SAFETY DESIGN OF A NUCLEAR POWER PLANT

continues

With regard to new nuclear facilities, this Guide shall apply as of 1 December 2013 until further notice. With regard to operating nuclear facilities and those under construction, this Guide shall be enforced through a separate decision to be taken by STUK. This Guide replaces Guides YVL 1.0, YVL 2.0, YVL 2.7, YVL 5.2, YVL 5.5 and YVL 5.6.

First edition
Helsinki 2014

ISBN 978-952-309-046-0 (print) Kopijyvä Oy 2014
ISBN 978-952-309-047-7 (pdf)
ISBN 978-952-309-048-4 (html)

STUK • SÄTEILYTURVAKESKUS
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O. Box 14, FIN-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

Authorisation

According to Section 7 r of the Nuclear Energy Act (990/1987), *the Radiation and Nuclear Safety Authority (STUK) shall specify detailed safety requirements for the implementation of the safety level in accordance with the Nuclear Energy Act.*

Rules for application

The publication of a YVL Guide shall not, as such, alter any previous decisions made by STUK. After having heard the parties concerned STUK will issue a separate decision as to how a new or revised YVL Guide is to be applied to operating nuclear facilities or those under construction, and to licensees' operational activities. The Guide shall apply as it stands to new nuclear facilities.

When considering how the new safety requirements presented in the YVL Guides shall be applied to the operating nuclear facilities, or to those under construction, STUK will take due account of the principles laid down in Section 7 a of the Nuclear Energy Act (990/1987): *The safety of nuclear energy use shall be maintained at as high a level as practically possible. For the further development of safety, measures shall be implemented that can be considered justified considering operating experience, safety research and advances in science and technology.*

According to Section 7 r(3) of the Nuclear Energy Act, *the safety requirements of the Radiation and Nuclear Safety Authority (STUK) are binding on the licensee, while preserving the licensee's right to propose an alternative procedure or solution to that provided for in the regulations. If the licensee can convincingly demonstrate that the proposed procedure or solution will implement safety standards in accordance with this Act, the Radiation and Nuclear Safety Authority (STUK) may approve a procedure or solution by which the safety level set forth is achieved.*

Translation. Original text in Finnish.

1 Introduction

101. The requirements pertaining to the safety design of a nuclear power plant are based on the defence-in-depth principle. According to this principle, a nuclear power plant shall be designed using multiple, successive mutually redundant structures and systems in order to prevent reactor damage and the detrimental effects of radiation. Safety functions in accordance with the defence-in-depth principle shall be based on five successive levels of protection; levels one and two are designed to prevent accidents, whereas the remaining levels are designed to protect the plant, its operators and the environment from the adverse effects of accidents. The requirements presented in the guidelines issued by IAEA and WENRA are based on the same principle. This Guide sets out the requirements for the design of a nuclear power plant and systems important to safety, and specifies in more detail the design requirements set forth in Government Decree 717/2013.

102. Requirements related to the safety design of a nuclear power plant have also been set out in the following Guides:
- YVL A.1 Regulatory oversight of safety in the use of nuclear energy
- YVL A.3 Management system for a nuclear facility
- YVL A.5 Construction and commissioning of a nuclear facility
- YVL A.6 Conduct of operations at a nuclear power plant
- YVL A.7 Probabilistic risk assessment and risk management of a nuclear power plant
- YVL A.11 Security of a nuclear facility
- YVL B.2 Classification of systems, structures and components of a nuclear facility.

103. Additional detailed requirements pertaining to the safety design of a nuclear power plant are given in the following Guides:
- YVL A.12 Information security management of a nuclear facility
- YVL B.3 Deterministic safety analyses for a nuclear power plant
- YVL B.4 Nuclear fuel and reactor
- YVL B.5 Reactor coolant circuit of a nuclear power plant
- YVL B.6 Containment of a nuclear power plant
- YVL B.7 Provisions for internal and external hazards at a nuclear facility
- YVL B.8 Fire protection at a nuclear facility
- YVL E.6 Buildings and structures of a nuclear facility
- YVL E.7 Electrical and I&C equipment of a nuclear facility
- YVL E.10 Emergency power supplies of a nuclear facility
- YVL E.11 Hoisting and transfer equipment of a nuclear facility.

104. The structural radiation safety of a nuclear facility, the radiation safety of workers and the environment as well as the requirements pertaining to radiation measuring instruments are addressed in the following Guides:
- YVL C.1 Structural radiation safety at a nuclear facility
- YVL C.2 Radiation protection and exposure monitoring of nuclear facility workers
- YVL C.3 Limitation and monitoring of radioactive releases from a nuclear facility
- YVL C.4 Assessment of radiation doses to the public in the vicinity of a nuclear facility
- YVL C.6 Radiation monitoring at a nuclear facility.

2 Scope

201. This Guide applies to the design of a nuclear power plant and its systems important to safety. The Guide shall apply equally to the original design of the plant and any design modifications. This Guide may also be applied to the design of other nuclear facilities.

3 Management of design

3.1 Organisations responsible for design

301. According to Section 7 f of the Nuclear Energy Act (amendment 990/1987), *safety shall take priority during the construction and operation of a nuclear facility.* The holder of a construction/operating licence shall be responsible for ensuring that the nuclear facility is constructed and operated in compliance with the safety requirements.

302. The license applicant/licensee shall
1. ensure that the design and implementation of the nuclear facility and its systems are safe and fulfil the safety requirements; and
2. demonstrate that the nuclear facility and its systems are safe and that the safety requirements are met.

303. The license applicant/licensee shall ensure the design integrity and safety of the facility during the design, construction, operation and decommissioning of the facility.

304. The licensee shall have competent and experienced staff at its disposal.

305. The licensee shall maintain detailed design documentation to be able to ensure the design integrity and safety of the facility over its entire service life, including the planning of modifications and component replacements.

306. The organisations involved in the design of a nuclear power plant and its systems important to safety shall have a management system in place that meets the requirements set forth in Guide YVL A.3 as applicable. Additionally, the design organisations shall fulfil the requirements set forth in Section 3 of the present Guide. The licensee shall demonstrate that the requirements are met.

307. The design organisations shall have the required resources and competences in place. The licensee shall ensure the adequacy of the resources and level of competence.

308. If an organisation involved in the design of a nuclear power plant and systems important to safety relies on subcontractors, it shall ensure that
1. the subcontractor is capable of executing the assigned task;
2. the safety requirements related to the subcontracted design task are communicated clearly and unambiguously;
3. the subcontractor is duly briefed, instructed and supervised and its services used as appropriate; and
4. the use of the subcontractor is transparent and documented in such detail as to allow an independent third party assessment of the design if necessary.

309. The licensee shall be able to demonstrate due fulfilment of the safety requirements across the entire design subcontractor supply chain.

3.2 Design processes

310. According to Section 26 of Government Decree 717/2013, *systems, structures and components important to the safety of a nuclear power plant shall be available as detailed in the design basis requirements. Their availability and the impact of the operating environment shall be supervised by means of inspections, tests, measurements and analyses. Availability shall be confirmed in advance by means of regular maintenance, and preparations shall be made for maintenance and repair to avoid reduced availability. Condition monitoring and maintenance shall be designed, instructed and implemented in a manner that can reliably ensure the integrity and operability of the systems, structures and components throughout their service life.*

311. A nuclear power plant and the systems important to safety shall be designed by using design processes and methods appropriate for the required level of quality, and by applying the relevant safety regulations, guidelines and standards. The selection of the standards applied in design shall be justified in terms of suitability and coverage.

312. The design of systems important to safety shall be based on a life-cycle model where design and implementation are divided into stages. The life-cycle model shall comprise all successive stages from the determination of the applicable requirements to the operation stage. In particular, the life-cycle model shall include a separate requirement specification stage that precedes the actual design stages.

313. Each design and implementation stage shall be verified. The verification activities and methods shall be duly planned.

314. Each design and implementation stage shall be reviewed before the stage is declared as complete.

315. The licence applicant/licensee shall reserve the opportunity to participate in the review of any of the stages. The licence applicant/licensee shall participate in any reviews that are important in terms of safety. The license applicant/licensee shall reserve the right to abort the stage if it is obvious that the safety requirements are not fulfilled.

316. The organisations involved in the design shall have capable processes in place for managing requirements.

317. In design tasks involving several fields of technology, a communication process shall be provided to ensure due exchange of information across the organisational interfaces.

318. The participation of competent personnel in every aspect of design that is relevant to safety shall be ensured through stage reviews covering several fields of technology.

3.3 Configuration management

319. The licensee's management system shall define the processes and procedures applied in configuration management related to the construction and operation of a nuclear facility.

320. The configuration management processes and procedures shall cover the entire lifecycle of the facility, from design to commissioning and operation.

321. The configuration management processes and procedures shall define responsibilities and provide a description of the procedures applied in the monitoring of configuration management.

322. All systems and equipment at a nuclear facility shall be divided into sufficiently small sub-assemblies (configuration units) in order to ensure that they are readily identified and easy to monitor and manage.

323. The facility, sets of systems, systems, components, software, auxiliary devices and their related documentation and parameters (settings) as well as internal and external connections and interfaces shall be defined as hierarchical configuration units.

324. The procedures used in configuration management shall be applied to configuration units and related documentation throughout the entire life cycle of the units.

325. When a nuclear facility is designed or modifications are made to an existing facility, baseline configuration levels shall be determined with regard to reference points relevant to the operational processes involved.

326. All changes between baseline configuration levels shall be made in accordance with predetermined change management procedures.

327. The configuration system documentation shall be updated in connection with any modifications made.

328. Each organisation involved in the design of, or modifications to, a nuclear facility shall have in place adequate configuration management procedures for managing the configurations of all the products provided by such an organisation, and for ensuring the compatibility of the systems as a whole.

329. If there are several configuration management procedures in the supply chain, the licensee shall verify their acceptability and compatibility.

330. When a new nuclear facility is constructed and commissioned or extensive modifications are made to an existing facility, a description of the configuration management processes and related instructions, responsibilities and resources shall be provided in a configuration management plan specific to each individual project. Additionally, the management plan shall present the baseline configuration levels to be applied relative to the progress made in the project and the reviews and processing to be carried out by STUK.

3.4 Quality plans

331. For the purpose of designing and implementing systems important to safety and any modifications to such systems, a quality plan specific to each individual system shall be prepared and adopted. However, the same quality plan may be utilised for several systems if the quality objectives, the methods for attaining the quality objectives and the organisation implementing the plan are the same for all the systems concerned.

332. The quality plan shall present

1. the organisation designing the system, complete with responsibilities and interfaces to other organisations involved in design;
2. the standards and guidelines, including the YVL Guides, to be applied in the design and implementation;
3. the stages of the design and implementation process;
4. the documents, records and other stage inputs serving as input data for each design stage;
5. the documents, records and other stage outputs created as an outcome of each design stage;
6. the stage reviews upon completion of individual stages including the timing, content and performer of the stage review, acceptance criteria, and the applicable decision-making procedures and responsibilities;
7. the procedures used in the supervision of subcontractors;
8. configuration and change management and procedures for product identification;
9. the management of conformity, design changes, and management of non-conformities;
10. the support processes utilised concurrently with design and implementation, complete with the associated management and quality procedures;
11. the division of responsibilities for the processes and decision-making procedures, including the procedures for modifying the quality plan.

333. The system-specific quality plan shall be prepared and implemented in compliance with the requirements set out in this YVL Guide and an applicable standard.

334. When standards-compliant processes and the quality manual of the design organisation are used, a detailed description of the application of the processes and guidelines shall be provided in the quality plan.

335. The requirements for the quality plan that complements the supplier's management system included in the delivery are set out in Guide YVL A.3.

3.5 Requirement specifications

336. The requirements concerning systems important to safety of the nuclear facility shall be defined to such a level of detail that a designer independent of the requirement specification process is able to carry out the re-design required for the in-service maintenance of the system its components as well as their modifications throughout the life cycle of the facility.

337. Requirements that are not considered functional requirements, such as the applicable quality requirements and standards, shall also be specified.

338. The applicability of the referenced standards and guidelines shall be justified. If an exception is made to a specified standard or guideline, such a departure shall be justified and its effect assessed.

339. The requirement specifications shall be unambiguous, consistent and traceable. It shall be possible to verify the fulfilment of the requirements.

340. The accuracy, completeness and consistency of the requirement specification of systems important to safety shall be assessed by experts who are independent of the design and implementation process. The assessment report shall present the observations made as well as a justified conclusion.

341. The traceability of the requirements in the various design stages shall be demonstrable. The traceability of the requirements in the various design stages shall be demonstrated as part of the qualification.

3.6 Safety assessment within the design organisation

342. Safety assessments shall be carried out within the design organisation to ensure that the safety requirements are duly fulfilled and the design processes properly executed.

343. The safety assessments shall be carried out by competent experts independent of the design and implementation process. When the assessments involve several fields of technology, cross-technological aspects shall be considered systematically.

344. The safety assessment of the design shall be
1. executed as a continuous process during the design and verification activities; and
2. reported to the licensee in all stages.

345. If several organisations are involved in the design process, the principal supplier of the design work shall carry out an overall safety assessment of the design under the supervision of the licensee.

346. With systems, structures and components of considerable safety significance, a safety assessment shall be carried out by an independent third-party organisation.

347. Probabilistic risk assessments shall be applied in all the stages of design and design reviews. Such an analysis shall be up to date and pertinent to the then-current design.

3.7 Justification for the choice of design solutions

348. The solutions and methods chosen during the course of the design shall be based on proven technology and operating experience, and they shall be in compliance with the applicable standards. The design shall strive for simplicity. If new solutions are proposed, they shall be validated through tests and experiments.

