WENRA SAFETY REFERENCE LEVELS FOR EXISTING REACTORS

UPDATE IN RELATION TO LESSONS LEARNED FROM TEPCO FUKUSHIMA DAI-ICHI ACCIDENT

For all Issues except Issue F, the current version of the RLs (of January 2008) is written in black, and suggested additions are written in red. Where necessary, deletions are shown in red with strikethrough.

Contents

Foreword

A principal aim of the Western European Nuclear Regulators’ Association (WENRA) is to develop a harmonized approach to nuclear safety within the member countries. One of the first major achievements to this end was the publication in 2006 of a set of safety reference levels (RLs) for operating nuclear power plants (NPPs).

The RLs are agreed by the WENRA members. They reflect expected practices to be implemented in the WENRA countries. As the WENRA members have different responsibilities, the emphasis of the RLs has been on nuclear safety, primarily focussing on safety of the reactor core and spent fuel. The RLs specifically exclude nuclear security and, with a few exceptions, radiation safety.

As RLs have been established for greater harmonization within WENRA countries, the areas and issues they address were selected to cover important aspects of nuclear safety where differences in substance between WENRA countries might be expected. They do not seek to cover everything that could have an impact upon nuclear safety or to form a basis for determining the overall level of nuclear safety in operating NPPs.

Given the various regulatory regimes and range of types of plants (PWR, BWR, CANDU and gas-cooled reactors) in operation in WENRA countries, the RLs do not go into legal and technical details.

There are significant interactions between some of the issues and hence each issue should not necessarily be considered self-standing and the RLs need to be considered as a whole set.

WENRA is committed to continuous improvement of nuclear safety. To this end WENRA is committed to regularly revising the RLs when new knowledge and experience are available. In line with this policy the initial RLs were updated in 2007 and 2008. After the TEPCO Fukushima Daiichi nuclear accident, they have been further updated to take into account the lessons learned, including the insight from the EU stress tests. As a result a new issue on natural hazards was developed and significant changes made to several existing issues.

By issuing the revised RLs WENRA aims at further convergence of national requirements and safety improvements at NPPs in WENRA member countries, as necessary.

For further information, several documents on the WENRA website describe the basis used and processes followed to develop and update these RLs. In particular for the explanation of the current update the accompanying report “Updating WENRA Reference Levels for existing reactors in the light of TEPCO Fukushima Dai-ichi accident lessons learned“ was written and can also be downloaded from the WENRA website.

Issue A: Safety Policy

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.

2.3 The safety policy shall require continuous improvement of nuclear safety by means of:

- Regular[2] review of the overall safety of the nuclear power plant taking into account operating experience, safety research, and advances in science and technology;
- Timely implementation of the reasonably practicable improvements identified;
- Addressing without delay significant new information that may be relevant to the safety of the plant.

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.

[2] Regular is understood as an ongoing activity to review and analyse the plant design and operation and identify opportunities for improvement. Periodic safety review is a complementary tool to verify and follow up this activity in a longer perspective.

Issue B: Operating Organisation

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[3] 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[4] 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 timely and 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 and processes are controlled through a documented management system covering all activities, including relevant activities of vendors and contractors, which may affect the safe operation of the plant.

3. Sufficiency and competency of staff

3.1 The required number of staff for safe operation[5], 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[6] 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] The arguments shall be provided that the organisational structure supports safety and an appropriate response in emergencies.

[4] A verification that the implementation of the organisational change has accomplished its safety objectives.

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

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

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.

Issue C: Management System

1. Objectives

1.1 An integrated management system shall be established, implemented, assessed and continually improved by the licensee. The main aim of the management system shall be to achieve and enhance nuclear safety by ensuring that other demands[7] on the licensee are not considered separately from nuclear safety requirements, to help preclude their possible negative impact on nuclear safety.

2. General requirements

2.1 The application of management system requirements shall be graded so as to deploy appropriate resources, on the basis of the consideration of:

- The significance and complexity of each activity and its products;
- The hazards and the magnitude of the potential impact associated with each activity and its products;
- The possible consequences if an activity is carried out incorrectly or a product fails.

2.2 The documentation of the management system shall include the following:

- The policy statements of the licensee;
- A description of the management system;
- A description of the organisational structure of the licensee;
- A description of the functional responsibilities, accountabilities, levels of authority and interactions of those managing, performing and assessing work;
- A description of the interactions with relevant external organisations;
- A description of the processes and supporting information that explain how work is to be prepared, reviewed, carried out, recorded, assessed and improved.

2.3 The documentation of the management system shall be understandable to those who use it. Documents shall be up to date, readable, readily identifiable and available at the point of use.

3. Management commitment

3.1 The licensee shall develop the goals, strategies, plans and objectives of the organization in an integrated manner so that their collective impact on safety is understood and managed.

