Western European
WENRA RHWG
Nuclear Regulators Association

Report

WENRA Safety Reference Levels for Existing Reactors 2020

17th February 2021

Western European
WENRA RHWG
Nuclear Regulators Association

Table of Content

WENRA
Safety Reference Levels for Existing Reactors

–

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 focusing on the main safety functions for ensuring the integrity 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. The last revision, in 2014, was after the TEPCO Fukushima Dai-ichi nuclear accident to take into account the lessons learned, including the insight from the EU stress tests.

This revision addresses issues not revised in the 2014 revision. Review against changes in knowledge, international standards and other factors have identified the need to introduce the notion of leadership into Issue C (Leadership and Management for Safety) and obsolescence into Issue I (Ageing Management), which also addresses the outcome of the recent ENSREG Topical Peer Review on the topic. There was also a need to complete the hazards to be addressed in the safety demonstration. To achieve this Issue S (Protection against Internal Fires) has been extended to cover all internal hazards (Issue SV), and Issue T (Natural Hazards) has been extended to address all external hazards (Issue TU). All other issues remain unchanged from the previous version.

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

Stakeholders were asked for comments on the revised Safety Reference Levels. All the comments were reviewed during the finalization process.

For further information, several documents on the WENRA website describe the basis used and processes followed to develop and update these RLs. Guidance on specific issues is also available on the WENRA website www.wenra.org.

01
Issue A: Safety Policy

Safety area: Management for Safety

A1. Issuing and communication of a safety

A1.1 A written safety policy[1] shall be issued by the licensee.

A1.2 The safety policy shall be clear about giving safety an overriding priority in all plant activities.

A1.3 The safety policy shall include a commitment to continuously develop safety.

A1.4 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.

A1.5 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.

A2. Implementation of the safety policy and monitoring safety performance

A2.1 The safety policy shall require directives for implementing the policy and monitoring safety performance.

A2.2 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.

A2.3 The safety policy shall require continuous improvement of nuclear safety by means of:

- Identifying and analysing any new information with a timeframe commensurate to its safety significance;
- Regular[2] review of the overall safety of the nuclear power plant including the safety demonstration, taking into account operating experience, safety research, and advances in science and technology;
- Timely implementation of the reasonably practicable safety improvements identified.

Continuous improvement applies to all nuclear safety activities and hence it is relevant to all of the issues addressed in this document. Therefore, this requirement is not repeated in the other issues although it is applicable to all of them.

---

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.

A3. Evaluation of the safety policy

A3.1 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.

02
Issue B: Operating Organisation

Safety area: Management for Safety

B1. Organisational structure

B1.1 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.

B1.2 The adequacy of the organisational structure, for its purposes according to B1.1, 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.

B1.3 Responsibilities, authorities, and lines of communication shall be clearly defined and documented for all staff with duties important to safety.

B2. Management of safety and quality

B2.1 The licensee shall ensure that the plant is operated in a safe manner and in accordance with all applicable legal and regulatory requirements.

B2.2 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.

B2.3 The licensee shall ensure that the staff is provided with the necessary facilities and working conditions to carry out work in a safe manner.

B2.4 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.

B2.5 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.

B2.6 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] 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.

B3. Sufficiency and competency of staff

B3.1 The required number of staff for safe operation[5], and their competence, shall be analysed in a systematic and documented way.

B3.2 The sufficiency of staff for safe operation, their competence, and suitability for safety work shall be verified on a regular basis and documented.

B3.3 A long-term staffing plan[6] shall exist for activities that are important to safety.

B3.4 Changes to the number of staff, which might be significant for safety, shall be justified in advance, carefully planned and evaluated after implementation.

B3.5 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.

B3.6 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.

[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.

03
Issue C: Leadership and Management for Safety

Safety area: Management for Safety

C1. Objectives

C1.1 Leadership[7] and management for safety shall be established, sustained and balanced in the licensee organisation to effectively foster a strong safety culture and enhance safety performance.

C1.2 The senior management shall ensure that the safety policy is implemented and that its objectives are fulfilled.

C2. Leadership for safety

C2.1 Leadership for safety shall be effective at all organisational levels within the licensee organisation.

C2.2 The senior management shall ensure that the developed goals, strategies, plans and objectives are consistent with the safety policy of the licensee organisation. Their collective impact on safety shall be understood and managed in such a way that safety is not compromised by other priorities.

C2.3 The senior managers shall ensure that decisions made at all levels take into account the priorities and accountabilities for safety.

C2.4 Managers at all levels shall develop competences for leadership for safety, demonstrate commitment to safety and foster a strong safety culture.

C2.5 Managers at all levels shall promote values and expectations for safety by means of their decisions, statements and actions.

C2.6 Managers at all levels shall ensure that relevant professional knowledge, skills and experience of individuals under their responsibility are used in making decisions.

[7] Leadership is understood as a person's ability to give direction to and motivate individuals and groups and to influence their commitment to shared goals, values and behaviour.

C3. Management for safety

Management system

C3.1 An integrated management system shall be established, implemented, assessed and continuously improved by the licensee. The main aim of the integrated management system shall be to achieve and enhance nuclear safety. Other demands[8] on the licensee and the licensee's management system shall be considered in unison with nuclear safety, in order to help preclude their possible negative impact on nuclear safety.

C3.2 The licensee shall ensure that management at all levels demonstrate its commitment to the establishment, implementation, assessment and continuous improvement of the management system.

C3.3 The human and organisational factors[9] that influence safety shall be taken into account in the management system in an integrated approach.

C3.4 It shall be defined in the management system when, how and by whom decisions[10] are to be made within the organisation, ensuring that safety is taken into account in decision making and is not compromised by any decision taken.

C3.5 Provisions shall be made in the management system to collect, process and document operating experience. Internal and external experience shall be used to improve safety.

C3.6 The potential safety impact of changes to the management system shall be analysed prior to their implementation. Changes with potential impact on safety shall be justified, planned, executed and evaluated accordingly.

C3.7 All individuals of the licensee organisation shall be trained in the relevant aspects of the management system with the aim to ensure its implementation and to foster their involvement in its continuous improvement.

Resources[11]

C3.8 The licensee shall determine and provide the necessary resources to establish, implement, assess and continuously improve the management system.

C3.9 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 result;
- The hazards and the magnitude of the potential impact associated with each activity and its result;
- The possible consequences if an activity is carried out incorrectly or its objective is not achieved.

[8] Examples of such demands are health, environmental, security, quality and economic requirements.

[9] Human and organisational factors (HOF) are understood as the factors which have influence, in a positive or adverse manner, on human performance in a given situation, keeping in mind that safety is the result of interaction of human, technology and organisation

[10] With respect to decisions that impact on nuclear safety.

[11] "Resources" include individuals, infrastructure, working environment, information and knowledge, suppliers, as well as material and financial resources.