349. The design of systems performing safety functions shall be justified by means of deterministic safety analyses. These analyses shall ensure that safety functions can be performed by the designed systems and that the safety targets established for the plant are met. Deterministic safety analyses shall be made of the initiating events after which the respective safety functions are needed. The functional requirements pertaining to systems performing safety functions shall be specified according to the consequences of such initiating events and the need to mitigate them. Detailed requirements concerning the deterministic safety analyses are given in Guides YVL B.3 and YVL B.5.

350. Probabilistic risk assessments (PRAs) shall be used to assess the probability of severe reactor core damage; the probability of a major release of radioactive substances, the balance of the design; and the risk significance of systems, structures and components. Detailed requirements concerning the probabilistic risk assessment are given in Guide YVL A.7.

351. Failure tolerance analyses shall be carried out to demonstrate that
- all systems performing safety functions and their auxiliary systems satisfy the failure criteria specified in section 4.3 of this Guide;
- systems assigned to different levels of defence according to the defence in depth approach have been functionally isolated from one another in such a way that a failure in any one level does not affect the other levels; and
- a common cause failure in any single component type (e.g. a similar check valve, same type and manufacturer) will not prevent the nuclear power plant from being brought to a controlled state and further to a safe state.

352. A failure tolerance analysis shall assess one functional complex at a time, with due regard both to the system that performs a safety function and its auxiliary systems. The analysis shall address each component that, in the event of a failure, may affect the successful execution of the safety function performed by the system following a specific initiating event. The analysis shall address all modes of failure for all the components affecting the system performing the safety function. Depending on the applicable failure criterion, the analysis shall focus on one failure at a time and examine its impact in terms of the operation of the system.

353. A common cause failure analysis shall be drawn up for initiating events in design basis categories DBC 2 and DBC 3. For the common cause failure analysis, the implementation of the safety functions shall be presented for each initiating event in a manner that indicates the use of the systems implementing the principles of diversity and redundancy. The common cause failure analysis shall address one safety function, or part of it, at a time with due regard to the systems implementing the function and the related auxiliary systems. The analysis shall address the common cause failures of all components whose common cause failures or spurious actuation may affect the performance of the safety function. The common cause failure analysis shall consider the initiating event, interdependencies between initiating events as well as common cause failures between components sharing a similar property, i.e. components that are similar or contain a significant number of similar parts.

354. Additionally, failure tolerance analyses shall consider human errors and demonstrate that single errors will not prevent the performance of the safety function concerned.

3.8 Documentation

355. The documentation describing the nuclear power plant, its systems and their design requirements shall be clearly structured, comprehensive and capable of accommodating any updates made during the course of design, implementation and operation.

356. The process of designing and implementing safety-classified systems shall be transparent, traceable and verifiable in its entirety. The work stages and their outcomes shall be documented to

- allow verification in all design stages so that the specified requirements are duly incorporated in the final system to be commissioned; and
- ensure that they can be assessed by an independent expert.

357. The documentation shall be of high quality, unambiguous and traceable.

358. Up-to-date and valid documentation shall be available to those involved in design and implementation.

359. The documentation concerning design and implementation shall be consistent and traceable to a frozen baseline of the plant design.

360. The documentation, including diagrams and illustrations (e.g. functional diagrams), shall be prepared using a clear and precise presentation method that is understandable to the experts in the various fields of technology who are involved in the design of the plant and its systems.

361. To permit efficient version management of programmable systems and to avoid human error, software and hardware versions shall be provided with unique identifiers.

3.9 Qualification

362. The systems, structures and components important to safety shall be qualified for their intended use. The qualification process shall demonstrate that the systems, structures and systems are suitable for intended use and satisfy the relevant safety requirements. Aside from the assurance of the correctness of the design bases and the sufficiency of the quality management of design and implementation, the qualification process shall also include environmental qualification.

363. A qualification plan shall be prepared and implemented for the system to guide the qualification process. The qualification plan shall

1. present the data generated in connection with the quality assurance stages (verification and validation) of the systems, structures and components to be used for qualification purposes;
2. identify the external assessments, tests and analyses to be used the purpose of qualification, including the methods to be used, their relevance and the performer;
3. present a qualification roadmap complete with estimated timetables and dependencies relative to the progress of the project; and

4. specify the documentation to be produced in connection with the qualification process and its submission for regulatory review.

364. The licensee shall evaluate the acceptability of the qualification results and present a justified conclusion drawn from the results.

4 Design requirements for ensuring the reliability of safety functions

4.1 General design principles and requirements

401. According to Section 7 a of the Nuclear Energy Act (990/1987), the safety of nuclear energy use shall be maintained at as high a level as reasonably achievable (the SAHARA principle). A high level of safety shall be attained by means of reliable safety functions and multiple redundant structural barriers that limit the release of radioactive substances.

402. According to Section 14(1) of Government Decree 717/2013, *in ensuring safety functions, inherent safety features attainable by design shall be primarily utilised. In particular, the combined effect of a nuclear reactor's physical feedback characteristics shall be such that it mitigates the increase in reactor power.*

403. According to Section 14(2) of Government Decree 717/2013, *if inherent safety features cannot be utilised in ensuring a safety function, priority shall be given to systems and components which do not require a power supply or which, in consequence of a loss of power supply, will settle in a state preferable from the safety point of view.*

404. All the systems, structures and components of a nuclear power plant shall be so designed as to ensure that they perform reliably under design-basis environmental conditions. Environmental conditions to be considered in the design shall include, as appropriate, vibration, temperature, pressure, electromagnetic effects, radiation, humidity, and combinations of these conditions.

405. The location and materials of systems, structures and components that need to be maintained or inspected shall be planned with due regard to the radiation protection of workers in accordance with the ALARA (As Low As Reasonably Achievable) principle.

406. Systems performing safety functions shall be so designed as to ensure that their operability can be tested or otherwise verified during the operation of the plant under operational states and operating conditions as close as possible to the actual operational states and operating conditions for which they were designed. Components important to the operability of a safety function shall be accessible for inspection.

407. Every effort shall be made to ensure the independence of the design solutions from any single technology. Due consideration shall be given to potential technological developments in order to enable future replacements of components in a controlled and timely manner.

408. Special consideration shall be given at the design stage to the incorporation of features that will facilitate the future waste management, decommissioning and demolition of the plant. In particular, special care shall be taken in the choice of materials in order to minimise the future quantities of radioactive waste to the extent practicable, and to facilitate decontamination. The design shall provide for facilities necessary for treating and storing the radioactive waste generated in the course of operation, and for managing the radioactive waste generated as a result of the future decommissioning of the plant.

409. In the design, due account shall be taken of security aspects to minimise potential conflicts between safety and physical protection considerations. Due consideration shall be given to cybersecurity in the design of a nuclear power plant. Specific requirements pertaining to security arrangements are provided in Guide YVL A.11 and those pertaining to information security in Guide YVL A.12.

410. Provisions shall be made in the design for requirements concerning the installation of the IAEA's safeguards equipment for non-proliferation control purposes. Requirements pertaining to nuclear safeguards are provided in Guide YVL D.1.

411. If shared structures, systems and components important to safety are designed for nuclear power plant units located on the same plant site, it shall be demonstrated – by means of reliability assessments – that this does not impair the capability of these structures, systems and components to perform their safety functions.

412. If cross-connections are designed between the systems of individual nuclear power plant units performing the same safety function, it shall be demonstrated that such cross-connections make the safety functions more reliable than they would be in the absence of the connections.

4.2 Design bases of systems performing safety functions

413. According to Section 7 d of the Nuclear Energy Act (990/1987), *the design of a nuclear facility shall provide for the possibility of operational occurrences and accidents. The probability of an accident must be lower, the more severe the consequences of such an accident would prove for people, the environment or property.*

414. The nuclear power plant design shall take into account events that may cause a deviation of the plant parameters from normal values, as well as events that may threaten the availability of components or systems performing safety functions. Such events may be caused, for example, by a rupture in pressure equipment or piping; a component failure; a fault in the plant's operation or automatic control; or an internal or external threat.

415. Internal threats to be considered shall include at least fires breaking out inside the plant; floods resulting from component or pipe failures; impact and jet forces; explosions; overvoltage; and the potential for malicious damage.

416. External threats to be considered shall include at least extreme weather conditions; a fire in the neighbourhood of the plant; high and low sea levels; seismic phenomena; clogging of the heat sink for reasons other than freezing or seismic phenomena; an aircraft crash; electromagnetic phenomena; an explosion or the presence of toxic gases within the plant site; an oil spill in the surrounding sea area; and unauthorised entry to the plant site or unauthorised access to information systems.

417. Detailed requirements concerning the events to be taken into account in the design of a nuclear power plant are specified in Guides YVL B.3, B.5, B.7, B.8, A.11 and A.12.

4.3 Application of the defence in depth principle in the design

418. According to Section 14(3) of Government Decree 717/2013, *in order to prevent accidents and mitigate the consequences thereof, a nuclear power plant shall be provided with systems for shutting down the reactor and maintaining it in a sub-critical state, for removing decay heat generated in the reactor, and for retaining radioactive materials within the plant. Design of such systems shall apply redundancy, separation and diversity principles that ensure implementation of a safety function even in the event of malfunctions.* According to Section 14(5) of Government Decree 717/2013, *common cause failures shall only have minor impacts on plant safety.*

419. According to Section 7 b of the Nuclear Energy Act (990/1987), *the safety of a nuclear facility shall be ensured by means of successive levels of protection independent of each other (safety principle of defence-in-depth). This principle shall extend to the operational and structural safety of the plant.*

420. The requirements contained in Sections 7 b and 7 d of the Nuclear Energy Act referenced above are specified in more detail in Section 12 of Government Decree 717/2013 as follows: *In order to prevent anticipated operational occurrences and accidents, and to mitigate the consequences* *thereof, the functional defence-in-depth principle shall be implemented in the design, construction and operation of a nuclear power plant.*

421. Safety functions in accordance with the operational principle of defence in depth shall be assured through five successive levels of protection. The first two are designed to prevent accidents, whereas the remaining levels are designed to protect the plant, its operators and the environment from the adverse effects of an accident. The levels of defence are as follows:

1. **Prevention.** The first level is to ensure that the plant operates reliably and deviations from normal operation are rare. To achieve this, the design, manufacture, installation, commissioning, inspection, testing and maintenance of systems, structures and components, and the operation of the plant shall comply with high standards of quality and reliability with adequate safety margins.
2. **Control of anticipated operational occurrences.** At the second level, in addition to the careful design and operation of the plant, provisions shall be made for deviations from normal operation; the plant shall be equipped with systems designed to detect any anticipated operational occurrences and limit their escalation into accidents and, where necessary, to achieve the plant to the controlled state.
3. **Control of accidents** At the third level, provisions shall be made for accidents by means of reliable systems that are automatically actuated in the event of an accident; protect the barriers for confinement of radioactive substances; prevent the occurrence of severe fuel failure in postulated accidents and design extension conditions; and prevent the accident from escalating into a severe accident. The third level shall be divided into two parts: levels 3a and level 3b.
   a. At level 3a, the objective is to control the postulated accidents (Class 1 and Class 2) arising from single initiating events and their consequential effects in order to limit the releases of radioactive substances.
   b. At level 3b, the objective is to control design extension conditions, meaning:
      – anticipated operational occurrences and Class 1 postulated accidents that involve a common cause failure in the system designed for coping with the event concerned;
      – combinations of failures selected on the basis of a probabilistic risk assessment; and
      – rare external events that are unlikely to occur but nevertheless considered possible, such as extreme weather phenomena or the impact of a large aircraft.
4. **Containment of release in a severe accident** At level 4, the objective is to mitigate the consequences of a severe reactor accident in such a way that the integrity and leaktightness of the containment are ensured so as to prevent the release limits set forth for severe accidents from being exceeded.
5. **Mitigation of consequences.** At level 5, provisions shall be made for limiting, by means of emergency preparedness arrangements, the radiological consequences to the population in the event that considerable amounts of radioactive substances are released to the environment from the plant.

422. The design objective shall be to ensure that any release of radioactive substances will not expose the local population to a radiation dose in excess of the limit specified in Sections 8–10 of Government Decree 717/2013 and Guide YVL C.3.

423. Events that may result in a release requiring measures to protect the population in the early stages of the accident shall be practically eliminated.

424. Events to be practically eliminated shall be identified and analysed using methods based on deterministic analyses complemented by probabilistic risk assessments and expert assessments. Practical elimination cannot be based solely on compliance with a cut-off probabilistic value. Even if the probabilistic analysis suggests that the probability of an event is extremely low, all practicable measures shall be taken to reduce the risk. As an example events to be practically eliminated include:

1. a rapid, uncontrolled increase of reactivity leading to a criticality accident or severe reactor accident;
2. a loss of coolant during an outage leading to reactor core uncovery;
3. a load jeopardising the integrity of the containment during a severe reactor accident (e.g. reactor pressure vessel breach at high pressure, hydrogen explosion, steam explosion, direct impact of molten reactor core on containment basemat or wall, uncontrolled containment pressure increase); and
4. a loss of cooling in the fuel storage resulting in severe damage to the spent nuclear fuel.

4.3.1 Independence of the defence in depth levels

425. According to Section 12 of Government Decree 717/2013, the levels of defence required under the defence-in-depth concept shall be as independent of one another as is reasonably achievable. The loss of any single level of defence may not impair the operation of the other levels of defence.

426. Such independence shall be based on the adequate application of functional isolation, the diversity principle and physical separation between the levels of defence.

427. Due consideration shall be given to the dependence on the auxiliary systems supporting safety functions at different levels of defence in depth. Any dependence shall not unnecessarily impair the reliability of the defence-in-depth concept.

428. The systems, structures and components required for each postulated initiating event shall be identified, and it shall be shown by means of deterministic analyses that the systems, structures and components required for implementing any one level of defence in depth are sufficiently independent from the other levels. The adequacy of the achieved independence shall also be judged by probabilistic analyses.