3.2 The licensee shall ensure that it is clear when, how and by whom decisions are to be made within the management system.[8]

3.3 The licensee shall ensure that management at all levels demonstrate its commitment to the establishment, implementation, assessment and continual improvement of the management system and shall allocate adequate resources to carry out these activities.

3.4 The licensee shall foster the involvement of all staff in the implementation and continual improvement of the management system.

[7] Examples of such demands are health, environmental, security, quality and economic requirements.
[8] With respect to operational decisions that impact on nuclear safety

4. Resources

4.1 The licensee shall determine the amount of resources[9] necessary and shall provide the resources to carry out the activities of the licensee and to establish, implement, assess and continually improve the management system.

5. Process implementation

5.1 The processes[10] that are needed to achieve the goals, provide the means to meet all requirements and deliver the products of the licensee organisation shall be identified, and their development shall be planned, implemented, assessed and continually improved. The sequence and interactions of the processes shall be determined.

5.2 The methods necessary to ensure the effectiveness of both the implementation and the control of the processes shall be determined and implemented.

5.3 Documents[11] shall be controlled. Changes to documents shall be reviewed and recorded and shall be subject to the same level of approval as the documents themselves. It shall be ensured that document users are aware of and use appropriate and correct documents.

5.4 Records shall be specified in the management system documentation and shall be controlled. All records shall, for the duration of the retention times specified for each record, be readable, complete, identifiable and easily retrievable.

5.5 The control of processes, or work performed within a process, contracted to external organizations shall be identified within the management system. The licensee shall retain overall responsibility when contracting any processes or work performed within a process.

5.6 Suppliers of products and services shall be selected on the basis of specified criteria and their performance shall be evaluated.

5.7 Purchasing requirements shall be developed and specified in procurement documents. Evidence that products meet these requirements shall be available to the licensee before the product is used.

5.8 It shall be confirmed[12] that activities and their products meet the specified requirements and shall ensure that products perform satisfactorily in service.

6. Measurement, assessment and improvement

6.1 In order to confirm the ability of the processes to achieve the intended results and to identify opportunities for improvement:

- The effectiveness of the management system shall be monitored and measured;
- The licensee shall ensure that managers carry out self-assessment of the performance of work for which they are responsible;
- Independent[13] assessments shall be conducted regularly on behalf of the licensee.

---

[9] Resources” includes individuals, infrastructure, the working environment, information and knowledge, and suppliers, as well as material and financial resources.

[10] This is not understood as a full process orientation of the management system. Also functional or organisational oriented routines and procedures could be used for certain activities together with cross cutting processes for other activities.

[11] Documents may include: policies; procedures; instructions; specifications and drawings (or representations in other media); training materials; and any other texts that describe processes, specify requirements or establish product specifications.

[12] Through inspection, testing, verification and validation activities before the acceptance, implementation, or operational use of products.

[13] By an external organisation or by an internal independent assessment unit.

6.2 An organizational unit shall be established with the responsibility for conducting independent assessments. This unit shall have sufficient authority to discharge its responsibilities. Individuals conducting independent assessments shall not assess their own work.

6.3 The licensee shall evaluate the results of the assessments and take any necessary actions, and shall record and communicate inside the organisation the decisions and the reasons for the actions.

6.4 A management system review shall be conducted at planned intervals to ensure the effectiveness of the management system.

6.5 The causes of non-conformances shall be determined and remedial actions shall be taken to prevent their recurrence.

6.6 Improvement plans shall include plans for the provision of adequate resources. Actions for improvement shall be monitored through to their completion and the effectiveness of the improvement shall be checked.

7. Safety culture

7.1 Management, at all levels in the licensee organization, shall consistently demonstrate, support, and promote attitudes and behaviours that result in an enduring and strong safety culture. This shall include ensuring that their actions discourage complacency, encourage an open reporting culture as well as a questioning and learning attitude with a readiness to challenge acts or conditions adverse to safety.

7.2 The management system shall provide the means to systematically develop, support, and promote desired and expected attitudes and behaviours that result in a strong safety culture. The adequacy and effectiveness of these means shall be assessed as part of self-assessments and management system reviews.

7.3 The licensee shall ensure that its suppliers and contractors whose operations may have a bearing on the safety of the nuclear facility comply with 7.1 and 7.2 to the appropriate extent.

Issue D: Training and Authorization of NPP Staff (Jobs with Safety Importance)

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 initial training in order to qualify for a certain position and regular 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[14].

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.[15]

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.

---

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

[15] Time includes the necessary briefings.

4. Authorization

4.1 Staff controlling changes in the operational status of the plant shall be required to hold an 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 carried out by contractor personnel on structures, systems, or components that are important to safety shall be approved and monitored by a suitably competent member of licensee's staff.