Documentation[12] of the management system

C3.10 The documentation of the management system shall include at least:

- The policy statements of the licensee[13];
- 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 and with interested parties;
- A description of the processes and supporting information that explain how work is to be prepared, reviewed, carried out, recorded, assessed and improved.

C3.11 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.

C3.12 Documentation 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.

C3.13 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.

Processes

C3.14 The processes[14] 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, their development shall be planned, and they shall be implemented, assessed and continuously improved. The sequence and interactions of the processes shall be determined.

C3.15 The methods necessary to ensure the effectiveness of both the implementation and the control of the processes shall be determined and implemented to achieve the organisation's goals without compromising safety.

Procurement

C3.17 Arrangements for qualification, selection, evaluation, procurement, and oversight of the supply of products and services important to safety[15] shall be made on the basis of specified criteria[16].

---

12 Documentation may include documents such as 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.

13 Including values and behavioural expectations

14 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.

15 Products and services participating in the technical or organisational provisions on which the safety demonstration of the plant is based.

16 Procurement procedures include specific instructions for preventing, detecting, reporting and disposing of counterfeit, fraudulent and suspect items.

C3.18 Purchasing requirements shall be developed and specified in procurement documents. Evidence that products and services meet these requirements shall be available to the licensee before they are used[17].

C3.19 The control of processes, or work performed within a process, contracted to external organisations shall be identified within the management system. The licensee shall retain overall safety responsibility when purchasing any products or contracting any services. It shall be ensured, that sufficient comprehension and knowledge about the product or service, that is being procured, are available within the licensee's organisation.

C4. Culture for safety

C4.1 Management, at all levels in the licensee organisation, 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.

C4.2 The management system shall include provisions to systematically develop, support, and promote desired and expected attitudes and behaviours that result in a strong safety culture.

C4.3 The licensee organisation shall ensure that its suppliers and contractors whose operations may have a bearing on the plant safety comply with C4.1 and C4.2 in a way that ensures that the resulting interfaces with the plant support the standards and expectations.

C5. Measurement, assessment and improvement

C5.1 The senior management shall ensure that:

- The adequacy and effectiveness of the management system is monitored and measured;
- Self-assessments and independent[18] assessments are conducted regularly regarding:
  - the performance of work for which they are responsible,
  - leadership for safety, and
  - safety culture, including the underlying attitudes and behaviours.

C5.2 An organisational unit shall be established with the responsibility for conducting independent internal assessments. This unit shall have sufficient authority to discharge its responsibilities. Individuals conducting independent assessments shall not assess their own work.

C5.3 The licensee organisation shall evaluate the results of the assessments and take any necessary actions, and shall record and communicate inside the licensee organisation the results, the decisions and the reasons for the necessary actions.

C5.4 Improvement plans shall include plans for the provision of adequate resources throughout all phases of implementation. Actions for improvement shall be monitored through to their completion and the effectiveness of the improvement shall be checked.

---

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

18 By an external organisation or by an internal independent assessment unit.

04
Issue D: Training and Authorization of NPP Staff (Jobs with Safety Importance)

Safety area: Management for Safety

D1. Policy

D1.1 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.

D1.2 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.

D2. Competence and qualification

D2.1 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.

D2.2 The Licensee shall define and document the necessary competence requirements for their staff.

D2.3 Appropriate training records and records of assessments against competence requirements shall be established and maintained for each individual with tasks important to safety.

D2.4 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.

D3. Training programmes and facilities

D3.1 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.

D3.2 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.

D3.3 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 to be used during an accident is effective. The simulator shall be equipped with software to cover normal operation, anticipated operational occurrences, and a range of accident conditions.[19]

D3.4 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.[20]

D3.5 Refresher training for control room operators shall include especially the following items as appropriate:

- Plant operation in normal operational states, selected anticipated operational occurrences and accident conditions;
- Shift crew teamwork;
- Operational experiences and modifications of plant and procedures.

D3.6 Maintenance and technical support staff including contractors shall have practical training on the required safety critical activities.

D4. Authorization

D4.1 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.

D4.2 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.

D4.3 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.

[19] This type of simulator is known as a full-scope simulator.
[20] Time includes the necessary briefings.

05
Issue E: Design Basis Envelope for Existing Reactors

Safety area: Design

E1. Objective

E1.1 The design basis[21] shall have as an objective the prevention or, if this fails, the mitigation of consequences resulting from anticipated operational occurrences and design basis accidents. 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.

E2. Safety strategy

E2.1 Defence-in-depth[22] shall be applied in order to prevent, or if prevention fails, to mitigate harmful radioactive releases.

E2.2 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 uncontrolled releases 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.

E3. Safety functions

E3.1 During normal operation[23], anticipated operational occurrences and design basis accidents, the plant shall be able to fulfil the fundamental safety functions[24]:

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

[21] The design basis shall be reviewed and updated during the lifetime of the plant (see RL E11.1).
[22] For further information see IAEA SSR-2/1 (2012).
[23] Normal operation includes start-up, power operation, shutting down, shutdown, maintenance, testing and refuelling.
[24] Under the conditions specified in the following paragraphs.

E4. Establishment of the design basis

E4.1 The design basis shall specify the capabilities of the plant to cope with a specified range of plant states[25] within the defined radiation protection requirements. Therefore, the design basis shall include the specification for normal operation, anticipated operational occurrences and design basis accidents from Postulated Initiating Events (PIEs), the safety classification, important assumptions and, in some cases, the particular methods of analysis.

E4.2 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 anticipated operational occurrences and design basis accidents shall be selected using deterministic or probabilistic methods or a combination of both, as well as engineering judgement.[26] 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.

E4.3 The design basis shall be systematically defined and documented to reflect the actual plant.

E5. Set of design basis events

E5.1 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.[27] The list of events shall be plant specific and take account of relevant experience and analysis from other plants.

E5.2 External hazards shall be taken into account in the design of the plant. In addition to natural hazards[28], human made external hazards – including airplane crash and 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 – shall as a minimum be taken into account in the design of the plant according to site specific conditions.

E6. Combination of events

E6.1 Credible combinations of individual events, including internal and external hazards, that could lead to anticipated operational occurrences or design basis accidents, shall be considered in the design. Deterministic and probabilistic assessment as well as engineering judgement can be used for the selection of the event combinations.

---

25 Normal operation, anticipated operational occurrences and design basis accident conditions.

26 Depending on the specific topic being under review, not all types of insights (deterministic, probabilistic or engineering judgement) may be relevant or needed.

27 Additional information on internal hazards is provided in IAEA Safety Standards NS-G-1.7 and NS-G-1.11.

28 See Issue T.

E7. Definition and application of technical acceptance criteria

E7.1 Initiating events shall be grouped into a limited number of categories that correspond to plant states[25], 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 frequency.

E7.2 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 accident.

E7.3 Criteria for the protection of the primary coolant pressure boundary shall be specified, including maximum pressure, maximum temperature, thermal- and pressure transients and stresses.