429. The systems required for implementing different levels of defence according to the defence in depth principle shall be functionally isolated from one another in such a way that a malfunction or failure in any one level does not propagate to another level.

430. The systems and components used at different levels of defence in depth shall be separated, within the same safety division, from one another by distance or protective structures, if there is an obvious possibility for consequential failures arising from a failure of a system or component at another level.

431. The systems intended for controlling severe accidents (level 4 of the defence in depth concept) shall be functionally and physically separated from the systems intended for normal operation and anticipated operational occurrences and for controlling postulated accidents and design extension conditions (levels 1, 2, 3a and 3b). The defence-in-depth level 4 systems intended for controlling severe reactor accidents may, for sound reasons, also be used for preventing severe core damage in design extension conditions provided that this will not undermine the ability of the systems to perform their primary function in case the conditions evolve into a severe accident.

4.3.2 Strength of individual levels of defence in depth

432. No single anticipated failure or spurious action of an active component taking place during normal plant operation shall lead to a situation requiring intervention by systems designed to manage postulated accidents.

433. Provisions shall be made for failures by ensuring that systems performing a safety function consist of two or more redundant systems or system parts in parallel, so that the safety function can be performed even if any of them is rendered inoperable.

434. The redundant parts of a system performing safety functions shall be assigned to different safety divisions.

435. A failure in a system performing safety functions shall not cause a failure in either any redundant part of the same system or any other system contributing to the same safety function.

436. The loss of any safety division and the components contained therein shall not result in the loss of any safety function.

437. The safety divisions hosting redundant parts of safety systems shall be located in different buildings or housed in dedicated compartments to separate them from the other safety divisions in the same building in order to prevent faults from spreading from one redundant system part to another as a result of internal events (e.g. fire, flood or dynamic effects) or external events. Detailed requirements regarding the separation of safety divisions hosting redundant parts of safety systems are provided in Guide YVL B.7.

438. The requirement for the separation of redundant system parts also applies to all auxiliary systems of systems necessary for performing a safety function and to all I&C systems controlling the safety function, from the measurement indicating a need to actuate the system up to the equipment performing the safety function.

439. If the redundant parts of a safety system are interconnected for the distribution of electricity or control signals, the safety advantage as compared to a solution without such interconnection shall be justified.

440. Systems and components assigned to different safety classes shall be functionally isolated from one another to ensure that the mode of operation or a failure of a system or component of a lower safety class does not result in the malfunction or loss of function of a system of a higher safety class.

441. Electromagnetic compatibility shall be taken into account in the placement of electrical equipment and cables.

442. The failure criterion shall be applied to the complete train of systems consisting of the safety system and all auxiliary systems that are needed to perform the safety function. Such auxiliary systems include equipment cooling and power supply, as well as the systems controlling such functions. The (N+2) or (N+1) failure criterion, as defined herein, shall be used as the failure criterion.

443. More detailed regulations concerning the physical separation of systems and components within a single safety division are given in Guides YVL B.7 and YVL B.8.

4.3.3 Specific requirements for systems needed for achieving and maintaining a controlled state

444. The reactor shall meet the acceptance criteria set for events in design basis categories DBC1, DBC2, DBC3, DBC4 and DEC. The acceptance criteria for radiological consequences in each event category are specified in Sections 8, 9 and 10 of Government Decree 717/2013 and in Guide YVL C.3. The acceptance criteria concerning fuel failures are specified in Guide YVL B.4, and those concerning overpressure protection in Guide YVL B.3. The analysis requirements for demonstrating fulfilment of the criteria are given in Guide YVL B.3.

445. The reactor shall have a fast shutdown system employing solid neutron absorbers that alone, or in combination with the reactivity poison provided by the emergency core cooling system, is capable of shutting down the reactor into a controlled state and keeping it subcritical for a prolonged period of time after any anticipated operational occurrence or postulated accident in such a way that the limits set forth for fuel integrity, radiological consequences and primary circuit pressure in the respective design basis category DBC2, DBC3 or DBC4 are not exceeded. The insertion of the neutron absorbers into the reactor core shall make use of gravity, stored energy of compressed gas, or another driving force that does not need external power during insertion. The shutdown shall be accomplished even if any of the neutron absorber sets to be driven in together were to fail to be inserted. The reactor protection system initiating fast shutdown shall meet the (N+2) failure criterion.

446. In addition to the fast shutdown system based on solid neutron absorbers, the reactor shall have a diverse shutdown system capable of shutting down the reactor into a controlled state and keeping it subcritical for a prolonged period of time following an initiating event of any anticipated operational occurrence or Class 1 postulated accident (with the exception of loss of coolant accidents included in Class 1 postulated accidents) in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design basis category DEC are not exceeded. The shutdown system that complies with the diversity principle shall satisfy the (N+1) failure criterion.

447. In events involving a combination of failures (DEC B) and in rare external events (DEC C), it shall be possible to shut down the reactor and keep it subcritical in a controlled state in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design basis category DEC are not exceeded.

448. In the event of anticipated operational occurrences or postulated accidents, it shall be possible to accomplish decay heat removal from the reactor and containment by one or several systems that jointly meet the (N+2) failure criterion and the 72-hour self-sufficiency criterion in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in the respective design basis category DBC2, DBC3 or DBC4 are not exceeded. If the decay heat removal systems or their auxiliary systems have passive components that have a very low probability of failure in connection with the anticipated operational occurrence or postulated accident, the (N+1) failure criterion may be applied to those components instead of the (N+2) failure criterion.

449. In addition to the decay heat removal system(s) meeting requirement 448, the nuclear power plant shall have a system that complies with the diversity principle and is capable of removing the decay heat from the reactor and containment following an initiating event of any anticipated operational occurrence or Class 1 postulated accident in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design basis category DEC are not exceeded. The decay heat removal system that complies with the diversity principle shall satisfy the (N+1) failure criterion and the 72-hour self-sufficiency criterion. If the system that complies with the diversity principle is capable of providing decay heat removal in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in the respective design basis categories DBC2, DBC3 or DBC4 are not exceeded, the system can also be counted among the systems that jointly meet the (N+2) failure criterion given in requirement 448.

450. In multiple failure events (DEC B) and in rare external events (DEC C), it shall be possible to accomplish decay heat removal from the reactor to outside the containment and control of reactivity in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design basis category DEC are not exceeded.

It shall be possible to accomplish decay heat removal and reactivity control in rare external events (DEC C) without relying on power supply from transportable sources for at least eight hours without any material replenishments or recharging of the DC batteries. In addition, a sufficient inventory of water and fuel and capability to recharge the DC batteries shall exist at the plant site to enable decay heat removal for a period of 72 hours.

451. For a loss of the on-site power distribution system, provisions shall be made for decay heat removal to outside the containment and control of reactivity by ensuring that

1. the systems required for this purpose operate without any external power source or operate on an independent power source; and that
2. a sufficient inventory of water and fuel and capability to recharge the DC batteries exist at the plant site to maintain these arrangements for a period of 72 hours.

The single failure criterion does not need to be applied to the systems necessary for such arrangements, and the related containment isolation valves including actuators and cabling and the pipelines between the reactor and steam generators may be shared with a system intended for a different use. Direct current (DC) systems are deemed to be serviceable when properly electrically isolated.

Such a situation is governed by the design basis category DEC's fuel failure criteria and dose limits. No assumption needs to be made in the course of design for this type of situation arising concurrently with an independent initiating event, rare external event (DEC) or other multiple failure event (DEC B).

452. The nuclear power plant shall have in place arrangements that can guarantee sufficient cooling for the fuel placed in fuel storage facilities during rare external events in accordance with requirement 450. These arrangements shall make it possible to supervise the water level in the spent fuel pools for a minimum of eight hours without recharging the DC batteries. Furthermore, it shall be possible to keep the fuel reliably submerged during the loss of the plant's internal electricity distribution system in accordance with requirement 451. A sufficient inventory of water and fuel and capability to recharge the DC batteries shall exist at the plant site to maintain these arrangements for a period of 72 hours.

453. In the event that the reactor is not directly brought to a safe state as a result of an anticipated operational occurrence, a postulated accident or a design extension condition, it shall be possible to maintain the reactor in a controlled state long enough to ensure that the systems required for achieving a safe state are operable. Provisions shall be made to enable the repair and service of the systems needed for cooling the reactor from a controlled state to a safe state.

4.3.4 Specific requirements for systems needed for reaching and maintaining a safe state

454. The reactor shutdown system employing solid neutron absorbers and meeting the requirements of requirement 446, or the reactor shutdown system that complies with the diversity principle and meets the (N+1) failure criterion, shall be able to keep the reactor subcritical at all possible reactor temperatures.

455. It shall be possible to cool the reactor from a controlled state to a safe state and maintain it in a safe state for a prolonged period of time after any anticipated operational occurrences, postulated accidents and design extension conditions by decay heat removal systems meeting the (N+1) failure criterion. Provisions shall be made to enable the repair and servicing of the systems needed for maintaining the safe state.

4.3.5 Other redundancy requirements

456. The following systems performing functions relevant to safety shall satisfy the (N+1) failure criterion:

1. All systems insofar as their failure could directly lead to a situation requiring intervention by systems designed to manage postulated accidents, as defined in requirement 432;
2. Systems used for fuel handling insofar as they might cause fuel damage in the event of a system failure;
3. Stationary radiation measuring systems and equipment designed to measure online the external radiation rate of the reactor building; to limit the radiation doses of employees by means of an automatic control function; to monitor the activity of releases; and to perform accident monitoring and management;
4. Systems designed to ensure the cooling of spent fuel;
5. Measuring systems necessary for the operator to monitor and control anticipated operational occurrences and accidents, if no higher failure criterion is applied to the system for other reasons;
6. Active components of the systems designed to control severe reactor accidents;
7. Systems located outside the reactor containment, intended for the prevention of the dispersal of radioactive substances due to the breakdown of equipment or structures containing radioactive substances;
8. Systems necessary for maintaining safe working conditions in the control room;
9. Systems necessary for the cooling or heating of rooms to maintain the required operating conditions for electrical and I&C system components affecting safety functions. If a loss of cooling or heating of a room may lead to the loss of the safety function of more than one of the redundant electrical or I&C system parts, the single failure criterion shall be satisfied within that room;

10. Systems needed to perform containment isolation. The isolation function shall satisfy the (N+1) failure criterion in spite of possible maintenance/repair operations on the I&C or other auxiliary systems needed to perform the isolation function. Detailed requirements concerning the containment isolation function are given in Guide YVL B.6.

457. System-specific requirements concerning the application of the redundancy principle are provided in chapter 5 of this Guide and in Guides YVL B.4 (Nuclear fuel and reactor), YVL B.5 (Reactor coolant circuit of a nuclear power plant), and YVL B.6 (Containment of a nuclear power plant).

4.4 Avoidance of human errors

458. According to Section 6 of Government Decree 717/2013, *special attention shall be paid to the avoidance, detection and correction of any human error at any life cycle phase of the nuclear power plant. The possibility of human error shall be taken into account in the design of the nuclear power plant and in the planning of its operation and maintenance, so that human errors and deviations from normal plant operations due to human error do not endanger plant safety. The possibility of common cause failures due to human error shall be reduced. The effects of human errors shall be limited by applying a functional defense in depth safety principle.*

459. The planning of manual control, testing, inspections and maintenance of systems and components important to safety shall be based on a task and reliability analysis. The results of this analysis shall be used as a basis for designing the systems so as to ensure sound preconditions for reliable operation, for avoiding errors to the extent possible, and for the prompt detection of possible errors.

460. The presentation of the information needed for controlling and testing systems important to safety – as well as the related instructions and the control equipment used – shall be designed with the objective of preventing human errors during system operation and testing.

461. The presentation of the information needed for performing maintenance work – as well as the related instructions and the tools used – shall be designed with the objective of preventing human errors during system maintenance. Due attention shall also be paid to the physical work environment and the accessibility of components.

462. The rooms and systems – including related components, structures and cables – shall be easy to identify as being interrelated during design, operation, testing, maintenance and repairs. An unambiguous coding system shall be used for identification.

5 Design of specific nuclear power plant systems

5.1 Reactor cooling and decay heat removal systems

5101. Nuclear power plants shall be provided with systems that cool the reactor in operational states and accidents, and remove the decay heat produced in the reactor to the ultimate heat sink. The systems shall be designed to meet the safety design requirements presented in section 4.

5102. The design of the plant shall provide a secondary ultimate heat sink for decay heat removal in case of the unavailability of the primary ultimate heat sink. The secondary ultimate heat sink shall fulfil the 72-hour self-sufficiency criterion.

5103. The reactor cooling system and the associated auxiliary, control and protection systems shall be so designed as to ensure that the design parameters of the reactor primary circuit are not exceeded in operational states.

5104. The reactor coolant system shall be so designed as to ensure that:

1. the risk of loss of reactor coolant due to leaks below the top of active fuel is extremely low in all operational states; and
2. the maintenance operations affecting the primary circuit during an outage do not pose an essentially significant risk of a loss of reactor coolant.

5105. The reactor coolant volume control system shall be so designed as to ensure that the coolant volume in the primary circuit can be maintained within the range required for normal cooling, even in the event of a single failure of a component or control system affecting volume control.

5106. The reactor coolant system shall be provided with a system which indicates leaks and their volumes promptly enough even in the event of a single failure, and helps locate the leak accurately enough.

5107. A reactor coolant clean-up system shall be designed for the removal of radioactive substances and other impurities from the coolant in operational states.

5108. An emergency core cooling system shall be provided to cope with coolant leaks in the primary circuit and the systems directly associated with it; it shall compensate for any loss of coolant or otherwise provide efficient reactor cooling in order to ensure that the design limits for fuel are not exceeded.