Issue E: Design Basis Envelope for Existing Reactors

1. Objective

1.1 The design basis[16] 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[17] 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 defence-in-depth concept shall be applied to provide several levels of defence including a design that provides a series of physical barriers to prevent the release of radioactive material to the environment, as well as a combination of safety features that contribute to the effectiveness of the barriers.

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 During normal operation[18], anticipated operational occurrences and design basis accidents, the plant shall be able to fulfil the ~~following~~ fundamental safety functions[19]:

- control of reactivity,
- removal of heat from the reactor core and from the spent fuel, and
- confinement of radioactive material.

~~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[20] 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.

[16] The design basis shall be reviewed and updated during the lifetime of the plant (see ref level 11.1).
[17] For further information see IAEA SSR-2/1 (2012).
[18] Normal operation includes startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.
[19] Under the conditions specified in the following paragraphs
[20] Normal operation, anticipated operational occurrences and design basis accident conditions.

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 using deterministic or probabilistic methods or a combination of both. The resulting design basis events shall be 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 internal hazards, and their consequential events, shall be taken into account in the design of the plant. The list of events shall be plant specific[21] and take account of relevant experience and analysis from other plants.

5.2 External hazards shall be taken into account in the design of the plant. In addition to natural hazards[22], the following types of ~~natural and~~ human made external ~~events~~ hazards shall as a minimum be taken into account in the design of the plant according to site specific conditions:

- ~~extreme[23] 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.

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[24] [20], 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~~ frequency.

7.2 Criteria for protection of the fuel rod integrity, including fuel temperature, Departure from Nucleate Boiling (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.

---

[21] For a listing of events commonly considered to be taken into account for design basis as a minimum, see Guidance to Issue F.

[22] See Issue T.

[23] ~~Definition of "extreme" is based on historical weather data for the site region~~

[24] ~~See footnote 17~~

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[25] 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 its function 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[26].

8.4 A stuck control rod shall be considered as an additional aggravating failure in the analysis of design basis events[27].

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

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 safety analysis shall:

(a) rely on methods, assumptions or arguments which are justified and conservative;

(b) provide assurance that uncertainties and their impact have been given adequate consideration[28];

(c) give evidence that adequate margins have been included when defining the design basis to guarantee that all the design basis events are covered;

(d) be auditable and reproducible.

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 Activation~~s~~ and ~~manoeuvring~~ control of the safety functions shall be automated or accomplished by passive means such that operator action is not necessary within 30 minutes ~~after~~ of the initiating event. Any operator actions required by the design within 30 minutes ~~after~~ of the initiating event shall be justified[29].

---

[25] 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.

[26] 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.

[27] 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.

[28] Conservative assumptions, safety factors, uncertainty and sensitivity analysis are means to address uncertainties and their impact on safety assessment.

[29] 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.

9.4 The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components[30], redundancy, diversity[31], physical and functional separation and isolation.

9.5 For sites with multiple units, appropriate independence between them shall be ensured.[32]

Reactor and fuel storage sub-criticality

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

9.7 At least one of the two systems shall, on its own, be capable of quickly[33] 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.

9.8 Sub-criticality shall be ensured and sustained:

- in the reactor after reactor shutdown during normal operation and anticipated operational occurrences, as long as needed;
- in the reactor, after a transient period (if any) following a design basis accident[34];
- for fuel storage during normal operation, anticipated operational occurrences, and design basis conditions.

Heat removal functions

9.9 Means for removing residual heat from the core after shutdown and from spent fuel storage, during and after anticipated operational occurrences and design basis accidents ~~conditions~~, shall be provided taking into account the assumptions of a single failure and the loss of off-site power.

Confinement functions

9.10 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;
- features for the management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.

9.11 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.

9.12 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.

---

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

[31] The potential for common cause failure, including common mode failure, shall be appropriately considered ~~to determine where diversity should be applied~~ to achieve the necessary reliability.

[32] The possibility of one unit supporting another could be considered as far as this is not detrimental for safety.

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

[34] Technical acceptance criteria have to be fulfilled during a transient period for which sub-criticality is not ensured.

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, the containment, and the state of the spent fuel storage. Instrumentation shall also be provided for obtaining any information on the plant necessary for its reliable and safe operation, and for determining the status of the plant in design basis accident conditions. Provision shall be made for automatic recording[35] 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 main 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 main 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 main 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.

10.6 For times when the main control room is not available, there shall be sufficient ~~instrumentation~~ monitoring and control equipment available, preferably at a single location that is physically separated, ~~and~~ electrically isolated and functionally independent ~~separated~~ from the main control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed from the reactor and spent fuel storage, and the essential plant parameters, including the conditions in the spent fuel storages, 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;

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

- 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 principle of continuous improvement[36] shall be applied to the design basis. In addition to regular review of the design basis, specific reviews shall be undertaken in response to significant operating experience and significant new information relevant to safety. All reviews of the design basis shall use both deterministic and probabilistic approaches to identify needs and opportunities for improvement.