E7.4 If applicable, criteria in E7.3 shall be specified as well for protection of the secondary coolant system.

E7.5 Criteria shall be specified for protection of containment, including temperatures, pressures and leak rates.

E8. Demonstration of reasonable conservatism and safety margins

E8.1 The initial and boundary conditions shall be specified with conservatism.

E8.2 The worst single failure[29] 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.

E8.3 Only systems that are suitably safety classified can be credited to carry out a safety function. Non safety classified systems shall be assumed to operate only if they aggravate the effect of the initiating event[30].

E8.4 A stuck control rod shall be considered as an additional aggravating failure in the analysis of design basis accidents.[31]

E8.5 The safety systems shall be assumed to operate at their performance level that is most penalising for the initiator.

E8.6 Any failure, occurring as a consequence of a postulated initiating event, shall be regarded to be part of the original PIE.

E8.7 The safety analysis shall:

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

---

29 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.

30 This means that non safety classified 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.

31 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 control rod position dependence) are used. A stuck rod can be handled as single failure in the analysis of design basis accidents (DBAs) if the stuck rod itself is the worst single failure.

(b) provide assurance that uncertainties and their impact have been given adequate consideration[32];

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

(d) be auditable and reproducible.

E9. Design of safety functions

General

E9.1 The fail-safe principle shall be considered in the design of systems and components important to safety.

E9.2 A failure in a system intended for normal operation shall not affect a safety function.

E9.3 Activations and control of the safety functions shall be automated or accomplished by passive means such that operator action is not necessary within 30 minutes of the initiating event. Any operator actions required by the design within 30 minutes of the initiating event shall be justified.[33]

E9.4 The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components[34], redundancy, diversity[35], physical and functional separation and isolation.

E9.5 For sites with multiple units, appropriate independence between them shall be ensured.[36]

Reactor and fuel storage sub-criticality

E9.6 The means for shutting down the reactor shall consist of at least two diverse systems.

E9.7 At least one of the two systems shall, on its own, be capable of quickly[37] 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.

E9.8 Sub-criticality shall be ensured and sustained:

- in the reactor after planned reactor shutdown during normal operation and after anticipated operational occurrences, as long as needed;
- in the reactor, after a transient period (if any) following a design basis accident[38];
- for fuel storage during normal operation, anticipated operational occurrences, and design basis accidents.

---

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

33 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.

34 Proven by experience under similar conditions or adequately tested and qualified.

35 The potential for common cause failure, including common mode failure, shall be appropriately considered to achieve the necessary reliability.

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

37 Within 4-6 seconds, i.e. scram system.

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

Heat removal functions

E9.9 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, shall be provided taking into account the assumptions of a single failure and the loss of off-site power.

Confinement functions

E9.10 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.

E9.11 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.

E9.12 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.

E10. Instrumentation and control systems

E10.1 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 accidents. Provision shall be made for automatic recording[39] of measurements of any derived parameters that are important to safety.

E10.2 Instrumentation shall be adequate for measuring plant parameters and shall be environmentally qualified for the plant states concerned.

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

Control room

E10.3 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.

E10.4 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.

E10.5 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.

E10.6 For times when the main control room is not available, there shall be sufficient monitoring and control equipment available, preferably at a single location that is physically, electrically and functionally separate from the main control room, so that, if the main control room is unavailable, 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.

Reactor protection system

E10.7 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.

E10.8 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.

E10.9 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.

E10.10 Computer based systems used in a protection system, shall fulfil the following requirements:

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

Emergency power

E10.11 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.

E11. Review of the design basis

E11.1 The actual design basis shall regularly[40], and when relevant as a result of operating experience and significant new safety information[41], be reviewed, using both a deterministic and a probabilistic approach as well as engineering judgement to determine whether the design basis is still appropriate. Based on the results of these reviews needs and opportunities for improvements shall be identified and relevant measures shall be implemented.

[40] See RL A2.3.
[41] 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.

06
Issue F: Design Extension of Existing Reactors

Safety area: Design

F1. Objective

F1.1 As part of defence in depth, analysis of Design Extension Conditions (DEC) shall be undertaken with the purpose of further improving the safety of the nuclear power plant by:

- 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, in such events or conditions.

F1.2 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.

In addition to 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.

F2. Selection of design extension conditions

F2.1 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.

F2.2 The selection process for DEC A shall start by considering those 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 severe fuel damage in the core or in the spent fuel storage. It shall cover:

- Events occurring during the defined operational states of the plant;
- Events resulting from internal or external hazards;
- Common cause failures.

Where applicable, all reactors and spent fuel storages on the site have to be taken into account. Events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity shall be covered.

F2.3 The set of category DEC B events shall be postulated and justified to cover situations, where the capability of the plant to prevent severe fuel damage is exceeded or where measures provided are assumed not to function as intended, leading to severe fuel damage.

F3. Safety analysis of design extension conditions

F3.1 The DEC analysis shall:

(a) rely on methods, assumptions or arguments which are justified[42], 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 reasonably practicable provisions to prevent severe fuel damage (DEC A) and mitigate severe accidents (DEC B);

(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, where applicable, sufficient margins to avoid "cliff-edge effects"[43] that would result in unacceptable consequences, i.e. for DEC-A severe fuel damage and for DEC-B a large or early radioactive release.

(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, when applicable, associated mission times for SSCs.

F4. Ensuring safety functions in design extension conditions

General

F4.1 In DEC A, it is the objective that the plant shall be able to fulfil, the fundamental safety functions:

- control of reactivity[44],
- 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 fuel shall be established.[45]

---

42 These methods can be more realistic up to best estimate. Modified acceptance criteria may be used in the analysis.

43 A cliff edge effect occurs when a small change in a condition (a parameter, a state of a system…) leads to a disproportionate increase in consequences.

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

45 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.

F4.2 It shall be demonstrated that SSCs[46] (including mobile equipment and their connecting points, if applicable) for the prevention of severe 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.

F4.3 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.

F4.4 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.

F4.5 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

F4.6 In design extension conditions, sub-criticality of the reactor core shall be ensured in the long term[47] and in the fuel storage at any time.

Heat removal functions

F4.7 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 external hazards more severe than design basis events.

Confinement functions

F4.8 Isolation of the containment shall be possible in DEC. For those shutdown states where this cannot be achieved in due time, severe core damage shall be prevented with a high degree of confidence.

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

F4.9 Pressure and temperature in the containment shall be managed.

F4.10 The threats due to combustible gases shall be managed.

F4.11 The containment shall be protected from overpressure.

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

F4.12 High pressure core melt scenarios shall be prevented.

F4.13 Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.

[46] SSCs including their support functions and related instrumentation.
[47] 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.

F4.14 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

F4.15 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.[48]

F4.16 There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations.

Emergency power

F4.17 Adequate power supplies during DEC shall be ensured considering the necessary actions and the timeframes defined in the DEC analysis, taking into account external hazards.