5109. The capacity of the emergency core cooling system shall be adequate to compensate for leaks of various magnitudes, with the largest postulated leak equalling the complete, instantaneous break of the largest primary circuit pipe.

5110. The operability and efficiency of emergency core cooling under postulated leak conditions shall be ensured through appropriate primary circuit configuration and the positioning of the emergency core cooling connections.

5111. The emergency core cooling system shall be designed to remove the decay heat produced in the reactor for as long as necessary. To achieve this, provisions shall be made to allow the recirculation of the leaked water back into the reactor. In the course of design, due consideration shall be given to any solid or chemical impurities that may be released into the water and impede water recirculation or impair reactor cooling. To control impurities, the coolant recirculation system shall be provided with filtering structures whose intended function and adequate performance is verified by tests. These tests shall be carried out in chemically representative conditions using representative aged insulation and coating materials. The design of the filtering structures shall take into account the following:

1. The amount of impurities passing through the filters shall be low enough so as not to interfere with the operation of the coolant recirculation pumps or reduce the efficiency of reactor cooling;
2. The pressure loss caused by the impurities trapped by the filtering structures shall not prevent the coolant recirculation system from performing as designed;
3. It shall be possible to clean the filtering structures by means of a reversed coolant flow or gas blowdown if the pressure loss across the filters suggests a risk of excessive clogging.

5.2 Instrumentation and control systems

5.2.1 General requirements

5201. The I&C system design of a nuclear power plant shall be carried out so as to ensure that the safety design requirements presented in section 4 of this Guide are met.

5202. The I&C architecture shall be designed with the same attention to detail as the system of the highest safety class connected to the architecture. The design shall be carried out in such a way that the requirements specified in section 3 of this Guide are met.

5203. When the I&C architecture of a nuclear power plant is designed, functional and non-functional requirements shall be specified for the architecture, including

1. requirements derived from the tasks analysis;
2. limitations and requirements for I&C system functionality and failure behaviour imposed by plant design;
3. requirements regarding independence and separation between systems and other entities to be separated, and the connections to be taken into account in design;
4. requirements regarding the expected service life of each I&C system, the independence from any single technology, and the integration of plant and I&C systems in a way that

facilitates the replacement of components and systems, even in view of potential technological breakthroughs.

5204. The design of the I&C architecture of a nuclear power plant shall be documented to allow an external party not involved in the design of the I&C architecture and the plant to verify the appropriateness of the design bases and requirements for the I&C architecture, the accuracy of the design, the soundness of the justification for the key design decisions, and the failure behaviour.

5205. The safety significance of the information technology tools and testing methods (such as computational software, software compilers and testing tools) used in the design of I&C systems shall be assessed in terms of the end product being designed. The tools used in the design and implementation of safety-classified systems shall be identified. If the quality of a tool or testing method is of direct significance to the proper functioning or failure rate of the end product, it shall be qualified for its intended use. Detailed requirements for the qualification of tools are specified in Guide YVL E.7. Each tool version shall be specifically qualified.

5206. No solutions based on wireless data transfer may be used in the safety functions.

5.2.2 User interfaces

5207. The division of duties between operators and I&C systems shall be determined by means of a task analysis related to the control of operational occurrences and accidents with due regard to human limitations. The task analysis shall be used in the design of the I&C architecture and related user interfaces.

5208. The sufficiency of the time available for operator response shall be evaluated based on the analyses of anticipated operational occurrences and accidents, and the operator actions called for under such circumstances. The length of time available for operator response and the arguments they are based on shall be documented in the task analysis.

5209. It must be possible for operators to actuate the systems providing safety functions as well as the I&C functions manually from the control room, if this is deemed necessary to ensure safety.

5210. The operators in the control room shall have access to clearly presented and reliable information on the status of the I&C systems.

5211. The operators shall have at their disposal an illustrated summary presentation of the status of the safety functions and the values of the key plant parameters essential to the control of accidents. The information shall be displayed in a format that allows the operators to have a clear overview of the status of the plant.

5212. In the qualification process and failure analyses, the I&C system user interfaces shall be addressed as part of the system to which the user interface is related. Any centralisation of the user interfaces of the individual systems, for example for reasons of control room ergonomics, shall not lower the separation requirements specified in this Guide.

5.2.3 Instrumentation

5213. Measurements related to protection systems shall be planned and designed to give accurate and reliable input data to the safety-classified I&C systems. Such input data shall be traceable to the plant and plant system design requirements.

5214. Nuclear power plants shall be provided with accident instrumentation necessary for bringing the plant to, and keeping it in, a controlled state and capable of indicating the completion of safety functions in accident conditions. Such accident instrumentation shall include all the devices in the data transmission connection all the way from the sensor to the display unit.

5215. The instrumentation for monitoring the nuclear reactor shall be so designed as to provide sufficiently accurate and reliable input data for the determination of the reactor power distribution and the reactor's thermal margins. Necessary calculations of these reactor parameters shall be conducted automatically and with a frequency necessary to ensure the maintenance of the operating conditions of the reactor.

5216. Reactor instrumentation shall provide adequate information for detecting any abnormal or unpredicted operational conditions related to the reactor core, including indication of any incorrect positioning of the reactor internals or the fuel.

5217. Monitoring instrumentation shall be provided for the primary circuit of a pressurised water reactor to detect any loose objects.

5218. For the purpose of accident monitoring and management, the containment shall be provided with measuring and monitoring instrumentation to provide adequate information on the state of the containment, and to allow the planning and execution of the necessary countermeasures.

5219. For the control of any severe reactor accidents, the containment shall be equipped with measuring and monitoring instrumentation that provides sufficient information on the progress of potential severe reactor accidents and any circumstances that may jeopardise containment integrity.

5220. The measurement systems shall be capable of performing measurements over the full range within which the parameters being measured may vary in operational states or accidents.

5221. Where possible, the measurements shall be planned and designed to make it easy for operators to detect if any measurement fails or if the measurement range is exceeded.

5222. The control equipment shall be designed to record the process parameters indicating the plant status as well as the system control signals to permit a post-incident analysis of the operational events and accidents.

5.2.4 Operational I&C systems

5223. The nuclear power plant shall be provided with reliable systems for monitoring and controlling the functioning of the reactor and the plant systems during normal operational states. Such systems are known as 'operational I&C systems'.

5224. The operational I&C systems shall maintain the process parameters within a range consistent with normal operation as well as monitor the condition of plant systems, structures and components.

5225. The operational I&C systems shall be so designed that no need will arise, as a consequence of a single failure in the operational I&C systems, to actuate the safety systems designed for managing postulated accidents.

5226. The operational I&C systems shall be supplied with sufficient measurement and status data to allow the automatic or operator-assisted actuation of corrective control actions in case the plant parameters transcend the normal operating range.

5227. The operating and alarm limits of the operational I&C systems shall be defined to ensure that control actions can be started at the right time and completed without exceeding the limits specified for the actuation of the safety functions by the safety-classified I&C systems.

5.2.5 Protection I&C systems

5228. A nuclear power plant shall be provided with instrumentation and control (I&C) systems that actuate the necessary systems for providing protection functions whenever required and control the operation of these systems to prevent accidents or mitigate their consequences. These protection I&C systems shall be capable of maintaining the plant in a controlled state long enough to provide the operators of the nuclear power plant with sufficient time to consider and implement the correct response. Protection I&C systems comprise the entire chain of functions from plant state monitoring to the actuators being controlled.

5229. The actuation of a safety function by the protection I&C systems shall be based on at least two different process parameters, both of which are physically dependent on an anticipated operational occurrence or accident, and the trip limits of which can be set low enough to ensure timely actuation.

5230. If it is not possible to define two different process parameters for the detection of an event requiring actuation of a safety function, at least two different principles of measurement shall be applied for measuring the single process parameter used for detection.

5231. The protection I&C systems shall be so designed that any action performed by the operators in the control room, or the operation of any other system, cannot prevent or terminate a safety function triggered by the protection system until the safety function is completed or until the plant parameters are restored to a state where the need for protection is removed.

5232. It shall be possible to test the safety functions during the operation of the plant. The test concept shall be designed so that for the duration of all tests, the part of the protection I&C system downstream of the section being tested can be brought to a state preferable from the plant safety point of view.

5233. In the design process of the protection I&C systems, due consideration shall be given to regular periodic testing of the protection functions. The periodic tests of the protection I&C systems shall cover the entire chain from measurements to actuators or protection I&C system outputs, depending on the type of actuation involved. Requirements shall be specified for the coverage and scope of periodic testing.

5234. The adequate coverage of the self-diagnostics used in the protection I&C systems shall be demonstrated by means of analyses. The effect of failures in the self-diagnostic functions on the performance of the protection I&C systems shall also be analysed.

5235. Protection I&C systems shall be designed to monitor the validity of the input and output signals, the internal operation of the systems themselves, and to transmit an alarm signal when necessary.

5.2.6 Separation of I&C systems and prevention of fault propagation

5236. In the design of the I&C systems, due consideration shall be given to random failures (e.g. component failures), systematic errors and failures (e.g. software errors) and any passive and active failures resulting from these.

5237. To avoid failures in the I&C systems controlling the nuclear power plant, the principles of defence in depth, redundancy, diversity and separation shall be applied.

5238. The I&C systems controlling the nuclear power plant shall be designed to ensure that any failure will not prevent the management of any initiating event.

5239. A single failure occurring in a nuclear power plant's I&C system must not cause an initiating event that exceeds the severity level of an anticipated operational occurrence.

5240. When I&C systems fail, they shall meet the below requirements:

1. Any I&C systems controlling safety functions shall be designed such that failure will cause them to return to a state that is beneficial in terms of plant safety.
2. The failure of I&C systems in lower safety classes shall not prevent the protection I&C system from implementing the safety functions.
3. A failure in Class EYT I&C systems shall not cause an initiating event that exceeds the level of an anticipated operational occurrence, or prevent the operation of the safety functions designed to mitigate the consequences of accidents.
   a. In an accident scenario, their failure shall not essentially degrade the state of the plant (the event shall stay within the same event category).
   b. Their active failure during an anticipated operational occurrence shall not result in consequences worse than a class 1 accident.

4. A failure in Safety Class 3 I&C systems shall not prevent the execution of the safety functions designed to mitigate the consequences of accidents, or essentially degrade the state of the plant in connection with an accident.
5. The failure of Safety Class 3 I&C systems (other than operational I&C systems) as an initiating event shall not result in consequences worse than a class 1 accident.
6. The failure of Safety Class 3 I&C systems (other than operational I&C systems) in connection with an anticipated operational occurrence or class 1 accident shall not result in consequences worse than a class 2 accident .
7. A common cause failure occurring during operational occurrences and class 1 postulated accidents is considered a category DEC A event.
8. The severe reactor accident instrumentation and management systems and their auxiliary systems shall be independent from all other I&C systems of the plant unit. The failure of other I&C systems shall not interfere with the management systems for severe accidents.

5241. The effects of the failures and errors of the controls and functions performed by the I&C systems shall be analysed as functional entities. Functional entities may consist of system-internal structures, and they may cross the interfaces between systems. The functional entities selected for analysis shall be justified. The analysis shall account for all possible failure modes of the I&C systems. The analysis shall demonstrate that the I&C systems meet the requirements of paras. 5238, 5239 and 5240.

5242. The interfaces between systems shall be defined as part of the design of the I&C architecture.

5243. The data communications systems of the safety I&C systems shall satisfy the response time requirements during normal operation, anticipated operational occurrences and accidents. This shall be demonstrated for all conceivable load conditions.

5244. The protection I&C system shall be functionally separated from the other I&C systems, so that the information flow from the protection I&C system towards other I&C systems is made unidirectional by means of physical separation.

5245. The interface of the I&C architecture with the administrative computer systems shall be implemented by making the transmission of data unidirectional in such a way that any transmission of data towards the I&C architecture is prevented through separation at the physical level.

5246. In the design of I&C and electrical systems, due consideration shall be given to cyber security, and all security-related countermeasures shall be designed on the basis of risks assessments based on plant safety. For example, unauthorised access to systems and devices containing software shall be prevented by means physical, technical and administrative security arrangements; the installation of unauthorised devices and software shall be reliably prevented; and any modifications to the software shall be detectable and traceable. (As well as actual software upgrades, configuration and definition of parameters are also deemed to constitute modifications.) Detailed data security requirements are provided in Guide YVL A.12.

5.2.7 Testing the I&C systems

5247. Testing plans shall be drawn up for the testing of the I&C architecture and systems.

5248. The testing plans and results shall be documented so as to allow for independent assessment.

5249. The testing plan shall unambiguously define the acceptance criteria for the tests. The scope of testing shall be determined unambiguously. The scope of I&C system testing shall be defined to the accuracy of I&C system diagrams, for example by making use of structural dimensions.

5250. The resources of a testing agency independent of the design and manufacturing shall be drawn upon in the planning and performance of the tests, and in the evaluation of the results.

The test results shall be analysed and the sufficiency of the tests substantiated.

5251. In addition to the actual functionality of the system or components incorporated in the system, account shall be taken in the testing and functional analyses of any latent functionality not directly used by the system. The consequences of a failure of unused functions shall be identified. In testing and functional analyses, the potential existence of a non-documented functionality shall be considered.

5252. The factory tests shall cover all system functions and time settings, failure behaviour and, where possible, self-diagnostic functions. Simulators shall be used as testing aids in both the tests intended to demonstrate system conformance and in the actual validation tests. In case of modifications, the need for simulator testing shall be evaluated with due regard to the extent of the modification.

5253. Software shall be extensively tested in the hardware setup to be installed.

5254. Factory tests shall be carried out in a factory acceptance test environment designed for testing purposes.

5255. Any design modifications prompted by factory testing shall be made in accordance with the pre-defined configuration management and regression procedures.