~~The actual design basis shall regularly[37], 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 in a timely manner with respect to backfitting or other measures justified from a safety point of view.~~

~~Appendix~~

(deleted)

[36] See RL A2.3.

[37] ~~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. site evaluation, safety analyses and the development of safety standards and practices.~~

Issue F: Design Extension of Existing Reactors

REMARK: Most of the RLs in this Issue have been completely rewritten or have been largely modified. Therefore, the whole issue F has been marked in red colour, and there is no difference in colour whether the RLs are the existing or new ones.

1. Objective

1.1 As part of defence in depth, analysis of Design Extension Conditions (DEC) shall be undertaken with the objective of improvement of the safety of the nuclear power plant by identifying ways of enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis, minimising radioactive releases harmful to the public and the environment as far as reasonably practicable, and ensuring sufficient margins to "cliff-edge effects"[38].

1.2 There are two categories of DEC:

- DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved;
- DEC B with postulated severe fuel damage.

The analysis shall identify reasonably practicable provisions that can be implemented for the prevention of severe accidents. Additional efforts to this end shall be implemented for spent fuel storage with the goal that a severe accident in such storage becomes extremely unlikely to occur with a high degree of confidence.

Despite these provisions, severe accidents shall be postulated for fuel in the core and, if not extremely unlikely to occur with a high degree of confidence, for spent fuel in storage, and the analysis shall identify reasonably practicable provisions to mitigate their consequences.

2. Selection of design extension conditions

2.1 A set of DECs shall be derived and justified as representative, based on a combination of deterministic and probabilistic assessments as well as engineering judgement.

2.2 The selection process for DEC A shall consider all events and combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to accident conditions more challenging than those included in the design basis accidents. It shall cover:

- Events occurring during any possible operational states of the plant;
- Events resulting from internal or external hazards;
- Common cause failures (CCFs);
- All reactors and spent fuel storages on the site;
- Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity.

2.3 The set of category DEC B events shall be postulated and justified to cover situations, where the design capability of the plant is exceeded or where the equipment provided is assumed not to function as intended, leading to severe core damage.

---

[38] A cliff edge effect occurs when a small parameter change leads to a disproportionate and severe increase in consequences.

3. Safety analysis of design extension conditions

3.1 The DEC analysis shall:

(a) rely on methods, assumptions or arguments which are justified[39], and should not be unduly conservative;

(b) be auditable, paying particular attention where expert opinion is utilized, and take into account uncertainties and their impact;

(c) identify means or possibilities to prevent fuel damage (DEC A) and mitigate severe accidents (DEC B) by enhancing the plant's capability to withstand more challenging conditions than those considered in the design basis;

(d) evaluate potential on-site and off-site radiological consequences resulting from the DEC (given successful accident management measures);

(e) consider plant layout and location, equipment capabilities, conditions associated with the selected scenarios and feasibility of foreseen accident management actions;

(f) demonstrate sufficient margins to "cliff-edge effects";

(g) reflect insights from PSA level 1 and 2;

(h) take into account severe accident phenomena, where relevant;

(i) define an end state, which should where possible be a safe state, and associated mission times for SSCs.

4. Ensuring safety functions and accident management in design extension conditions

General

4.1 In DEC A, it is the objective that the plant shall be able to fulfil, the fundamental safety functions:

- control of reactivity[40],
- removal of heat from the reactor core and from the spent fuel, and
- confinement of radioactive material.

In DEC B, it is the objective that the plant shall be able to fulfil confinement of radioactive material. To this end removal of heat from the damaged core shall be established[41].

4.2 It shall be demonstrated that SSCs[42] (including mobile equipment and their connecting points, if applicable) for the prevention of fuel damage or mitigation of consequences in DEC have the capacity and capability and are adequately qualified to perform their relevant functions for the appropriate period of time.

4.3 If accident management relies on the use of mobile equipment, permanent connecting points, accessible (from a physical and radiological point of view) under DEC, shall be installed to enable the use of this equipment. The mobile equipment, and the connecting points and lines shall be maintained, inspected and tested.

---

[39] These methods can be more realistic than for DBA, including best estimate. Modified acceptance criteria may be used in the analysis.

[40] Preferably, this safety function shall be fulfilled at all times; if it is lost, it shall be re-established after a transient period.

[41] For the fulfilment (or re-establishment) of the fundamental safety functions in DEC A and DEC B, the use of mobile equipment on-site can be taken into account, as well as support from off-site, with due consideration for the time required for it to be available.

[42] SSCs including their support functions and related instrumentation.

4.4 A systematic process shall be used to review all units relying on common services and supplies (if any), for ensuring that common resources of personnel, equipment and materials expected to be used in accident conditions are still effective and sufficient for each unit at all times. In particular, if support between units at one site is considered in DEC, it shall be demonstrated that it is not detrimental to the safety of any unit.