F4.18 Batteries shall have adequate capacity to provide the necessary DC power until recharging can be established or other means are in place.

F5. Review of the design extension conditions

F5.1 The design extension conditions shall regularly[49], and when relevant as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach as well as engineering judgement to determine whether the selection of design extension conditions is still appropriate. Based on the results of these reviews needs and opportunities for improvements shall be identified and relevant measures shall be implemented.

[48] This refers to decisions concerning measures on-site as well as, in case of DEC B, off-site.
[49] See RL A2.3.

07
Issue G: Safety Classification of Structures, Systems and Components

Safety area: Design

G1. Objective

G1.1 All SSCs[50] important to safety shall be identified and classified on the basis of their importance for safety.

G2. Classification process

G2.1 The classification of SSCs shall be primarily based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment.

G2.2 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

G3. Ensuring reliability

G3.1 SSCs important to safety shall be designed, constructed and maintained such that their quality and reliability is commensurate with their classification.

G3.2 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.

G4. Selection of materials and qualification of equipment

G4.1 The design of SSCs important to safety and the materials used shall take into account the effects of operational conditions over the lifetime of the plant and, when required, the effects of accident conditions on their characteristics and performance.

G4.2 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[51] over the lifetime of the plant and when required in anticipated operational occurrences and accident conditions.

[50] SSCs include software for I&C.
[51] Environmental conditions include as appropriate vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity, and combinations thereof.

08
Issue H: Operational Limits and Conditions (OLCs)

Safety area: Operation

–

H1. Purpose

H1.1 OLCs shall be developed to ensure that plants are operated in accordance with design assumptions and intentions as documented in the Safety Analysis Report (SAR).

H1.2 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.

H2. Establishment and review of OLCs

H2.1 Each established OLC shall be justified based on plant design, safety analysis and commissioning tests.

H2.2 OLCs shall be kept updated and reviewed in the light of experience, the current state of science and technology, and every time modifications in the plant or in the safety analysis warrant it, and changed if necessary.

H2.3 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.

H3. Use of OLCs

H3.1 The OLCs shall be readily accessible to control room personnel.

H3.2 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.

H4. Scope of OLCs

H4.1 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 and testing.

H5. Safety limits, safety systems settings and operational limits

H5.1 Adequate margins shall be ensured between operational limits and the established safety systems settings, to avoid undesirably frequent actuation of safety systems.

H5.2 Safety limits shall be established using a conservative approach to take uncertainties in the safety analyses into account.

H6. Unavailability limits

H6.1 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.

H6.2 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.

H6.3 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.

H7. Unconditional requirements

H7.1 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.

H7.2 Plant shall not be returned to service following unplanned shutdown until it has been shown to be safe to do so.

H8. Staffing levels

H8.1 Minimum staffing levels for shift staff shall be stated in the OLCs.

H9. Surveillance

H9.1 The licensee shall ensure that an appropriate surveillance[52] program is established and implemented to ensure compliance with OLCs and shall ensure that results are evaluated and retained.

H10. Non-compliance

H10.1 In cases of non-compliance with OLC, remedial actions shall be taken immediately to re-establish compliance with OLC requirements.

H10.2 Reports of non-compliance shall be investigated and corrective action shall be implemented in order to help prevent such non-compliance[53] in future.

---

[52] 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)

[53] 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.

09
Issue I: Ageing Management

Safety area: Operation

I1. Objectives and scope of ageing management

I1.1 The licensee shall establish suitable organizational and functional arrangements to manage physical ageing[54] and technological obsolescence[55] of in-scope SSCs with foresight and anticipation through the entire life time of the plant, including design, construction, commissioning, operation and decommissioning phases. The licensee shall mitigate ageing degradation effects and prevent them, where reasonably practicable.

I1.2 In order to accomplish the safety functions through the entire life time of the nuclear power plant, the licensee shall, within the integrated management system:
- implement an effective overall Ageing Management Programme[56] and
- address technological obsolescence.

I1.3 The following SSCs shall be included in the scope of ageing management:
- SSCs important to safety
- Other SSCs whose failure may prevent SSCs important to safety from fulfilling their intended functions.

I2. Technical requirements, methods and procedures

I2.1 The ageing management programmes shall identify in a systematic and knowledge-based manner all relevant potential degradation mechanisms and their ageing effects, determine their possible consequences and the necessary activities to ensure and monitor the availability and reliability of in-scope SSCs.

I2.2 The licensee shall provide monitoring, testing, sampling and inspection activities to assess ageing effects and to detect, in a timely manner, unexpected behaviour of the in-scope SSCs or degradation symptoms. Where necessary, corrective actions shall be taken in a timely manner, taking into account prioritization by safety significance. Acceptance criteria against which the need of corrective actions is evaluated shall be defined.

---

54 Physical ageing is considered as a process by which the physical characteristics of a structure, system or component (SSC) gradually change with time or use. It occurs due to physical, chemical and/or biological processes (degradation mechanisms).

55 Technological obsolescence, relates to hardware availability, as a lack of spare parts and technical support (e.g. lack of suppliers) or to industrial policies (e.g. lack of industrial capabilities). Conceptual aspects of obsolescence relates to the evolution of knowledge, standards and regulations; conceptual aspects of obsolescence are not covered in Issue I.

56 An overall Ageing Management Programme may include several ageing management programmes.

I2.3 The ageing management programmes for SSCs shall take into account design basis, manufacture, environmental and process conditions and operating history (duty cycles, maintenance schedules, service life, testing schedules and replacement strategy), as well as the outcomes of Periodic Safety Reviews. Due consideration shall be given to the outcomes from qualification processes for the service life of SSCs.

I2.4 In case of specific conditions resulting from e.g. extended shutdown the licensee shall implement measures to manage the potential impact on ageing of in-scope SSCs.

I2.5 The licensee shall proactively identify the in-scope SSCs for which the reliability and availability can be endangered due to technological obsolescence. The licensee shall prioritize the identified SSCs based upon the safety impact to the plant, and develop a strategy to ensure that adequate solutions are implemented in a timely manner.

I2.6 The ageing management programmes shall be regularly reviewed and updated, in order to incorporate new information as it becomes available, to address new issues as they arise, to use adequate and proven tools and methods as they become available and to assess the effectiveness of these programmes.

I3. Major structures and components

I3.1. Ageing management of the reactor pressure vessel[57] 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.

I3.2. 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.

57 Or its functional equivalent in other designs.

10
Issue J: System for Investigation of Events and Operational Experience Feedback

Safety area: Operation

–

J1. Programmes and Responsibilities

J1.1 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.

J1.2 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.

J1.3 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.

J1.4 Staff responsible for evaluation of operational experience and investigation into events shall receive adequate training, resources, and support from the line management.

J1.5 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.

J2. Collection and storage of information

J2.1 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.