5256. The factory tests pertaining to Safety Class 2 and 3 I&C systems shall be made on a configuration conforming to the design documents approved by STUK.

5257. Before the disassembly of a Safety Class 2 or 3 I&C system on the factory testing field, the licensee shall submit to STUK for approval a report on the conformance of the system at the time of completion of the factory field tests, and approval of this report shall be secured from STUK.

5.3 Control rooms

5.3.1 General

5301. For the purposes of the design process and the regulatory control exercised by STUK, the control room and emergency control room shall be perceived as a functional entity similar to a Safety Class 3 system. Individual control room systems shall be classified in accordance with the general classification principles.

5302. Due consideration shall be given to human factors and organisational circumstances right from the outset when plans are prepared for control room operations or changes affecting the control room.

5303. With new projects and extensive modifications to the control room, design and implementation shall be governed by the Human Factors Engineering (HFE) concept that covers, among other things, the following items:

1. the utilisation of accumulated operating experience;
2. function allocation and tasks analyses;
3. personnel and training planning;
4. user interface design;
5. the development of guides and standards;
6. a verification and validation plan regarding human factors and its implementation;
7. an assessment of human reliability; and
8. installation and commissioning, including the assessment and monitoring of control room performance.

The instructions required for control room and nuclear power plant operations shall form a coherent body of procedures, whose appropriateness shall be determined using the plant simulator. Similarly, the appropriateness of any modifications to the control room procedures and significant ergonomic changes shall be determined in advance by means of tests carried out in the plant simulator.

5304. The redundant parts of the control and protection I&C systems shall be functionally isolated from one another within the control room.

5305. The main control room and the command centre for emergency preparedness shall be protected to permit working without protective equipment during normal operation and under accidents and threat conditions. Due consideration shall be given to fire protection, protection against flooding, lighting, air conditioning, noise abatement, radiation protection and access control.

5306. The main control room and the emergency control room shall be physically separated to ensure that the probability of their simultaneous damage due to the same internal or external event remains extremely low.

5.3.2 Main control room

5307. According to Section 19 of Government Decree 717/2013, *the control room of a nuclear power plant shall contain equipment that provides information on the states of the nuclear reactor and any deviations from normal operation.*

5308. All the measures required for controlling the plant in its operational states and accident conditions shall be available from within the control room.

5309. For accident management purposes, the operators shall – in addition to the alarm systems – be assisted by a support function that displays comprehensive summary information on the state of the safety functions. The information provided by the accident management support function shall be displayed separately from other information displayed in the control room. Dedicated displays to provide summary information on the state of safety functions shall also be provided for controlling outage situations.

5310. The alarms required for detecting, identifying and managing anticipated operational occurrences and accidents shall be prioritised according to the safety significance of the respective event. Alarms shall be designed to ensure that they are detected as reliably as possible.

5311. The displays showing the measurement and status data generated by key accident instrumentation shall be easily recognisable.

5312. The main control room shall provide facilities for monitoring the state of the off-site grid.

5313. A qualification plan shall be provided for the main control room and the necessary monitoring and control posts when the application for a construction licence is filed.

5.3.3 Emergency control room

5314. According to Section 19 of Government Decree 717/2013, *the nuclear power plant shall have a supplementary control room independent of the main control room, and the necessary local control systems for shutting down and cooling the nuclear reactor, and for removing decay heat from the nuclear reactor and spent fuel stored at the plant.*

5315. The emergency control room shall be designed to allow the plant to be brought to a controlled state following the loss of the main control room and any anticipated operational occurrences associated with it. Local controls may also be used for the subsequent transition from a controlled state to a safe state. Requirements pertaining to the design of the emergency control room are specified in Guide YVL A.11.

5316. A safe passage shall be provided from the main control room to the emergency control room.

5317. The mutual independence of the main and emergency control room controls shall be accomplished by means of physical separation and functional isolation. The destruction of any single fire compartment shall not result in the loss of both the main and emergency control room controls.

5318. The hierarchy between the control systems of the main and emergency control rooms shall be defined to allow the plant to be controlled from only one control room at a time.

5.4 Electrical power systems

5401. According to Section 14 of Government Decree 717/2013, *a nuclear power plant shall have off-site and on-site electrical power supply systems to cope with anticipated operational occurrences and accidents. It shall be possible to supply the electrical power needed for safety functions using either of the two electrical power supply systems.*

5402. The plant shall be provided with systems permitting power supply from the main generator to the plant systems important to safety in case the connection to the off-site grid is lost. When this power supply is designed, due consideration shall be given to the requirements presented in Section 5.5 of Guide YVL E.7.

5403. The off-site and on-site systems for supplying power to the plant unit shall be designed to ensure that each of them has sufficient capacity to power the safety functions independently in accordance with the design criteria specified in Section 4.

5404. The plant's off-site and on-site electrical power supply units shall be designed to ensure that the probability of the loss of the plant's other power supply units as a consequence of the loss of a single power supply unit, or the loss of more than one power supply unit due to the same cause, is extremely low.

5405. Cross-connections between the redundant parts of safety-classified electrical systems shall be avoided unless they are demonstrated to improve the reliability of the system.

5406. If so, the cross-connections between the redundant parts of safety-classified electrical systems shall be designed to reliably prevent any unintentional coupling of the connections, and to make any human errors during commissioning and operation unlikely.

5407. The propagation of faults from one redundant electrical system part to another via cross-connections shall be reliably prevented.

5408. Local frequency and voltage fluctuations caused by the off-site grid and on-site electrical equipment or faults shall be analysed and given due consideration in the requirement specifications pertaining to electrical power systems and consumers. When this power supply is designed, due consideration shall be given to the requirements presented in Section 5.5 of Guide YVL E.7.

5409. Local frequency and voltage fluctuations caused by the off-site grid and on-site electrical equipment or faults shall not endanger the safety functions during normal operation, anticipated operational occurrences or accidents.

5410. The electrical systems shall be designed to ensure that operator actions, as well as the periodic inspections, maintenance, testing and repair of electrical systems and components, can be carried out without endangering the safety of the plant or personnel.

5411. The time during which the electrical systems are inoperable as a result of periodic inspections, maintenance, testing and repairs shall be kept as short as practicable.

5412. The periodic inspections and tests of electrical systems shall be extensive enough to permit quick detection of any deterioration in the performance of safety-classified electrical systems and components before they cease to meet the acceptance limits.

5413. Regular tests and inspections shall be carried out to ensure that the components associated with emergency power supply, as well as any other parts of the electrical systems that are not in use during normal plant operation, are ready for operation at all times.

5414. When software-based or programmable technology is used, the related requirements of Section 5.2 shall also be fulfilled.

5415. The power supply (electricity, compressed air, etc.) to the systems designed for managing severe reactor accidents shall be independent of all the other power supply units and power distribution systems of the plant.

5416. In the design, installation and operation of the electrical power systems and components of nuclear power plants, due consideration shall be given to the safety standards applied in Finland regarding the safety of electrical equipment and electrical installations, as well as other electrical safety regulations issued by electrical safety authorities (e.g. the set of standards: SFS 6000: Low-voltage electrical installations; SFS 6001: High-voltage electrical installations; and SFS 6002: Safety at electrical work).

5.4.1 Off-site grid connections

5417. For electrical power supply, there shall be two separate, independent grid connections from the off-site grid to each of the redundant sections of the on-site power distribution system.

5418. Both of the independent off-site grid connections shall be designed to ensure that a simultaneous failure of both connections due to the same cause remains unlikely.

5419. It shall be possible to activate both of the independent off-site grid connections quickly enough following the disconnection of the main generator from the grid.

5420. The same off-site grid connections may be shared by several plant units if adequate justification for this is provided. If so, each individual connection shall have sufficient capacity for simultaneous implementation of the safety functions at all plant units.

5421. Due consideration shall be given to equipment damage and fires caused by potential short circuits in the grid connections so as to make the simultaneous loss of both grid connections as a result of a single fault occurring in the switchyards or transmission line right-of-ways unlikely.

5422. The plant shall be provided with a reliable switch-over automation to permit automatic switch-over between the off-site grid connections.

5423. The automatic switch-over between the plant's off-site grid connections shall be designed to ensure that any switch-over does not actuate the plant unit's safety systems designed to cope with postulated accidents.

5424. When necessary, the plant concept shall also permit manual change-over between the off-site grid connections activated from within the main control room or, in case of the loss of the main control room, from within the emergency control room.

5.4.2 Power supply systems

5425. The plant unit's power supply systems shall be dimensioned to supply sufficient electrical power for the implementation of the safety functions in all plant conditions.

5.4.3 Alternating current power systems with back-up arrangements

5426. Power supply to alternating current electrical equipment important to safety shall be assured by using an on-site emergency power supply system as a back-up for off-site power supply.

5427. The on-site emergency power supply system shall fulfil the 72-hour self-sufficiency criterion.

5428. The on-site emergency power supply system shall start-up and switch on automatically to ensure uninterrupted power supply to the safety functions in accordance with the response-time requirements.

5429. It shall be possible to actuate the on-site emergency power supply system manually from the main control room and the emergency control room.

5430. It shall be possible to switch from the on-site emergency power supply back to the regular off-site electrical power supply using the manual controls in the main control room and emergency control room provided that the regular off-site electrical power supply is available.

5431. The on-site emergency power supply system shall be dimensioned to start, switch on, receive loads and supply electrical power reliably even under extreme load conditions (e.g. start-ups or short circuits in power distribution sub-systems).

5432. The quality of the alternating current supplied by the on-site emergency power supply system shall be consistently maintained to ensure that the operability of the supplied components is not endangered.

5433. More detailed requirements regarding the equipment used for emergency power supply at nuclear power plants are specified in Guide YVL E.10.

5434. The on-site emergency power supply system shall be provided with a condition monitoring system with a comprehensive set of alarms to promptly alert to and locate failures that prevent or endanger the system's performance.

5435. It shall be possible to safely isolate redundant parts of the on-site emergency power supply system from other electrical systems or system parts for the purpose of functional testing, maintenance and repairs.

5436. In the design of a nuclear power plant, due consideration shall be given to the possibility of a simultaneous loss of the off-site power supply and on-site emergency power supply system (total loss of alternating current supply).

5437. With a view to a total loss of alternating current supply, the plant shall have access to independent alternating current power supply units that are independent of the supply units designed for operational conditions and postulated accidents.

5438. The independent alternating current power supply unit shall fulfil the 72-hour self-sufficiency criterion.

5439. The independent alternating current power supply unit shall be capable of being activated quickly enough while at the same time minimising the risk of human errors.

5440. The capacity of the independent alternating current power supply unit shall be sufficient to maintain the plant unit in a controlled state in the event of anticipated operational occurrences and Class 1 postulated accidents.

5.4.4 Uninterruptible power supply systems

5441. To assure the proper operation of components important to safety requiring uninterruptible power supply, the electrical power supply to such components shall be ensured by means of reliable battery-backed systems that secure an uninterrupted supply of power in the event of a disruption in the supply of alternating current power.

5442. The battery sets, charging devices and any converters shall be dimensioned to assure the operability of uninterruptible power supply systems in accordance with the operating time requirements specified for each individual system.

5443. The battery sets supplying loads important to safety shall be dimensioned to provide a two-hour discharge time under the highest conceivable load.

5444. The battery sets supplying severe accident management systems shall be dimensioned to provide a 24-hour discharge time under the highest conceivable load.

5445. The dimensioning criteria applied for the start-up batteries of combustion engines and other special-purpose batteries shall be justified on a case-by-case basis.

5446. The charging devices of the battery sets related to uninterruptible power supply systems shall be capable of simultaneously supplying electricity to the load consumers and charging the batteries.

5447. The charging devices of the battery sets related to uninterruptible power supply systems shall be dimensioned to deliver full performance even under extreme load conditions (e.g. charging of discharged battery sets and simultaneous supply of loads following a power failure) and operating conditions.

5448. The uninterruptible power supply devices shall be capable of supplying the necessary direct current to the components being supplied even if the battery set is disconnected.

5449. In the event that uninterruptible power supply is provided while the battery sets are disconnected, the electricity being supplied shall be of sufficiently high quality not to cause any disruptions to the components under load.

5450. The uninterruptible power supply devices shall be designed to reliably prevent the transmission of potential disruptions in the supplying alternating current power grid to the final consumers.

5451. Safety-classified uninterruptible power supply systems shall be provided with comprehensive condition monitoring devices complete with alarms to promptly alert to and locate failures that prevent or endanger the system's performance.

5.4.5 Power supply connections between plant units

5452. The power supply systems of nuclear power plant units shall be so designed as to allow the supply of electrical power from one unit to another within the same site to ensure that the latter unit can be maintained in a controlled state in case of loss of electrical power.

5453. The power supply connection between plant units shall be designed to ensure that the probability of the propagation of any electrical failure from one unit to another via such a connection and its unplanned activation and coupling is low.

5454. If necessary, the supply connection between plant units shall be capable of being activated quickly and reliably, while at the same time minimising the risk of human error.

5.4.6 Electromagnetic compatibility (EMC) of electrical and I&C systems

5455. The safety-classified electrical power and I&C systems and components of nuclear power plants, including related cabling and installations, shall be reliably protected from the effects of electromagnetic interference.

5456. Electrical equipment and related cabling shall be designed and installed so as to ensure that they themselves do not generate any harmful electromagnetic interference in their operating environment.

5457. The following types of electromagnetic interference, among others, shall be considered in the design of electrical systems, components and cabling:

1. (emission of and immunity to) radiated radio frequency interference;
2. (emission via cables of and immunity to) conducted radio frequency interference; and
3. electrostatic discharge (ESD) tolerance.