4.5 The NPP site shall be autonomous regarding supplies supporting safety functions for a period of time until it can be demonstrated with confidence that adequate supplies can be established from off site..

Long-term sub-criticality

4.6 In design extension conditions, sub-criticality of the reactor core shall be ensured in the long term[43] and in the fuel storage at any time.

Heat removal functions

4.7 There shall be sufficient independent and diverse means including necessary power supplies available to remove the residual heat from the core and the spent fuel. At least one of these means shall be effective after events involving natural hazards within the DEC.

Confinement functions

4.8 Isolation of the containment shall be possible in DEC. For those shutdown states where this cannot be achieved in due time, core damage shall be prevented with a high degree of confidence.

If an event leads to bypass of the containment, core damage shall be prevented with a high degree of confidence.

4.9 Pressure and temperature in the containment shall be managed.

4.10 The threats due to combustible gases shall be managed.

4.11 The containment shall be protected from overpressure.

If venting is to be used for managing the containment pressure, adequate filtration shall be provided.

4.12 High pressure core melt scenarios shall be prevented.

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

4.14 In DEC A, radioactive releases shall be minimised as far as reasonably practicable.

In DEC B, any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable to:

(a) allow sufficient time for protective actions (if any) in the vicinity of the plant; and

(b) avoid contamination of large areas in the long term.

Instrumentation and control for the management of DEC

4.15 Adequately qualified instrumentation shall be available for DEC for determining the status of plant (including spent fuel storage) and safety functions as far as required for making decisions[44].

4.16 There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations.

---

[43] It is acknowledged that in case of DEC B, sub-criticality might not be guaranteed during core degradation and later on during some time in a fraction of the corium.

[44] This refers to decisions concerning measures on-site as well as, in case of DEC B, off-site.

Emergency power

4.17 Adequate power supplies during DEC shall be ensured considering the necessary actions and the timeframes defined in the DEC analysis, taking into account natural hazards.

4.18 Batteries shall have adequate capacity to provide the necessary DC power until recharging can be established or other means are in place.

5. Review of the design extension conditions

5.1 The principle of continuous improvement[45] shall be applied to design extension conditions. In addition to regular review of design extension conditions, specific reviews shall be undertaken in response to significant operating experience and significant new information relevant to safety. All reviews of design extension conditions shall use both deterministic and probabilistic approaches to identify needs and opportunities for improvement.

[45] See RL A2.3.

Issue G: Safety Classification of Structures, Systems and Components

1. Objective

1.1 All SSCs[46] important to 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 applicable quality requirements

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~~ take into account the effects of operational conditions over the plant lifetime and the effects of ~~design basis~~ accidents on their characteristics and performance.

4.2 Qualification procedures 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[47] over the lifetime of the plant and when required in anticipated operational occurrences and accident conditions.

[46] SSCs include software for I&C.

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

Issue H: Operational Limits and Conditions

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, the current state of ~~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[48] 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 with OLC, remedial actions shall be taken immediately to re-establish compliance with 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[49] in future.

---

[48] 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)

[49] 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

1. Objective

1.1. The operating organisation shall have an Ageing Management Programme[50] to identify all ageing mechanisms relevant to structures, systems and components (SSCs) important to safety, 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 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[51] 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.

[50] 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.

[51] Or its functional equivalent in other designs

Issue J: System for Investigation of Events and Operational Experience Feedback

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 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

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[52] 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.

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.

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

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 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 requirements of the management system.

3.11 Any in-service inspection process shall be qualified[53], 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 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).

[53] 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.

Issue LM: Emergency Operating Procedures and Severe Accident Management Guidelines

1. Objectives

1.1 A comprehensive set of emergency operating procedures (EOPs) ~~for design basis accidents (DBAs) and beyond design basis accidents (BDBAs)~~, as well as guidelines for severe accident management (SAMG) shall be provided, covering accidents initiated during all operational states.

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 DEC A ~~Beyond Design Basis Accidents up to, but not including, the onset of core damage or spent fuel damage~~. The aim shall be to re-establish or compensate for lost safety functions and to set out actions to prevent core and spent fuel damage.

2.3 SAMGs shall be provided to mitigate the consequences of severe accidents for the cases where the response to events including 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[54] procedures. EOPs for DEC shall be ~~only~~ symptom based unless an event based approach can be justified.

2.5 EOPs and SAMGs shall be suitable to manage accidents that simultaneously affect the reactor and spent fuel storages, and shall take potential interactions between reactor and spent fuel storages into account.

2.6 Possibilities for one unit, without compromising its safety, supporting another unit on the site shall be covered by EOPs and SAMGs.

