after a fire event.

2.2 Buildings that contain equipment that is important to safety shall be designed as fire resistant, subdivided into compartments that segregate such items from fire loads and segregate redundant safety systems from each other[61]. When a fire compartment approach is not practicable, fire cells shall be used[62], providing a balance between passive and active means, as justified by fire hazard analysis.

2.3 Buildings that contain radioactive materials that could cause radioactive releases in case of fire shall be designed to minimize such releases.

2.4 Access and escape routes for fire fighting and operating personnel shall be available.

3. Fire hazard analysis

3.1 A fire hazard analysis shall be carried out and kept updated to demonstrate that the fire safety objectives are met, that the fire design principles are satisfied, that the fire protection measures are appropriately designed and that any necessary administrative provisions are properly identified.

3.2 The fire hazard analysis shall be developed on a deterministic basis, covering at least:

---

[60] In this context, safety refers to all sources of nuclear safety risk, including radioactive waste facilities.

[61] A fire compartment is a building or part of building that is completely surrounded by fire resistant barriers of sufficient rating so that a total combustion of the fire load can occur without breaching the barriers. (Barriers comprise doors, walls, floors and ceilings.) The fire resistance rating of the barriers must be sufficiently high so that the total combustion of the fire load in the compartment can occur without breaching the barriers.

[62] In the fire cell approach the spread of fire is avoided by substituting the fire resistant barriers primarily with other passive provisions (e.g. distance, thermal insulation, etc.), that take into account all physical and chemical phenomena that can lead to propagation. Provision of active measures (e.g. fire extinguishing systems) may also be needed in order to achieve a satisfactory level of protection. The achievement of a satisfactory level of protection is demonstrated by the results of the fire hazard analysis.

- For all normal operating and shutdown states, a single fire and consequential spread, anywhere that there is fixed or transient combustible material;
- Consideration of credible combination of fire and other PIEs likely to occur independently of a fire.

3.3 The fire hazard analysis shall demonstrate how the possible consequential effects of fire and extinguishing systems operation have been taken into account.

3.4 The fire hazard analysis shall be complemented by probabilistic fire analysis. In PSA level 1, the fires shall be assessed in order to evaluate the fire protection arrangements and to identify risks caused by fires.

4. Fire protection systems

4.1 Each fire compartment or fire cell shall be equipped with fire detection and alarm features, with detailed annunciation for the control room staff of the location of a fire. These features shall be provided with non-interruptible emergency power supplies and appropriate fire resistant supply cables.

4.2 Fixed or mobile, automated or manual extinguishing systems shall be installed. They shall be designed and located so that their rupture, spurious or inadvertent operation does not significantly impair the capability of SSCs important to safety to carry out their safety functions.

4.3 The distribution loop for fire hydrants outside building and the internal standpipes shall provide adequate coverage of areas of the plant relevant to safety. The coverage shall be justified by the fire hazard analysis.

4.4 Ventilation systems shall be arranged such that each fire compartment fully fulfils its segregation purpose in case of fire.

4.5 Parts of ventilation systems (such as connecting ducts, fan rooms and filters) that are located outside fire compartments shall have the same fire resistance as the compartment or be capable of isolation from it by appropriately rated fire dampers.

5. Administrative controls and maintenance

5.1 In order to prevent fires, procedures shall be established to control and minimize the amount of combustible materials and minimize the potential ignition sources that may affect items important to safety. In order to ensure the operability of the fire protection measures, procedures shall be established and implemented. They shall include inspection, maintenance and testing of fire barriers, fire detection and extinguishing systems.

6. Fire fighting organization

6.1 The licensee shall implement adequate arrangements for controlling and ensuring fire safety, as identified by the fire hazard analysis[63]

6.2 Written emergency procedures that clearly define the responsibility and actions of staff in responding to any fire in the plant shall be established and kept up to date. A fire fighting strategy shall be developed, kept up-to date, and trained for, to cover each area

[63] Such arrangements must include nominating persons to be responsible for or have duties with respect to fire protection. The arrangements must set out the requirements for control of all activities that can have impact on fire safety, e.g. Maintenance; control of materials; training; tests and drills; modifications to layouts and systems – such as fire detection, fire extinguishing, ventilation, electrical and control systems.

in which a fire might affect items important to safety and protection of radioactive materials.

6.3 When reliance for manual fire fighting capability is placed on an offsite resource, there shall be proper coordination between the plant personnel and the off site response group, in order to ensure that the latter is familiar with the hazards of the plant.

6.4 If plant personnel are required to be involved in fire fighting, their organization, minimum staffing level, equipment, fitness requirements, and training shall be documented and their adequacy shall be confirmed by a competent person.