J3. Reporting and dissemination of safety significant information

J3.1 The licensee shall report events of significance to safety in accordance with established procedures and criteria.

J3.2 Plant personnel shall be required to report abnormal events and be encouraged to report internally near misses relevant to the safety of the plant.

J3.3 Information resulting from the operational experience shall be disseminated to relevant staff and shared with relevant national and international bodies.

J3.4 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.

J4. Assessment and investigation of events

J4.1 An initial assessment of events important to safety shall be performed without delay to determine whether urgent actions are necessary.

J4.2 The licensee shall have procedures specifying appropriate investigation methods, including methods of human performance analysis.

J4.3 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.

J4.4 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.

J4.5 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.

J5. Review and continuous improvement of the OEF process

J5.1 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.

11
Issue K: Maintenance, In-Service Inspection and Functional Testing

Safety area: Operation

K1. Scope and objectives

K1.1 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.

K1.2 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.

K2. Programme establishment and review

K2.1 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.

K2.2 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.

K2.3 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.

K2.4 The maintenance programme shall be periodically reviewed[58] 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.

K2.5 The potential impact of maintenance upon plant safety shall be assessed.

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

K3. Implementation

K3.1 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.

K3.2 Procedures shall be established, reviewed, and validated for maintenance, testing, surveillance and inspection tasks.

K3.3 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.

K3.4 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.

K3.5 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.

K3.6 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.

K3.7 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.

K3.8 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.

K3.9 The reactor coolant pressure boundary shall be subject to a system pressure test at or near the end of each major inspection interval.

K3.10 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.

K3.11 Any in-service inspection (ISI) process shall be qualified[59], in terms of required inspection area(s), method(s) of non-destructive testing, defects being sought and required effectiveness of inspections.

[59] 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 use as reference documents e.g. the European Regulators Common Position on NDT Qualification, ENIQ methodology and/or IAEA – EBP-VVER-11 documents.

K3.12 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.

K3.13 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).

12
Issue LM: Emergency Operating Procedures and Severe Accident Management Guidelines

Safety area: Operation

–

LM1. Objectives

LM1.1 A comprehensive set of procedures and guidelines, including emergency operating procedures (EOPs) and severe accident management guidelines (SAMGs) shall be provided, covering accident conditions initiated during all operational states.

LM2. Scope

LM2.1 EOPs shall be provided to cover Design Basis Accidents. These EOPs shall provide instructions for recovering the plant state to a safe condition.

LM2.2 EOPs, with other specific procedures or guidelines when applicable, shall be provided to cover DEC A. The aim shall be to re-establish or compensate for lost safety functions and to set out actions to prevent severe fuel damage in the core or in the spent fuel storage.

LM2.3 SAMGs, with other specific procedures or guidelines when applicable, shall be provided to mitigate the consequences of severe accidents for the cases where the responses to events including the measures provided by EOPs have not been successful in the prevention of severe fuel damage.

LM2.4 EOPs for design basis accidents shall be symptom based or a combination of symptom based and event based[60] procedures. EOPs for DEC A shall be symptom based unless an event based approach can be justified.

LM2.5 The set of procedures and guidelines shall be suitable to manage accident conditions that simultaneously affect the reactor and spent fuel storages, and shall take potential interactions between reactor and spent fuel storages into account.

---

[60] Event-based EOPs enable the operator to identify the specific event and encompass:
- Information for determining the status of the plant,
- 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).

LM2.6 Possibilities for one unit, without compromising its safety, supporting another unit on the site shall be covered by the set of procedures and guidelines.

LM2.7 The set of procedures and guidelines 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.

LM3. Format and Content of Procedures and Guidelines

LM3.1 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.

LM3.2 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.

LM3.3 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.[61]

LM3.4 EOPs for design basis accidents shall rely on adequately qualified equipment and instrumentation. EOPs for DEC and SAMGs shall primarily rely on adequately qualified equipment.

LM3.5 The set of procedures and guidelines shall consider the anticipated on-site conditions, including radiological conditions, associated with the accident conditions they are addressing and the initiating event or hazard that might have caused it.

LM4. Verification and validation

LM4.1 The set of procedures and guidelines 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[62] and with the human resources available.

LM4.2 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.

[61] 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 F4.8 to F4.14. It is understood that for these accident conditions also SAMGs shall be developed.

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

LM5. Review and updating

LM5.1 The set of procedures and guidelines shall be kept updated to ensure that they remain fit for their purpose.

LM6. Training and exercises

LM6.1 Control room staff shall be regularly trained and exercised, using full-scope simulators for the EOPs and simulators, where practicable, for the SAMGs.

LM6.2 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 the set of procedures and guidelines.

LM6.3 The transition from EOPs to SAMGs for management of severe accidents shall be regularly exercised.

LM6.4 Interventions called for in the set of procedures and guidelines 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.

13
Issue N: Contents and Updating of Safety Analysis Report (SAR)

Safety area: Safety Verification

N1. Objective

N1.1 The Licensee shall provide a SAR[63] to demonstrate that the plant fulfils relevant safety requirements and use it as a basis for continuous support of safe operation.

N1.2 The Licensee shall use the SAR as a basis for assessing the safety implications of changes to the plant, or to operating practices.

N2. Content of the SAR

N2.1 The SAR shall describe the site, the plant layout and normal operation and demonstrate how safety is achieved.

N2.2 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.

N2.3 The SAR shall identify applicable regulations codes and standards.

N2.4 The SAR shall describe the relevant aspects of the plant organization and the management of safety.

N2.5 The SAR shall contain the evaluation of the safety aspects related to the site.

N2.6 The SAR shall outline the general design concept and the approach adopted to meet the fundamental safety objectives.

N2.7 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 anticipated operational occurrences, design basis accidents and design extension conditions against safety criteria and radiological release limits. Safety margins shall be described.

N2.8 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.

N2.9 The SAR shall contain the technical bases for the operational limits and conditions.

N2.10 The SAR shall describe the policy, strategy, methods, and provisions for radiation protection.

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

N2.11 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.

N2.12 The SAR shall describe the on-site radioactive waste management provisions.

N2.13 The SAR shall describe how the relevant decommissioning and end-of-life aspects are taken into account during operation.[64]

N2.14 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.

N3. Review and update of the SAR

N3.1 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, in a timely manner after the new information is available and applicable.

[64] 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.

14
Issue O: Probabilistic Safety Analysis (PSA)

Safety area: Safety Verification

O1. Scope and content of PSA

O1.1 For each plant design, a specific PSA shall be developed for level 1 and level 2, considering all relevant[65] operational states, covering fuel in the core and in the spent fuel storage and all relevant internal and external initiating events. External hazards shall be included in the PSA for level 1 and level 2 as far as practicable, taking into account the current state of science and technology. If not practicable, other justified methodologies shall be used to evaluate the contribution of external hazards to the overall risk profile of the plant.