2.7 EOPs and SAMGs shall be such that they are able to be implemented even if all nuclear installations on a site are under accident conditions, taking into account the dependencies between the systems and common resources.

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.

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[55].

---

[54] Event-based EOPs enable the operator to identify the specific event and encompass:

- Information for determining the status of the plant ~~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).

3.4 EOPs for design basis accidents shall rely on adequately qualified equipment and instrumentation. For DEC, EOPs and SAMGs shall primarily rely on adequately qualified equipment.

3.5 EOPs and SAMGs shall consider the anticipated on-site conditions, including radiological conditions, associated with the accidents they are addressing and the initiating event or hazard that might have caused it.

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, as far as practicable, to ensure that they are administratively and technically correct for the plant, are compatible with the environment in which they will be used[56] and with the human resources available.

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 and exercises

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

6.2 Licensee emergency response staff shall be regularly trained and exercised, commensurate with their expected role in managing an emergency, for situations and conditions covered by EOPs and SAMGs.

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

6.4 Interventions called for in EOPs and SAMGs and needed to restore necessary safety functions, including those which may rely on mobile or off-site equipment, shall be planned for and regularly exercised. The potential unavailability of instruments, lighting and power and the use of protective equipment shall be considered.

[55] 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 4.8 to 4.14. It is understood that for these accident conditions also SAMGs shall be developed.

[56] In particular, expected manual operation of equipment shall be possible.

Issue N: Contents and Updating of Safety Analysis Report (SAR)

1. Objective

1.1 The Licensee shall provide a SAR[57] to demonstrate that the plant fulfils relevant safety requirements 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 include justification that it adequately demonstrates that the plant fulfils relevant safety requirements. The SAR shall describe the safety analyses performed to assess the safety of the plant in response to ~~postulated initiating events~~ anticipated operational occurrences, design basis accidents and design extension conditions against safety criteria and radiological release limits. Safety margins shall be described.

2.8 The SAR shall describe the emergency operation procedures and severe 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.

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.[58]

2.14 The descriptions, assessments and arrangements mentioned in the SAR shall consider the site as a whole, to take into account hazards:

- which may challenge all installations within a short period of time;
- which arise from harmful interactions between installations.

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

[58] 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.

3. Review and update of the SAR

3.1 The licensee shall update the SAR to reflect modifications, new regulatory requirements, new information relevant for the safety assessment (including those related to characteristics of the site and the site environment), and relevant standards, ~~as soon as practicable~~ in a timely manner after the new information is available and applicable.

Issue O: Probabilistic Safety Analysis (PSA)

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~~ operational states and all relevant initiating events including internal fire and internal flooding and covering fuel in the core and in the spent fuel storage. External hazards shall be included in the PSA for level 1 and level 2, as far as reasonably practicable. If not reasonably practicable, other justified methodologies shall be used to evaluate the contribution of natural hazards to the overall risk profile of the plant. ~~Severe weather conditions and seismic events shall be addressed~~[59]~~.~~

1.2 PSA shall include relevant dependencies[60].

1.3 The ~~basic~~ Level 1 PSA shall contain sensitivity and uncertainty analyses. The ~~basic~~ Level 2 PSA shall contain sensitivity analyses and, as appropriate, uncertainty 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. The mission times in the PSA shall be justified.

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

2. Quality of PSA

2.1 PSA shall be performed, documented, and maintained according to requirements of the 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[61] 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"~~[62]~~.

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.

~~[59] 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.~~

[60] Such as functional dependencies, area dependencies (based on the physical location of the components, systems and structures) and other common cause failures. Site aspects and interaction with other units could also be relevant.

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

~~[62] Small deviations in the plant parameters that could give rise to severely abnormal plant behaviour.~~

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.

Issue P: Periodic Safety Review (PSR)

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~~ taking into account operating experience, relevant research findings, and the current state of technology.

1.4 All reasonably practicable improvement measures shall be ~~taken~~ implemented by the licensee as a result of the review, in a timely manner.

1.5 An overall assessment of the safety of the plant covering the period until the next PSR shall be provided, and adequate confidence in plant safety for continued operation demonstrated, based on the results of the review in each area. This assessment shall highlight any issues that might limit the future safe operation of the plant and explain how they will be managed.

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 (including ageing management and equipment qualification);
- Site characteristics and the protection against external hazards (see Issue T concerning natural hazards);
- Safety analyses and their use;
- Operating experience and relevant research findings during the review period and the effectiveness of the system used for experience feed-back;
- Organisation, human factors, management system and safety culture;
- ~~Organisational arrangements;~~
- ~~Staffing and qualification of staff;~~
- Relevant procedures;
- Emergency preparedness;
- Radiation protection of the workers and the public as well as the radiological impact on the environment;
- ~~Radiological impact on the environment.~~
- Interactions between units at sites with more than one unit (e.g. hazards, possible common SSCs, organisation and management system, procedures, emergency preparedness).