5458. Detailed EMC requirements shall be defined in the requirement specifications for safety-classified electrical and I&C systems and components.

5459. One basis for the determination of the EMC requirements is provided by the general international EMC standards for industrial environments. Where necessary, these requirements shall be modified with due regard to the potentially more demanding ambient conditions prevailing at the installation site of individual components.

5460. When the EMC requirements are defined, due consideration shall be given to the exposure of components to potential recurring rapid transients (such as the switching off of inductive loads and the ringing of relays) and high-energy transients (such as various switching transients and strokes of lightning).

5461. When the EMC requirements are defined, due consideration shall be given to electromagnetic interference caused by human action, such as interference emissions from the wireless data transmission and telephone systems and the repair, maintenance and measuring devices used at the nuclear power plant.

5462. A radio frequency table shall be created for the nuclear power plant in support of the preparation of EMC specifications and qualification.

5463. The radio frequency table shall list all the radio frequencies allowed on the nuclear power plant site, including the highest permissible field intensities.

5464. Advisably, the radio frequency table shall indicate the maximum permissible transmission power levels for a specific device type (such as mobile phones or the phones used in the government network). Any such table shall also specify the theoretical assumptions on which the transmission power level is based.

5465. To determine the EMC environment of electrical systems and components at each nuclear power plant unit, unit-specific analyses shall be performed to evaluate the adequacy of the EMC requirements imposed.

5466. When the electrical and I&C systems of a nuclear power plant are replaced, special attention shall be paid to the EMC conditions prevailing on each installation location and the EMC characteristics of the equipment in order to avoid compatibility problems.

5.4.7 Earthing and lightning protection systems

5467. Earthing and lightning protection systems shall be designed, installed and maintained so as to effectively protect people, buildings, equipment as well as electrical and I&C systems from overvoltage and overcurrent caused by strokes of lightning and other potential electromagnetic interference due to meteorological conditions.

5468. The nuclear power plant's earthing and overvoltage protection systems shall be designed to effectively prevent the occurrence of harmful on-site or off-site overvoltage in electrical and I&C systems.

5469. When earthing and overvoltage protection is designed, electrical systems shall be understood as a single entity because insufficient protection of even one part of the system may expose other systems to disruptions.

5.4.8 Protection of electrical power systems and components

5470. The electrical power systems shall be provided with reliable protection devices that, in the event of disturbances and failures, only deactivate the affected component or section of the electric power network (selectively) under any foreseen grid switching condition.

5471. Fault currents shall be cut off quickly enough to avoid hazards and to minimise disruptions.

5472. All the plant's safety-classified high-power switchgears shall be provided with reliable arc protection, or other appropriate protection, to minimise equipment damage due to potential arc faults and to ensure the safety of the plant and its operating and maintenance personnel.

5473. Adequate alarms shall be provided to ensure that any electrical failures can be promptly detected, located and repaired.

5474. Adequate logging devices shall be provided to monitor the power distribution network to ensure that any electrical disturbances are promptly detected, located and repaired.

5475. The operation of the protection devices of safety-classified electrical power systems shall be capable of being tested across the entire protection chain.

5476. The testing of the protection devices of the electrical power systems of a nuclear power plant shall be carried out on a regular basis in order to ensure the operability of the protection system.

5477. When the protection devices of the electrical power systems of a nuclear power plant are tested, it shall be ensured – in addition to testing the operability of the protection system – that the protection will not trip any safety-classified electrical equipment at the highest consumer load.

5478. The safety significance of the blocking of a safety function, brought about by a protection device, shall be evaluated and a device bypass feature designed, where necessary, provided that this does not endanger the availability of any safety-classified electrical power supply.

5479. Any protection devices placed in service to safeguard components during testing shall be identified and designed in such a way that their operation does not endanger the operational capability of the system during an actual event.

5.5 Ventilation and air conditioning systems

5.5.1 General requirements

5501. The plant spaces where an airborne release of radioactive substances may occur shall be provided with ventilation and filtering systems that

- reduce the concentrations of airborne radioactive substances within the plant;
- prevent the spread of radioactive substances to other areas within the plant; and
- limit the release of radioactive substances to the environment.

5502. In terms of nuclear safety, the most important function of the ventilation and air conditioning systems is to maintain and secure such ambient conditions in all the rooms of a nuclear power plant as to ensure that the components and structures important to plant safety are kept in good condition and operate flawlessly.

5503. An analysis shall be provided of the consequences of any loss of the ventilation, heating and cooling of the spaces hosting systems important to safety, and of the temperature-related behaviour of such spaces during anticipated operational occurrences in plant operation.

5504. An assessment shall be made based on the analyses to determine whether it is necessary to apply the diversity principle in the heating or cooling of important spaces (such as air and seawater).

5505. Spaces that house heat-producing equipment, for which a maximum temperature limit has been specified in order to deliver the required performance, shall be provided with reliable cooling systems.

5506. The ventilation and air conditioning systems shall maintain appropriate working conditions for the plant's operating and maintenance staff in such a way that the cleanness, temperature and humidity of indoor air comply with the regulations issued for occupational health and safety.

5507. Each safety division of the plant, with the exception of containment and control room spaces comprising parts of several safety divisions, shall be fitted with a ventilation and air conditioning system, independent of the ventilation and air conditioning systems of other safety divisions, in order to maintain the heating, cooling, fire safety and other required ambient conditions of the spaces.

5508. The ventilation and air conditioning systems shall perform the aforementioned functions during normal operation, anticipated operational occurrences and accidents. Accident conditions shall be used as the design basis for the ventilation and air conditioning systems designed to operate during accidents or thereafter. The ventilation and air conditioning system components shall remain operable in the accidents and anticipated operational occurrences they are designed to manage.

5509. A definition of room conditions shall be carried out for rooms containing systems important to safety. The definition of room conditions shall cover the circumstances most relevant to the design of the ventilation and air conditioning system, such as temperature, humidity, radiation level, heat loads, pressure differences, and leaktightness and isolation requirements. Preliminary air change rates shall be proposed for the rooms based on the definition of room conditions.

5510. he rules and regulations issued by the Ministry of the Environment and the Ministry of the Interior (Finnish Building Code, RakMK) concerning the design and operation of ventilation systems, and the related fire protection design bases shall be met.

5511. The control room, emergency control room, command centre for emergency preparedness, civil defence shelter and other rooms needed under accident conditions shall be provided with isolating and filtering devices controlling supply air, and with measuring instruments to detect concentrations of radioactive and toxic substances. Due consideration in the design shall be given to the storage and transportation of hazardous materials, threats and accidents on the plant site and in its surroundings.

5.5.2 Area and zone classification

5512. The buildings of a nuclear power plant and their rooms shall be classified into zones. Predetermined verifiable pressure differences shall prevail between these zones in order to ensure that air always flows from the clean areas towards the less clean areas in terms of radiation safety.

5513. When classifying rooms into zones, due consideration shall be given to:

- the amounts and forms of radioactive substances potentially released from the plant systems and components in the event of leaks; and
- the accessibility of the rooms during normal operation and accidents.

5514. The air flow shall be designed to ensure that the concentrations of radioactive substances in the indoor air in manned plant rooms can be kept sufficiently low. Due consideration shall be given in the design to the required periods of stay in these rooms.

5515. The ventilation systems serving the rooms in the controlled area and in the clean area shall be completely separate from each other. The only exception to this rule is the rooms used for personnel access at the boundary of the controlled area and the clean area. Area and zone classification during operation based on the nuclear facility's radiation conditions is presented in Guide YVL C.1.

5516. The plans for the ventilation systems of the rooms located in the controlled area shall also describe how the release of radioactive substances to the environment is prevented in the event of a fire.

5.5.3 Supply air

5517. The intake air centres and supply air systems in the buildings housing safety-classified systems shall be designed and positioned so as to ensure that the ingress of smoke into these areas is unlikely in the event of a fire. Should smoke spread to the intake air centres in the event of a fire, it shall be possible to prevent the smoke from spreading further to the plant rooms by, for instance, switching off the supply air system.

5518. Additionally, the intake air centres and supply air systems in the buildings housing safety-classified systems shall be designed and positioned so as to ensure that the ingress of any combustible, toxic or otherwise hazardous substances to such centres and systems is unlikely. The ingress of hazardous substances to the plant rooms shall be capable of being observed and prevented by, for instance, switching off the supply air system.

5519. The supply air systems shall be fitted with filtering equipment to prevent the impurities contained in the outdoor air from accumulating in the plant rooms.

5520. The availability of supply air shall be ensured in circumstances in which it may be adversely affected by snow or ice.

5.5.4 Exhaust air

5521. Exhaust air from the controlled area shall be led in a controlled manner into the environment via ventilation ducts and through the vent stack. The exhaust air system of the rooms in the controlled area containing safety-classified systems may comprise – upstream of the vent stack – shared ducts outside these rooms, provided that adequate smoke and fire compartmentation is provided in such ducts.

5522. The amount of radioactive substances in the exhaust air, the rooms through which the ventilation duct is laid, and the pressure differences between the ducts and their surroundings shall be duly considered when specifying the requirements for the leaktightness of the ducts.

5523. In determining the materials and coatings for the ventilation ducts and equipment, and designing their geometrical shape, due consideration shall be given to easy decontamination of the surfaces from potential radioactivity.

5524. Any combustible, toxic or otherwise hazardous gases and vapours released into the plant rooms shall be removed by the ventilation system.

5525. If the exhaust air from plant rooms contains or may contain radioactive substances (in gaseous, aerosol or particulate form) in amounts significant in terms of environmental radiation exposure, the exhaust air shall be sufficiently filtered.

5526. If it is necessary to restrict the flow of exhaust air to reduce releases in the event of an accident, provisions shall be made, where necessary, to filter and cool the air of the rooms involved by means of room-specific equipment.

5527. Due consideration in the design shall be given to the risk of the filters catching fire and burning. Any burning filters shall be capable of being isolated from the rest of the ventilation system.

5.5.5 Coatings

5528. The requirements for the coatings of structures inside the containment building are presented in Guide YVL E.6. These requirements shall also be taken into account in the design of ventilation and air conditioning systems, except for such individual components whose coated surface area is deemed so small that any coating material released from the surface does not clog the air flow paths.

6 Documentation to be submitted to STUK

6.1 Design and construction of a new nuclear power plant

601. The documents pertaining to a new nuclear power plant and its systems and the system design documents shall be submitted to STUK on a timely basis in such a format as to allow STUK to use them as a basis for safety assessment in each individual licensing process. The documents may be submitted as indicated in the plan submitted by the licence applicant, in an order that is logical from the review point of view and arranged according to the relevant subject matter in one or several sets, prior to the filing of the licence application; as a rule, the documents are to be submitted at the time of filing of the licence application. If, exceptionally, some documents are submitted during the processing of the licence application, they shall be provided in such a way that all of the required information is available well in advance of the expected issuance of the statement concerning the respective licence.

6.1.1 Documents to be submitted when applying for a decision-in-principle

602. According to Section 24 of the Nuclear Energy Decree (161/1988), *the application for a decision-in-principle shall, in respect of each nuclear facility project, be accompanied by*
a) an outline of the technical principles of the planned nuclear facility;
b) a description of the safety principles that will be observed.

603. The information enclosed with the application for a decision-in-principle shall provide STUK with sufficient grounds for preparing a preliminary safety assessment of each nuclear facility project. The following information on a general level shall be included:

1. A general description of the safety principles and design bases to be used in the design of the plant and its systems;
2. A description of the series of key standards to be complied with in systems design;
3. A general description of the nuclear power plant and its main safety-classified systems (the reactor, primary circuit and containment, as well as the systems performing safety functions and their auxiliary systems designed to maintain the integrity of the above).
4. A general description of how the following safety issues are observed in the overall plant design and in the design of the principal safety-classified systems:
   a. the practical implementation of the defence in depth concept and independence between the levels in the overall plant design;
   b. the consideration of the redundancy, physical separation, functional isolation and diversity principles in plant systems performing safety functions in the various operational conditions of the plant;

c. the preliminary layout of the systems and the related structures and components;
d. the principles of protection against internal and external hazards;
e. the preliminary plans to cope with an aircraft crash;
f. a summary of performed safety analyses for a standard facility and their main results, including estimated environmental consequences of severe reactor accidents;

5. references to the facilities that have served as reference in the design, and a summary of the principal modifications and the reasons for the modifications;
6. the principal organisations involved in the design of the plant and its systems, and information on how they satisfy the requirements set for a design organisation in section 3 of the present Guide; and
7. the licence applicant's own assessment of how the plant satisfies the most essential Finnish safety requirements affecting design.

6.1.2 Documents to be submitted in the construction licence stage

604. According to Section 32 of the Nuclear Energy Decree (161/1988), *the application for a construction licence shall be accompanied by 5) an outline of the technical operating principles and features and other arrangements used to ensure the safety of the nuclear facility 6) a description of the safety principles that the applicant intends to observe and an evaluation of the fulfilment of the principles. […]*

605. According to Section 35 of the Nuclear Energy Decree (161/1988), the following documents pertaining to the design of the plant and its systems shall be submitted to STUK when an application for a construction licence is filed: *1) the preliminary safety analysis report, which shall include the general design and safety principles of the nuclear facility,…, a description of the operation of the facility, a description of the behaviour of the facility during accidents 2) a probabilistic risk assessment of the design stage 3) a proposal for a classification document, which shows the classification of structures, systems and components important to the safety of the nuclear facility on the basis of their significance with respect to safety. […]*

Preliminary Safety Analysis Report

606. The information enclosed with the application for a construction licence shall provide STUK with sufficient grounds for preparing the safety assessment. Information shall be provided on the safety functions and the systems performing safety functions to such a level of accuracy that the operation of the plant in anticipated operational occurrences and accidents in all operational states can be analysed and the PRA can be reviewed. The information may be presented to the required level of accuracy in the preliminary safety analysis report or, alternatively, summarised in the preliminary safety analysis report and specified in more detail in separate topical reports supplementing it.