O1.2 PSA shall include relevant dependencies.[66]

O1.3 The Level 1 PSA shall contain sensitivity and uncertainty analyses. The Level 2 PSA shall contain sensitivity analyses and, as appropriate, uncertainty analyses.

O1.4 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.

O1.5 Human reliability analysis shall be performed, taking into account the factors which can influence the performance of plant staff in all plant states.

O2. Quality of PSA

O2.1 PSA shall be performed, documented, and maintained according to requirements of the management system of the licensee.

O2.2 PSA shall be performed according to an up to date proven methodology, taking into account international experience currently available.

O3. Use of PSA

O3.1 PSA shall be used to support safety management. The role of PSA in the decision making process shall be defined.

---

65 Relevant means that the considered initiating event (or operational state) is relevant for the risk as determined with the PSA. Adequate screening criteria shall be defined in order to identify the relevant initiating events and operational states.

66 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.

O3.2 PSA shall be used[67] 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.

O3.3 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".

O3.4 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.

O3.5 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.

O3.6 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.

O4. Demands and conditions on the use of PSA

O4.1 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.

O4.2 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.

O4.3 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.

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

15
Issue P: Periodic Safety Review (PSR)

Safety area: Safety Verification

-

P1. Objective of the periodic safety review

P1.1 The licensee shall have the prime responsibility for performing the Periodic Safety Review.

P1.2 The review shall confirm the compliance of the plant with its licensing basis and any deviations shall be resolved.

P1.3 The review shall identify and evaluate the safety significance of deviations from applicable current safety standards and internationally recognised good practices taking into account operating experience, relevant research findings, and the current state of technology.

P1.4 All reasonably practicable improvement measures shall be implemented by the licensee as a result of the review, in a timely manner.

P1.5 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.

P2. Scope of the periodic safety review

P2.1 The review shall be made periodically, at least every ten years.

P2.2 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 safety factors shall be covered by the review[68]:

(a) Plant design;

(b) Actual condition of structures, systems and components (SSCs) important to safety;

(c) Equipment qualification;

(d) Ageing;

(e) Deterministic safety analysis;

(f) Probabilistic safety assessment;

(g) Hazard analysis;

[68] Radiation protection is not regarded as a separate safety factor since it is related to most of the other safety factors. As far as there are other units at the site, interactions between them should also be covered by the review.

(h) Safety performance;

(i) Use of experience from other plants and research findings;

(j) Organization, the management system and safety culture;

(k) Procedures;

(l) Human factors;

(m) Emergency planning;

(n) Radiological impact on the environment.

P3. Methodology of the periodic safety review

P3.1 The review shall use an up to date, systematic, and documented methodology, taking into account deterministic as well as probabilistic assessments.

P3.2 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.

16
Issue Q: Plant Modifications

Safety area: Operation

-

Q1. Purpose and scope

Q1.1 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.[69]

Q1.2 The licensee shall control plant modifications using a graded approach with appropriate criteria for categorization according to their safety significance.[70]

Q2. Procedure for dealing with plant modifications

Q2.1 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.

Q2.2 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.

Q3. Requirements on safety assessment and review of modifications

Q3.1 An initial safety assessment shall be carried out to determine any consequences for safety.[71]

Q3.2 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.

Q3.3 Comprehensive safety assessments shall demonstrate all applicable safety aspects are considered and that the system specifications and the relevant safety requirements are met.

Q3.4 The scope, safety implications, and consequences of proposed modifications shall be reviewed by personnel not immediately involved in their design or implementation.

---

69 RL Q2.2 specifically addresses modifications to SSCs, all other RLs relate to all type of modifications in the sense of IAEA SSR-2/2, Para 4.39.

70 Para 4.5 of IAEA Guide NS-G-2.3 contains information about possible categories.

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

Q4. Implementation of modifications

Q4.1 Implementation and testing of plant modifications shall be performed in accordance with the applicable work control and plant testing procedures.

Q4.2 The impact upon procedures, training, and provisions for plant simulators shall be assessed and any appropriate revisions incorporated.

Q4.3 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.

Q5. Temporary modifications[72]

Q5.1 All temporary modifications shall be clearly identified at the point of application and at any relevant control position.[73] Operating personnel shall be clearly informed of these modifications and of their consequences for the operation of the plant.

Q5.2 Temporary modifications shall be managed according to specific plant procedures.

Q5.3 The number of simultaneous temporary modifications shall be kept to a minimum. The duration of a temporary modification shall be limited.

Q5.4 The licensee shall periodically review outstanding temporary modifications to determine whether they are still needed.

[72] 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.

[73] 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.

17
Issue R: On-site Emergency Preparedness

Safety area: Emergency Preparedness

R1. Objective

R1.1 The licensee shall provide arrangements for responding effectively to events requiring protective measures at the scene for:

(a) Controlling an emergency situation arising at their site, following any reasonably foreseeable event, including events related to combinations of hazards as well as events involving all nuclear installations and 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 to workers and the public.

R2. Emergency Preparedness and Response Plan

R2.1 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.

R2.2 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.[74]

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

R2.3 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 severe events occur.

R3. Organization

R3.1 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.[75]

R3.2 Sufficient numbers of qualified personnel shall be available at all times for staffing appropriate positions promptly following the declaration and notification of an emergency. Arrangements shall be established to ensure that sufficiently qualified personnel can staff appropriate emergency positions in long-lasting situations.

R3.3 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.

R3.4 Arrangements shall be made to alert off-site responsible authorities promptly.

R3.5 The licensee shall identify those who are authorized to carry out the response functions assigned in the emergency plan.

R3.6 The licensee emergency response shall be functional in cases where infrastructures at the site and around the site are severely disrupted.

R3.7 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.

R4. Facilities and equipment

R4.1 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.

R4.2 An “On-site Emergency Control Centre”, which is separated from the main 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.[76]

R4.3 Emergency facilities shall be suitably located, designed and protected to

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

[76] 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.

- 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[77].

Appropriate measures shall be taken to protect those occupying emergency facilities for a protracted time from hazards resulting from accident conditions.[78]

R4.4 Instruments, tools, equipment, documentation, and communication systems for use in emergencies (including necessary mobile equipment and consumables such as fuel, lubrication oil etc.), 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.

R5. Training, drills and exercises

R5.1 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.

R5.2 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.

R5.3 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.

R5.4 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.

R5.5 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.

[77] 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.

[78] 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 or affected by radiation fields and, where appropriate, this will include provision of re-circulatory air conditioning and continuous radiation monitoring systems.

18
Issue SV: Internal Hazards

Safety area: Design

-

SV1. Objective

SV1.1 Internal hazards[79] shall be considered an integral part of the safety demonstration of the plant (including spent fuel storage).

Threats from internal hazards shall be removed or minimised as far as reasonably practicable for all operational states.