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. The safety significance of all findings shall be evaluated using an appropriate approach. A global assessment shall consider all findings (positive and negative) and their cumulative effect on safety, and shall identify what safety improvements are reasonably practicable.

Issue Q: Plant Modifications

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.[63]

1.2 The licensee shall control plant modifications using a graded approach with appropriate criteria for categorization according to their safety significance[64].

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[65].

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.

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.

---

[63] RL 2.2 specifically addresses modifications to SSCs, all other reference levels relate to all type of modifications in the sense of IAEA SSR-2/2, Para 4.39.

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

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

5. Temporary modifications[66]

5.1 All temporary modifications shall be clearly identified at the point of application and at any relevant control position[67]. 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.

[66] 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

[67] 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

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~~ Controlling an emergency situation arising at their site, following any reasonably foreseeable event, including events related to combinations of ~~non-nuclear and nuclear~~ hazards as well as events involving all nuclear installations and ~~other~~ facilities on the site;

(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 in a timely manner and throughout all phases of an emergency.

2.2 The licensee shall provide for:

(a) Prompt recognition and classification of emergencies, consistent with the criteria set for alerting the appropriate authorities;

(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 current and foreseeable situation on the technical and 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[68].

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:

- address long-lasting situations;
- clarify how site (and if applicable corporate) resources (human and material) common to several installations are used;
- be co-ordinated with all other involved bodies;

The plan shall be 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[69].

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

3.2 Sufficient number~~s~~ of qualified personnel shall be available at all times for staffing appropriate positions promptly following the declaration and notification of an emergency. Arrangements shall be established to ensure that sufficiently qualified personnel can staff appropriate emergency positions in long-lasting situations.

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.

3.6 The licensee emergency response shall be functional in cases where infrastructures at the site and around the site are severely disrupted.

3.7 Arrangements to support on-site actions shall be in place with considerations for large-scale destruction of infrastructure in the vicinity of the site due to external hazards.

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”, which is separated from the main ~~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[70].

4.3 Emergency facilities shall be suitably located, designed and protected to~~ enable the exposure of emergency workers to be controlled~~

- remain operational for accident conditions to be managed (including design extension conditions) from these facilities;
- allow the protection from radiation as well as control of radiation exposure of emergency workers[71].

Appropriate measures shall be taken to protect those occupying emergency facilities for a protracted time from hazards resulting from accidents[72].

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

[70] 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 or where the licensee emergency response is directed. It may have plant information systems available, but is not expected to have any plant controls.

[71] Emergency workers include workers from the operating organisation and, if necessary, contractors, as well as off-site emergency responders that may be needed on-site.

[72] 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.

4.4 Instruments, tools, equipment, documentation, and communication systems for use in emergencies (including necessary mobile equipment), whether located on-site or off-site, shall be stored, maintained, tested and inspected sufficiently frequently so that they will be available and operational during DBA and DEC. Access to these storage locations shall be possible even in case of extensive infrastructure damage.

5. Training, drills and exercises

5.1 Arrangements shall be made to identify the knowledge, skills, and abilities needed for personnel (operating organization staff and, if necessary, contractors) 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 (operating organization staff and, if necessary, contractors) meet the training obligations.

5.4 The site emergency plan shall be regularly exercised at least annually. Some exercises shall be integrated to include as many as possible of the off-site organizations concerned. For sites with multiple nuclear installations, some exercises shall address situations affecting multiple facilities on the site. Exercises shall also include the use and connection of mobile equipment, if any.

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

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[73].

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 SSCs important to safety shall be suitably[74], fire resistant.

2.3 Buildings that contain equipment that is important to safety shall be subdivided into compartments that segregate such items from fire loads and segregate redundant safety systems from each other[75]. When a fire compartment approach is not practicable, fire cells shall be used[76], providing a balance between passive and active means, as justified by fire hazard analysis.

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

2.5 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:

- 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.

---

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

[74] In accordance with the results of the fire hazard analysis.

[75] 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.

[76] 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.

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.[77]

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 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.

[77] 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.

Issue T: Natural Hazards

1. Objective

1.1 Natural hazards shall be considered an integral part of the safety demonstration of the plant (including spent fuel storage). Threats from natural hazards shall be removed or minimised as far as reasonably practicable for all operational plant states. To achieve this, assessments of the design basis and design extension conditions[78] shall be performed to identify needs and opportunities for improvement.

2. Identification of natural hazards

2.1 All natural hazards that might affect the site shall be identified, including any related hazards (e.g. earthquake and tsunami). Justification shall be provided that the compiled list of natural hazards is complete and relevant to the site.

2.2 Natural hazards shall include:

- Geological hazards;
- Seismotectonic hazards;
- Meteorological hazards;
- Hydrological hazards;
- Biological phenomena;
- Forest fire.