607. The following information concerning the overall plant design shall be provided:

1. A description of the safety principles and design bases used in the design of the plant and its systems;
2. A description of the series of key standards to be complied with in systems design;
3. A description of the nuclear power plant and its safety-classified systems; overall architecture of systems;
4. A report on the principles of operation of the facility;
5. A description of how the following issues are observed in the overall plant design and in the design of the safety-classified systems:
   a. the practical implementation of the defence in depth concept and independence between the levels in the overall plant design;
   b. the implementation of the redundancy, physical separation, functional isolation and diversity principles in all plant systems performing safety functions required in the various operational states of the plant;
   c. the layout of systems and the related structures and components;

   d. the protection against internal and external hazards;
   e. the plans to cope with an aircraft crash;
   f. the principles related to the avoidance of human errors;
   g. a summary of the results of the deterministic and probabilistic safety analyses including estimated environmental consequences of severe reactor accidents;
6. the principal organisations involved in the design of the plant and its systems, and a description on how they satisfy the requirements set for design organisations in Section 3 of the present Guide;
7. The principal organisations involved in the implementation of the project and their plans for quality management; and
8. the licence applicant's own assessment on how the plant and the participating organisations satisfy Finnish safety and quality requirements.

608. The preliminary safety analysis report shall provide an overview of the plant-wide design principles and the technical implementation of each safety-classified system and its relationship with the overall plant complex. When an application for a construction licence is filed, the systems' design shall have been frozen to the extent that the detailed design will not necessitate any substantial changes to the information pertaining to the layout design of the plant, the location of main system components, or the systems listed in para. 609, and that the requirement specifications can be made for the purpose of procuring components and structures.

609. At least the following information shall be provided concerning Safety Class 1, 2 and 3 systems:
1. A description of the system, system functions and interfaces with other systems; at least the information presented in Annex 1 shall be provided;
2. Design bases and requirements concerning the system and the related components and structures:
   a. safety functions and the associated performance requirements as part of the defence-in-depth concept in different operational conditions of the plant;
   b. ambient conditions and the design criteria derived from such conditions;
   c. internal and external threats to the system;
   d. safety classification of the system and its structures and components;
   e. failure criteria and the physical separation, functional isolation and diversity principles to avoid common cause failures;
   f. a description of the analyses, tests and type tests carried out or foreseen for the purpose of validation of the system and its structures and components;
   g. requirements for maintenance, inspections and testing in different operational states of the plant;
   h. requirements for the construction materials;
   i. radiological protection requirements taken into account in the design of the system;
   j. standards and guidelines to be applied in the design;
3. operation and use of the system in different operational conditions of the plant:
   a. normal operation;
   b. system malfunctions; and
   c. anticipated operational occurrences and accidents.
4. methods used for the physical separation of the system and its components (compartmentation, separation by distance, protection), and the preliminary positioning of the components at the plant;
5. functional isolation: interaction with other systems, dependencies on auxiliary systems, and the prevention of fault propagation;
6. a summary of the results of the failure tolerance analysis of the system;
7. a description of how the avoidance of human errors has been taken into account in design; and
8. a preliminary safety assessment independent of the designer drawn up by the licensee.

610. The information listed in para. 609 shall be provided on systems assigned to Class EYT/STUK (non-nuclear) if

1. the system is of plant-specific risk significance as a result of the initiating events arising from its failure;
2. the system (e.g. a fire protection system) protects systems performing safety functions from internal or external threats;
3. the system is used for monitoring the radiation present in the plant, tools, workers or the environment (e.g. an environmental radiation-monitoring network), surface contamination or radioactivity without, however, being assigned to Safety Class 3;
4. the system is necessary for bringing the facility to a controlled state in case of a design basis category DEC event involving a combination of failures (DEC B) or a rare external event (DEC C).

611. Other Class EYT (non-nuclear) systems shall be described to the extent necessary for the assessment of the plant's overall operation.

612. The ability of the plant and its systems to perform the assigned safety functions shall be demonstrated by means of deterministic analyses of anticipated operational occurrences and accidents, which shall be presented in the preliminary safety analysis report. Analyses of internal and external hazards and the main results of structural analyses for the primary circuit and the containment shall also be presented in the preliminary safety analysis report.

Probabilistic risk assessment in the design stage

613. A preliminary probabilistic risk assessment shall be prepared based on the information presented in the preliminary safety analysis report. Insofar as there are any details missing, the plant model shall include reliability estimates, the accuracy of which shall be verified after the completion of the final designs. Such reliability estimates shall also be used as the starting point when setting goals to guide the design work regarding the missing details. The requirements pertaining to the probabilistic risk assessment and the related documents are given in Guide YVL A.7.

Proposal for a classification document

614. The safety classification of systems and their components and structures shall be presented in the respective system descriptions and summarised in a separate classification document. The requirements pertaining to the safety classification of systems and the classification document are given in Guide YVL B.2.

6.1.3 Documents to be submitted in the operating license stage

615. According to Section 34 of the Nuclear Energy Decree (161/1988), *the application for an operating licence shall be supplemented with*

3. *an outline of the technical operating principles and solutions, and other arrangements whereby safety has been ensured;*
4. *a description of the safety principles that have been observed, and an evaluation of the fulfilment of the principles.*

616. According to Section 36 of the Nuclear Energy Decree (161/1988),

1) the final safety analysis report;

2) a probabilistic risk assessment;

3) a classification document, which shows the classification of structures, systems and components important to the safety of the nuclear facility, on the basis of their significance with respect to safety […]

Final Safety Analysis Report

617. The final safety analysis report shall provide an as-built description of the plant prior to the loading of nuclear fuel into the reactor. The safety analysis report shall provide an overview of the principles applied in the design of the entire plant and in the design of each system contained in the plant.

618. The following information concerning the overall plant design shall be provided:

1. A description of the safety principles and design bases used in the design of the plant and its systems;
2. A description of the pivotal series of standards complied with in systems design.

3. A description of the nuclear power plant and its safety-classified systems; overall architecture of systems;
4. A report on the principles of operation of the facility;
5. A description of how the following safety issues have been taken into account in the overall plant design and in the design of the safety-classified systems:
   a. the practical implementation of the defence in depth concept and independence between the levels in the overall plant design;
   b. the implementation of the redundancy, physical separation, functional isolation and diversity principles in all plant systems performing safety functions required in the various operational states of the plant;
   c. the layout of systems and the related structures and components;
   d. the protection against internal and external hazards;
   e. the protection against an aircraft crash;
   f. the principles related to the avoidance of human errors; and
   g. a summary of the results of the deterministic and probabilistic safety analyses including estimated environmental consequences of severe reactor accidents.
6. The principal organisations involved in the design of the plant and its systems, and a description of how they satisfy the requirements set for a design organisation in section 3 of the present Guide.
7. The principal organisations involved in the implementation of the project and a description on their quality management programmes.
8. The licence applicant's own assessment on how the plant and the participating organisations satisfy Finnish safety and quality requirements.

619. The technical implementation of each safety-classified system and its relationship with the overall plant complex shall be described in detail, supplementing the system descriptions contained in the preliminary safety analysis report with component specifications and other similar detailed information accumulated during the course of construction. System information may be presented to the required level of accuracy in the final safety assessment report or, alternatively, summarised in the safety assessment report and detailed in separate topical reports supplementing it. The system description of each system shall be submitted to STUK for review as soon as the system design has been brought to completion in all respects and detailed information on the design bases of the system structures and components is available. Similarly, the deterministic analyses of anticipated operational occurrences and accidents demonstrating the performance of the systems shall only be submitted when the design of all systems affecting the course of an anticipated operational occurrence or accident has been brought to completion. The final safety analysis report shall be a compilation of these previously submitted parts unless STUK has, based on its review, indicated a need for changes.

620. In addition to the requirements concerning the content of the preliminary safety analysis report specified in paragraph 609 and Annex, at least the following information shall be provided in the final safety analysis report on any systems assigned to Safety Classes 1, 2 or 3:

1. A detailed description of the implemented system; in particular, the description is to be complemented by assembly and components lists, as well as design bases of the structures and components included in the systems.
2. A layout description detailing how the requirements pertaining to the location and protection of systems, structures and components, and the actions performed on the components during operation have been considered in the layout:
   – the physical separation of components (compartmentation, separation by distance, protection);
   – location requirements for pressure equipment;
   – radiation protection and ventilation zone classification;
   – the collection and monitoring of leaks;

- provisions for component maintenance, inspections and testing, accessibility under operating and accident conditions; and
- ergonomics.

3. A description of the implemented functional isolation: interaction with other systems, dependencies on auxiliary systems, and the prevention of fault propagation;
4. Results of the failure tolerance analysis of the system.
5. A description of the analyses, tests and type tests carried out for the purpose of validation of the system and its structures and components.

621. The information listed in para. 620 shall be provided on systems assigned to Class EYT/STUK (non-nuclear) if

1. the system is of plant-specific risk significance as a result of the initiating events arising from its failure;
2. the system (e.g. a fire protection system) protects systems performing safety functions from internal or external threats;
3. the system is used for monitoring the radiation present in the plant, tools, workers or environment (e.g. an environmental radiation-monitoring network), surface contamination or radioactivity without, however, being assigned to Safety Class 3;
4. the system is necessary for bringing the facility to a controlled state in case of a design basis category DEC event involving a combination of failures (DEC B) or a rare external event (DEC C).

622. Other Class EYT (non-nuclear) systems shall be described to the extent necessary for the assessment of the plant's overall operation.

623. The ability of the systems to perform the safety functions assigned to them in all operational conditions and the observance of the defence in depth approach in compliance with the requirements shall be demonstrated by means of deterministic analyses of anticipated operational occurrences and accidents, which shall be presented in the final safety analysis report. Analyses of internal and external hazards and the main results of structural analyses for the primary circuit and the containment shall also be presented in the final safety analysis report.

Probabilistic risk assessment

624. A probabilistic risk assessment shall be prepared based on the information presented in the final safety analysis report. The requirements pertaining to the probabilistic risk assessment and the related documents are given in Guide YVL A.7.

Classification document

625. The safety classification of systems and their components and structures shall be presented in the respective system descriptions and summarised in a separate classification document. The document shall be kept up-to-date at all times during the construction and operation of the plant. The requirements pertaining to the safety classification of systems and the classification document are given in Guide YVL B.2.

6.2 System modifications

6.2.1 General requirements for documents

626. System descriptions shall be updated in connection with modifications made during the construction and operation of a nuclear power plant.

627. During the operation of a nuclear power plant, conceptual design plans and system-specific pre-inspection documents shall be submitted to STUK for approval for any modifications of Safety Class 1, 2 and 3 systems prior to the commencement of the detailed design of components and structures. Following the approval of the conceptual design plan, system pre-inspection documents shall be submitted to STUK, the approval of which is a precondition for the acceptance of the construction plans of structures and components. The revisions to the final safety analysis report shall be made as specified in the approved system pre-inspection documents. The pre-inspection documents of systems assigned to Class EYT/STUK (non-nuclear) defined in paragraph 621 shall be submitted to STUK for information.

628. A conceptual design plan is not required if the modification is modest enough so as not to entail any revision in the design basis, operating principle or function of the system. The scope and level of detail of the pre-inspection documents concerning the system modification depend on the safety significance of the modification.

629. The final safety analysis report shall be regularly updated during the operation of the nuclear power plant, with due regard to any modifications made at the plant. The final safety analysis report and topical reports shall be updated where necessary based on the results obtained during commissioning.

6.2.2 Conceptual design plan

630. The contents of the system's conceptual design plan shall correspond to that of the preliminary safety analysis report. Additionally, the conceptual design plan shall contain a report on quality management principles, including design reviews and the competence of the design organisation.

631. In connection with system modifications, the conceptual design plan shall demonstrate – by means of a probabilistic risk assessment – that the system modification will not compromise overall plant safety.

6.2.3 System pre-inspection documents

632. System pre-inspection documents shall, as a rule, contain descriptions that correspond to the content of the final safety analysis report.

7 Regulatory oversight of safety design

7.1 Processing of the application for a decision-in-principle

701. STUK reviews the information enclosed with the application for a decision-in-principle for each plant project, requesting further information as it may deem necessary for the preparation of the preliminary safety assessment. No separate approval decisions shall be issued on the documents enclosed with the application; however, STUK may, at the licence applicant's request, give its preliminary opinion on issues concerning the application of safety principles or specific technical solutions.

702. Based on its review, STUK shall prepare a preliminary safety assessment. With regard to the safety design of the plant, the preliminary safety assessment:

1. addresses any issues detected in the plant's design bases or their application in design that may prevent a construction licence from being granted;
2. provides an assessment of the needs for improving the structure of the plant to satisfy Finnish safety requirements; and
3. identifies the design solutions that require closer scrutiny or justification in STUK's view in case the project proceeds.

Guide YVL A.1 includes further requirements on the documentation required for the decision-in-principle.

7.2 Processing of the construction licence

703. STUK first carries out an overall assessment of each document submitted to STUK in connection with the filing of the application for a construction licence, establishing the sufficiency and adequacy of the information provided, and issuing a decision on the document's acceptance for more detailed processing. Documents requiring substantial additions or corrections will be returned to the licence applicant without closer scrutiny. If so, STUK will suspend the processing of the document, notify the licensee or license applicant of this and demand that the party concerned provide the requested additional information by the set date.

704. With regard to plant design, STUK will review and assess the design basis of the plant, the requirement specifications, the analyses substantiating the fulfilment of safety criteria, the implementation of defence-in-depth concept in the design as well as the implementation of redundancy, physical separation, functional isolation and diversity principles in the design and implementation of safety functions.