SV2. Identification of plant specific internal hazards

SV2.1 All internal hazards[80] that might affect SSCs important to safety shall be identified. Justification shall be provided that the compiled list of internal hazards to be considered is complete and relevant to the design of the nuclear power plant. Any location where permanent or temporary hazard sources[81] are present shall be taken into account.

SV2.2 The list of internal hazards from which identification as stated in SV2.1 is conducted shall at least include:

- Fires;
- Explosions;
- Missiles;
- Pipe breaks (with consequential hazardous conditions);
- Flooding;
- Collapse of structures and falling objects;
- Electrical disturbances and electromagnetic interferences;
- Release of hazardous substances.

SV3. Assessment of plant specific internal hazards

SV3.1 For all internal hazards that might affect SSCs important to safety, hazard assessments shall be performed using deterministic and, as far as practicable, probabilistic methods as well as engineering judgement. Assessment shall account for all individual hazard sources and corresponding direct and credible indirect effects.

---

79 Malicious acts are not considered within this issue.

80 Internal hazards are initiated within the site area which is defined as the geographical area that contains an authorized NPP. It is enclosed by a physical barrier to prevent unauthorized access and the management of the authorized facility can exercise direct authority over it (in accordance with IAEA SSG-3 and IAEA Safety Glossary). Consequential hazards and causally linked hazards shall be considered, as well as random combinations of relatively frequent hazards. Secondary effects of countermeasures (e.g. flooding due to water from firefighting) should be considered.

81 A hazard source is understood as certain location or SSC from which a threat arises. For example, two tanks containing water are two different potential hazard sources for internal flooding.

SV3.2 Internal hazard sources shall, as far as reasonably practicable, be removed or minimised until it can be shown that:
- the most severe physically possible impact is incapable of posing a threat to SSCs important to safety or
- the occurrence of an event induced by a hazard source is extremely unlikely with a high degree of confidence.

SV3.3 The hazard assessment, applied methods and input data as well as the utilization of the results, including implementation of actions, shall be justified, documented and kept up to date.

SV4. Definition of the design basis events for internal hazards

SV4.1 Design basis events[82] shall be defined based on the unit specific internal hazard assessments and shall address all internal hazards not removed / minimized according to SV3.2.

SV4.2 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. Using the most severe physically possible impact is the preferred way for the conservative approach. Exceptions shall be justified.

SV5. Protection against internal hazards

SV5.1 A protection concept[83] shall be established to provide a basis for the design of suitable protection measures.

SV5.2 The licensee shall implement the defence in depth concept for protection against internal hazards. This shall include provisions to prevent the occurrence of events induced by internal hazards, to detect these events and, if relevant, control and/or mitigate their consequences.

SV5.3 The protection concept shall be of sufficient reliability so that the fundamental safety functions are conservatively ensured for any direct and credible indirect effects of design basis events for internal hazards.

SV5.4 The protection concept for internal hazards shall:
(a) apply conservatism to provide safety margins in the design;
(b) rely primarily on passive measures as far as reasonably practicable;
(c) ensure adequate physical separation or segregation of redundant / diverse trains of safety systems, to prevent propagation of the effects of internal hazards to other trains. Exceptions shall be justified;
(d) ensure that procedures and means are available to verify the plant conditions during and following an impact initiated by a design basis event;
(e) minimize, as far as reasonably practicable, the event propagation within the site area;
(f) ensure that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;

---

82 Design basis events for internal hazards cover single internal hazards or credible 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.

83 A protection concept, as meant here, describes the overall strategy to cope with internal hazards.

(g) not inadmissibly affect the protection against other design basis events (not limited to internal hazards);

SV5.5 SSCs identified as part of the protection concept with respect to design basis events shall be considered as important to safety (see G1.1).

SV5.6 If there is a credible combination of the hazard under consideration with another internal or external event the SSCs for protection shall remain effective in this combination[84].

SV5.7 Access and escape routes identified as necessary to bring and maintain the plant in a safe state for the considered design basis event shall be available and safe to use.

SV5.8 Where appropriate, detection and monitoring equipment shall be part of the protection concept to cope with internal hazards. Where appropriate, thresholds shall be identified and intervention values shall be defined to facilitate the timely initiation of protection measures.

SV5.9 Analyses applying the design extension approach (see Issue F) shall be performed in order to identify reasonably practicable improvements to protect fundamental safety functions against more challenging events than those considered in the design basis events unless the most severe physical possible impact has been considered for the definition for the design basis events (see SV4.1). Analyses shall also consider credible failures of the protection measures.

SV5.10 Adequate organisational arrangements, including minimum staffing levels, equipment, fitness for duty, skills and training, and procedures shall be in place to ensure safety, as identified by the hazard assessment.

SV6. Additional RLs specific for internal fire

Assessment of plant specific fire hazard

SV6.1 A fire hazard analysis shall be developed on a deterministic basis, covering at least:

- all plant operational states of normal operating and shutdown, a single fire and consequential spread;
- any plant location where fixed or transient combustible material is present;
- credible combinations (see RL E6.1) of fire and other events (including external hazards).

The deterministic analysis shall be complemented by PSA in order to evaluate the fire protection arrangements and to identify risks caused by fires.

SV6.2 The extent of reliance on on-site or off-site fire brigades shall be shown to be adequate in the fire hazard analysis.

Design principles

SV6.4 In accordance with the fire hazard assessment, buildings that contain SSCs important to safety shall be suitably fire resistant and shall maintain their structural integrity after a fire.

[84] e.g. seismic qualification of fire protection systems.

SV6.5 Use of a fire compartment approach is preferred. The fire resistance rating of the fire barriers of the fire compartment shall be sufficiently high so that the total combustion of the fire load in the compartment can occur without breaching the barriers taking into account the fire hazard analysis. If a fire compartment[85] approach is not practicable, fire cells[86] shall be used and duly justified by the fire hazard analysis. For fire barrier resistance assessment oxygen availability within and oxygen supply to the fire compartment shall be conservatively considered and justified.

SV6.6 Ventilation systems shall be arranged such that each fire compartment fulfils its segregation purpose in case of fire and designed such that the ventilation of other fire compartments which contain other trains of the safety system is maintained as far as required to fulfil their safety functions.

SV6.7 If parts of the ventilation systems (such as connecting ducts, fan rooms and filters) are located outside fire compartments they shall have a fire resistance consistent with the fire hazard analyses or be capable of isolation from fire effects by appropriately rated fire dampers.

Fire Detection

SV6.8 Fire detection and alarm features, with detailed annunciation of the location of a fire to the control room personnel, shall be installed at the plant and their adequacy shall be supported by results of the fire hazard assessment. These features shall be provided with non-interruptible[87] emergency power supplies and failures of the cable connections shall be announced to the main control room.

Fire extinguishing

SV6.9 Suitable fire extinguishing features shall be in place according to the fire hazard assessment. They shall be designed and located such that their rupture, spurious or inadvertent operation does not inadmissibly impair the SSCs important to safety.