3. Site specific natural hazard screening and assessment

3.1 Natural hazards identified as potentially affecting the site can be screened out on the basis of being incapable of posing a physical threat or being extremely unlikely with a high degree of confidence. Care shall be taken not to exclude hazards which in combination with other hazards[79] have the potential to pose a threat to the facility. The screening process shall be based on conservative assumptions. The arguments in support of the screening process shall be justified.

3.2 For all natural hazards that have not been screened out, hazard assessments shall be performed using deterministic and, as far as the current state of science and technology permits, probabilistic elements. This shall take into account all available data, and produce a relationship between the hazards severity (e.g. magnitude and duration) and exceedance frequency, where practicable. The maximum credible hazard severity shall be determined where this is practicable.

3.3 The following shall apply to hazard assessments.

- The hazard assessment shall be based on all relevant site and regional data. Particular attention shall be given to extending the data available to include beyond recorded and historical data.
- Special consideration shall be given to hazards that change with time.
- The methods and assumptions used shall be justified. Uncertainties affecting the results of the hazard assessments shall be evaluated.

---

[78] Design extension conditions could result from natural events exceeding the design basis events or from events leading to conditions not included in the design basis accidents.

[79] This could include other natural hazards, internal hazards or human induced hazards.

4. Definition of the design basis events

4.1 Design basis events[80] shall be defined based on the site specific hazard assessment.

4.2 The exceedance frequencies of design basis events shall be low enough to ensure a high degree of protection with respect to natural hazards. A common target value of frequency, not higher than 10^{-4} per annum, shall be used for each design basis event. Where it is not possible to calculate these probabilities with an acceptable degree of certainty, an event shall be chosen and justified to reach an equivalent level of safety. For the specific case of seismic loading, as a minimum, a horizontal peak ground acceleration value of 0.1g (where 'g' is the acceleration due to gravity) shall be applied, even if its exceedance frequency would be below the common target value.

4.3 The design basis events shall be compared to relevant historical data to verify that historical extreme events are exceeded by a sufficient margin.

4.4 Design basis parameters shall be defined for each design basis event taking due consideration of the results of the hazard assessments. The design basis parameter values shall be developed on a conservative basis.

5. Protection against design basis events

5.1 Protection shall be provided for design basis events. A protection concept[81] shall be established to provide a basis for the design of suitable protection measures.

5.2 The protection concept shall be of sufficient reliability that the fundamental safety functions are conservatively ensured for any direct and credible indirect effects of the design basis event.

5.3 The protection concept shall:

(a) apply reasonable conservatism providing safety margins in the design;

(b) rely primarily on passive measures as far as reasonable practicable;

(c) ensure that necessary accident management measures remain effective during and following a design basis event;

(d) take into account the predictability and development of the event over time;

(e) ensure that procedures and means are available to verify the plant condition during and following design basis events;

(f) consider that events could simultaneously challenge redundant or multiple SSCs, several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures;

(g) ensure that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;

(h) not adversely affect the protection against other design basis events (not originating from natural hazards).

5.4 For design basis events, SSCs identified as part of the protection concept with respect to natural hazards shall be considered as important to safety.

5.5 Monitoring and alert processes shall be available to support the protection concept when forewarning of the hazard is possible. Where appropriate, thresholds (intervention values) shall be defined to facilitate the timely initiation of administrative protection measures and to trigger the execution of pre-planned post-event actions (e.g. inspections).

---

[80] These design basis events are individual natural hazards or combinations of hazards (causally or non-causally linked). The design basis may either be the original design basis of the plant (when it was commissioned) or a reviewed design basis for example following a PSR.

[81] A protection concept, as meant here, describes the overall strategy followed to cope with natural hazards. It shall encompass the protection against design basis events, events exceeding the design basis and the links into EOPs and SAMGs.

5.6 During long-lasting natural events, arrangements for the replacement of personnel and supplies shall be available.

6. Considerations for events more severe than the design basis events

6.1 Events that are more severe than the design basis events shall be identified as part of DEC analysis. Further detailed analysis of an event will not be necessary, if it is shown that its occurrence can be considered with a high degree of confidence to be extremely unlikely.

6.2 To support identification of events and assessment of their effects, the hazards severity as a function of exceedance frequency or other parameters related to the event shall be developed, when practicable.

6.3 When assessing the effects of natural hazards included in the DEC analysis, and identifying reasonably practicable improvements related to such events, analysis shall, as far as practicable, include:

(a) determining the severity of the event at which fundamental safety functions cannot be assured;

(b) demonstration of sufficient margins to “cliff-edge effects”;

(c) identification and assessment of the most resilient means for ensuring the fundamental safety functions;

(d) consideration that events could simultaneously challenge redundant or multiple SSCs, several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures;

(e) demonstration that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;

(f) on-site verification (typically by walk-down methods).