705. STUK reviews the information provided on the systems in the preliminary safety analysis report broken down into logical subject matters comprising one or several systems. If the performance of the system needs to be demonstrated by means of deterministic analyses of anticipated operational occurrences and accidents, the analyses will be reviewed concurrently with the design information of the systems.

706. STUK reviews the probabilistic risk assessment concurrently with the preliminary safety analysis report, using the observations made in this review when assessing the safety of the plant and each system.

707. When reviewing the PSAR and related design documentation submitted for the construction licence, STUK verifies that the design of the plant and its systems can be used as a design basis for structures and components.

708. When STUK has reviewed all sections of the preliminary safety analysis report and the related topical reports, and there are no further questions or comments to be addressed, STUK will issue an approval decision on the entire document. This decision is a necessary prerequisite for STUK's endorsement of the application for a construction license.

709. With regard to the probabilistic risk assessment in the design stage, STUK issues a separate decision after having ascertained that the assessment demonstrates that the plant meets, with sufficient confidence, the quantitative objectives set by STUK for the probability of severe reactor core damage and a large release of radioactive substances. This decision is another necessary prerequisite for any endorsement of the application for a construction licence.

710. The document concerning the safety classification of systems, structures and components will be approved in its entirety by STUK prior to the issuance, by STUK, of an endorsement for the application for a construction licence.

7.3 Processing of the operating licence

711. STUK reviews the probabilistic risk assessment concurrently with the final safety analysis report, using the observations made in this review when assessing the design of the plant and each of its systems.

712. When STUK has reviewed all sections of the final safety analysis report and there are no further questions or comments to be addressed, STUK will issue an approval decision on the entire document. This decision is a necessary prerequisite for STUK's endorsement of the application for an operating license.

713. STUK accepts the probabilistic risk assessment after the design of the plant has been brought to completion in all respects, and the plant model used in the risk assessment has been updated to reflect the structure of the final plant. A precondition for the endorsement by STUK of the application for an operating licence is that the assessment demonstrates that the plant meets, with sufficient confidence, the quantitative objectives set by STUK for the probability of severe reactor core damage and a large release of radioactive substances.

714. The additions to the safety classification will be reviewed concurrently with the review of the systems' design. A precondition for the endorsement by STUK of the application for an operating licence is that the safety classification is up-to-date and the safety classification document is approved by STUK in its entirety.

7.4 System modifications at nuclear power plants

715. When the plant systems are modified or taken out of use or totally new systems are installed at the plant, STUK will review the conceptual design plans and system pre-inspection documents and approve them prior to starting such modifications.

Definitions

Active failure
Active failure shall refer to failure mechanisms other than passive failure mechanisms (such as malfunctions).

Initiating event
Initiating event shall refer to an identified event that leads to anticipated operational occurrences or accidents.

Diversity principle
Diversity principle shall refer to the backing up of functions through systems or components having different operating principles or differing from each other in some other manner, with all systems or components able to implement a function separately. (Government Decree 717/2013)

Separation principle
Separation principle shall refer to physical and functional separation (Government Decree 717/2013).

Physical separation
Physical separation shall refer to the separation of systems or components from one another by means of adequate barriers, distance or placement, or combinations thereof. (Government Decree 717/2013)

Controlled state
Controlled state shall refer to a state where a reactor has been shut down and the removal of its decay heat has been secured. (Government Decree 717/2013)

Ventilation
Ventilation shall refer to maintaining and improving the quality of indoor air by circulating it; in some rooms of a nuclear power plant, ventilation systems are also used to limit the spread of radioactive substances.

Air conditioning systems
Air conditioning systems shall refer to systems designed to manage the purity, temperature, humidity and movement of indoor air by treating supply air or circulating air.

System
System shall refer to a combination of components and structures that performs a specific function.

Review
Review shall refer to activity undertaken to determine the suitability, adequacy and effectiveness of the measures needed to achieve set objectives.

Qualification
Qualification shall refer to a process to demonstrate the ability to fulfil specified requirements (corresponds to the qualification process of the ISO 9000 standard).

Validation
Validation shall refer to confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. (ISO 9000)

Criticality
Criticality shall refer to a state where the output and loss of neutrons, created in nuclear fission and maintaining a chain reaction, are in equilibrium so that a steady chain reaction continues. (Government Decree 717/2013)

Criticality accident
Criticality accident shall refer to an accident caused by an uncontrolled chain reaction of nuclear fissions. (Government Decree 717/2013)

Operational state:
Operational state shall mean normal operation (DBC 1) and anticipated operational occurrences (DBC 2).

Redundancy

Redundancy shall refer to the use of alternative (identical or diverse) structures, systems or system components, so that any one of them can perform the required function regardless of the state of operation or failure of any other.

Normal power supply systems

Normal power supply systems shall refer to power supply systems whose operation is not secured by safety-classified auxiliary power supply systems located within the plant site.

Anticipated operational occurrence (DBC 2)

Anticipated operational occurrence (DBC 2) shall refer to such a deviation from normal operation that can be expected to occur once or several times during any period of a hundred operating years. (Government Decree 717/2013)

Postulated accident

Postulated accident shall refer to a deviation from normal operation which is assumed to occur less frequently than once over a span of one hundred operating years, excluding design extension conditions; and which the nuclear power plant is required to withstand without sustaining severe fuel failure, even if individual components of systems important to safety are rendered out of operation due to servicing or faults. Postulated accidents are grouped into two classes on the basis of the frequency of their initiating events: a) Class 1 postulated accidents (DBC 3), which can be assumed to occur less frequently than once over a span of one hundred operating years, but at least once over a span of one thousand operating years; b) Class 2 postulated accidents (DBC 4), which can be assumed to occur less frequently than once during any one thousand operating years.

Design extension condition (DEC)

Design extension condition (DEC) shall refer to:

a. an accident where an anticipated operational occurrence or class 1 postulated accident involves a common cause failure in a system required to execute a safety function (DEC A);
b. an accident caused by a combination of failures identified as significant on the basis of a probabilistic risk assessment (DEC B); or
c. an accident caused by a rare external event and which the facility is required to withstand without severe fuel failure (DEC C).

Power supply systems

Power supply system shall refer to systems designed to supply the necessary electrical power to the actuators and instrumentation and control systems of the plant unit.

72-hour self-sufficiency criterion

72-hour self-sufficiency criterion shall means that the system to which the criterion is applied must be able to perform its function for a minimum of 72 hours so that for the first 24 hours no material replenishments (such as filling the water or fuel tank of the system) are needed, and for the following 48 hours provisions and material reserves exist at the plant site to arrange the necessary material replenishments for the system, even if all of the plant's fixed active systems would be inoperable.

Accident

Accident shall refer to postulated accidents, design extension conditions and severe accidents (Government Decree 717/2013).

Passive failure

Passive failure shall refer to a mode of failure that can be treated as an operability deficiency (such as a total or partial lack of a device or operability).

Baseline configuration

Baseline configuration shall refer to a configuration of a product, formally established at a specific point in time, which serves as reference for further activities (ISO 10007).

Random failure

Random failure shall refer to a failure the events of which cannot be anticipated other than by means of statistical or probability-based methods.

Consequential failure

Consequential failure shall refer to a failure caused by a failure of another system, component or structure or by an internal or external event at the facility.

Internal events

Internal events shall refer to events occurring inside a nuclear power plant that may have an adverse effect on the safety or operation of the plant.

Protection I&C systems

Protection I&C systems shall refer to instrumentation and control (I&C) systems that actuate the systems necessary to execute the safety functions whenever required, and control the operation of these systems to prevent or mitigate an accident. Protection I&C systems comprise the entire chain of functions from plant state monitoring to the actuators controlled.

Design organisation

Design organisation shall refer to any organisation involved in design activities, including any design modifications.

Systematic failure

Systematic failure shall refer to failure that is not random failure.

Probabilistic risk assessment

Probabilistic risk assessment (PRA) shall refer to a quantitative assessment of hazards, probabilities of event sequences and adverse effects influencing the safety of a nuclear power plant. (Government Decree 717/2013)

Verification

Verification shall refer to confirmation, through the provision of objective evidence, that set requirements have been fulfilled.

Functional isolation

Functional isolation shall refer to the isolation of systems from one another so that the operation or failure of one system does not adversely affect another system; functional isolation also covers electrical isolation and isolation of the processing of information between systems. (Government Decree 717/2013)

Auxiliary system

Auxiliary system shall refer to a system required to actuate, control, cool or operate a system executing a safety function, or otherwise maintain the conditions required by the operational prerequisites of the safety function.

Safe state

Safe state shall refer to a state where the reactor has been shut down and is non-pressurised, and removal of its decay heat has been secured. (Government Decree 717/2013)

Safety system

Safety system shall refer to a system that has been designed to execute safety functions.

Safety divisions

Safety division shall refer to premises, physically separated from one another, and the components and structures contained therein, where one of the redundant parts of each safety system is placed.

Safety-classified system/structure/component

Safety-classified system/structure/component shall refer to a system, structure or component assigned to safety classes on the basis of its safety significance.

Safety functions

Safety functions shall refer to functions important from the point of view of safety, the purpose of which is to control disturbances or prevent the generation or propagation of accidents or to mitigate the consequences of accidents. (Government Decree 717/2013)

External events

External events shall refer to exceptional situations or incidents occurring in the vicinity of a nuclear power plant that could have a detrimental effect on the safety or operation of the plant.

Severe reactor accident

Severe reactor accident shall refer to an accident in which a considerable part of the fuel in a reactor loses its original structure. (Government Decree 717/2013)

(N+1) failure criterion

(N+1) failure criterion shall mean that it must be possible to perform a safety function even if any single component designed for the function fails.

(N+2) failure criterion

(N+2) failure criterion shall mean that it must be possible to perform a safety function even if any single component designed for the function fails and any other component or part of a redundant system – or a component of an auxiliary system necessary for its operation – is simultaneously out of operation due to repair or maintenance.

Annual dose

Annual dose shall refer to committed effective dose arising from external radiation within the period of one year and from intake of radioactive substances within the same period of time. (Government Decree 717/2013)

Common cause failure

Common cause failure shall refer to a failure of two or more structures, systems and components due to the same single event or cause.

Single failure

Single failure shall refer to a failure due to which a system, component or structure fails to deliver the required performance.

References

1. Nuclear Energy Act (990/1987).
2. Nuclear Energy Decree (161/1988).
3. Government Decree on the Safety of Nuclear Power Plants (717/2013)
4. Government Decree on the Security in the Use of Nuclear Energy (734/2008)
5. Government Decree on Emergency Response Arrangements at Nuclear Power Plants (716/2013)
6. Government Decree on the Safety of Disposal of Nuclear Waste (736/2008)
7. IAEA, Fundamental Safety Principles, Series No. SF-1, November 07, 2006.
8. IAEA, The Management System for Facilities and Activities Safety Requirements, Series No. GS-R-3, July 21, 2006.
9. IAEA, Safety Assessment for Facilities and Activities General Safety Requirements Part 4 Series, No. GSR Part 4, May 19, 2009.
10. IAEA, Safety of Nuclear Power Plants: Design, Series No. SSR-2/1, February 20, 2012.
11. IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants Safety Guide, Series No. GS-G-4.1, April 27, 2004.
12. IAEA, Software for Computer Based Systems Important to Safety in Nuclear Power Plants Safety Guide, Series No. NS-G-1.1, November 14, 2000.
13. IAEA, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide, Series No. NS-G-1.3, March 29, 2002.
14. IAEA, Design of Fuel Handling and Storage Systems in Nuclear Power Plants Safety Guide, Series No. NS-G-1.4, August 08, 2003.
15. IAEA, Deterministic Safety Analysis for Nuclear Power Plants Specific Safety Guide, Series No. SSG-2, January 05, 2010.
16. IAEA, Ageing Management for Nuclear Power Plants Safety Guide, Series No. NS-G-2.12, February 06, 2009.
17. IAEA, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide, Series No. NS-G-1.9, September 23, 2004.
18. IAEA, Design of Emergency Power Systems for Nuclear Power Plants Safety Guide, Series No. NS-G-1.8, September 01, 2004.
19. IAEA, Modifications to Nuclear Power Plants Safety Guide, Series No. NS-G-2.3, October 23, 2001.
20. IAEA, Periodic Safety Review of Nuclear Power Plants Safety Guide, Series No. NS-G-2.10, March 09, 2003.
21. WENRA reference requirements, Appendix E, 6.1.

Appendix Detailed requirements for system descriptions

A01. Description of the systems shall include, in a minimum:

1. A verbal description of the system supplemented by figures, diagrams, lists and tables.
2. For process systems: the main parts and components of the system; interfaces with other systems; process and instrumentation diagrams; a 3D diagram/computer model of the main parts; auxiliary systems (e.g. cooling, power supply) required for the operation of the system; monitoring and control of the system functions; operating parameters in different operational conditions (e.g. pressures, temperatures, volumetric flow rates, cooling capacities); and protection functions and limits related to the operation of the system.
3. For I&C systems: the overall I&C system architecture, including system interfaces, connections and interaction between systems and connections to the outside environment; prioritisation of the commands given by the I&C systems; equipment platforms of programmable systems complete with qualification details.
4. For electrical systems: a main diagram outlining the integrated structure of all electrical systems; the structure and operating parameters of each system (e.g. voltages); monitoring and control of the systems; the switch positions in designed operational conditions; and automatic switching operations in the event of anticipated operational occurrences.
5. For buildings: master plans; structural materials, including coatings and steel or similar claddings; the location of components performing safety functions and main equipment contributing to the power production process inside the buildings; loads and load combinations to be considered in the design of buildings; and methods for mounting components into structures, containment access locks and penetrations.