SV6.10 The fire water distribution network for fire hydrants outside buildings and the internal standpipes shall provide adequate coverage of all plant areas. The coverage shall be justified by the fire hazard assessment.

Administrative measures

SV6.11 In order to prevent fires, procedures shall be established to control and minimize the amount of combustibles and the potential ignition sources. In order to ensure the operability of the fire protection measures, procedures shall be established and implemented. They shall include examination, inspection, maintenance and testing of fire barriers, fire detection, alarm features and extinguishing systems.

---

85 A fire compartment is a building or part of building that is completely surrounded by fire resistant barriers of sufficient rating. Barriers could be passive like walls, floors, ceilings, and penetration seals, or active like doors, hatches, dampers, etc.

86 In the fire cell approach, the spread of fire is avoided by substituting qualified fire barriers primarily with other passive provisions (e.g. distance, enclosures, protective coatings, paintings, wrappings), that take into account all physical and chemical phenomena that can lead to fire spreading. 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. (see also IAEA DS494)

87 To ensure functionality in the event of a loss of normal power supply

Firefighting organization

SV6.12 Written procedures that clearly define the responsibility and actions of staff in responding to any fire in the plant shall be in place and kept up to date. A firefighting strategy shall be developed, kept up-to date, and appropriate training provided, to cover each area in which a fire might affect SSCs important to safety.

SV6.13 If plant internal firefighting capability is supported by offsite resources, there shall be proper coordination between the plant personnel and the offsite response group, in order to ensure that the latter is familiar with the hazards of the plant. Emergency training, drills and exercises shall be performed.

SV6.14 If plant personnel are required for firefighting, their organization, minimum staffing level, equipment, fitness requirements, skills and training shall be documented and their adequacy shall be confirmed by a competent person.

19
Issue TU: External Hazards

Safety area: Design

-

TU1. Objective

TU1.1 External hazards, comprising natural and external human induced hazards[88], shall be considered an integral part of the safety demonstration of the plant (including spent fuel storage). Threats from external hazards shall be removed or minimised as far as reasonably practicable for all operational plant states. The safety demonstration in relation to external hazards shall include assessments of the design basis and design extension conditions with the aim to identify needs and opportunities for improvement.

TU2. Identification of external hazards

TU2.1 All external hazards that might affect the site shall be identified, including any related hazards (e.g. earthquake and tsunami, accidental aircraft crash with consequential aircraft fuel fire)[89].

Justification shall be provided that the compiled list of external hazards is complete and relevant to the site.

TU2.2 The list of external hazards from which identification as stated in TU2.1 is conducted shall at least include

- Geological hazards;
- Seismotectonic hazards;
- Meteorological hazards;
- Hydrological hazards;
- Biological phenomena;
- External fire;
- Accidental aircraft crash;
- Accidents at facilities outside the site area;
- Transportation accidents;
- Electrical disturbances and electromagnetic interferences.

88 Within these reference levels malicious acts are not considered.

89 Human induced external hazards originate from any kind of human activity outside the site area. In accordance with IAEA Safety Glossary the "site area" is defined as the geographical area that contains an authorized NPP. It is enclosed by a physical barrier to prevent unauthorized access, by means of which the management of the authorized facility can exercise direct authority.

TU3. Site specific external hazard screening and assessment

TU3.1 External 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[90] 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.

TU3.2 For all external hazards that have not been screened out, hazard assessments shall be performed using deterministic and, as far as practicable, probabilistic methods taking into account the current state of science and technology. This shall take into account all relevant 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.

TU3.3 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 events beyond recorded and historical data.
- Special consideration shall be given to hazards whose severity changes during the expected lifetime of the plant.
- The methods and assumptions used shall be justified. Uncertainties affecting the results of the hazard assessments shall be evaluated.

TU4. Definition of the design basis events for external hazards

TU4.1 Design basis events[91] shall be defined based on the site specific hazard assessment.

TU4.2 The exceedance frequencies of design basis events shall be low enough to ensure a high degree of protection with respect to external hazards. An exceedance frequency not higher than 10^{-4} per annum[92], shall be used for the design basis events. Where it is not possible to calculate these frequencies 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 10^{-4} per annum.

For accidental airplane crashes and explosion blast waves a design basis event shall be defined to ensure a minimum protection of the plant.

TU4.3 The design basis events for natural hazards shall be compared to relevant historical data to verify that historical extreme events are enveloped by the design basis with a sufficient margin.

---

90 This could include other natural hazards, internal hazards or human induced hazards. Consequential hazards and causally linked hazards shall be considered, as well as random combinations of relatively frequent hazards.

91 These design basis events are individual external hazards or credible 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.

92 According to the current practices, several WENRA countries require a value lower than 10-4 per annum for human induced and some also for natural hazards.

TU4.4 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.

TU5. Protection against design basis events

TU5.1 Protection shall be provided for design basis events.[93] A protection concept[94] shall be established to provide a basis for the design of suitable protection measures.

TU5.2 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.

TU5.3 The protection concept for external hazards shall:

(a) apply conservatism to provide safety margins in the design;
(b) rely primarily on passive measures as far as reasonably practicable;
(c) ensure that sufficient measures to cope with a design basis accident remain effective during and following a design basis event as defined in TU4.2;
(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 several redundant or diverse trains of a safety system, multiple SSCs or 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 inadmissibly affect the protection against other design basis events (not originating from external hazards).

TU5.4 For design basis events, SSCs identified as part of the protection concept with respect to external hazards shall be considered as important to safety.

TU5.5 Where appropriate, monitoring and alert processes shall be part of the protection concept to cope with external hazards and thresholds (intervention values) shall be defined to facilitate the timely initiation of protection measures. In addition, thresholds shall be identified to initiate the execution of pre-planned post-event actions (e.g. inspections).

TU6. Considerations for events more severe than the design basis events

TU6.1 Events that are more severe than the design basis events shall be identified as part of DEC analysis. Their selection shall be justified.[95] 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.

---

93 If the hazard levels of RL TU4.2 for seismic hazards were not used for the initial design basis of the plant and if it is not reasonably practicable to ensure a level of protection equivalent to a reviewed design basis, methods such as those mentioned in IAEA NS-G-2.13 may be used. This shall quantify the seismic capacity of the plant, according to its actual condition, and demonstrate the plant is protected against the seismic hazard established in RL TU4.2. A comparable approach may be used for demonstrating the minimum protection against aircraft crashes and explosion blast waves.

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

95 See Issue F section 2.

TU6.2 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.

TU6.3 When assessing the effects of external hazards included in the DEC analysis, and identifying reasonably practicable improvements related to such events, analysis shall, as far as practicable, include:

(a) demonstration of sufficient margins to avoid “cliff-edge effects” that would result in unacceptable consequences;
(b) identification and assessment of the most resilient means for ensuring the fundamental safety functions;
(c) consideration that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures;
(d) demonstration that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;
(e) on-site verification (typically by walk-down methods).