GUIDE YVL B.1

SAFETY DESIGN OF A NUCLEAR POWER PLANT

Definitions

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.*

With regard to new nuclear facilities, this Guide shall apply as of 1 July 2019 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 Guide YVL B.1 (15.11.2013).

Translation. Original text in Finnish.

STUK • SÄTEILYTURVAKESKUS
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY
Osoite / Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FI-00811 Helsinki, FINLAND
Puh. / Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

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 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 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 Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2018). **[**2019-06-15 **]**

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 Leadership and management for safety
- 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.

[2019-06-15 **]**

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
- YVL E.13 Ventilation and air conditioning equipment of a nuclear facility.

[2019-06-15 **]**

104. The structural radiation protection of a nuclear facility, the radiation protection 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
- YVL C.7 Radiological monitoring of the environment of a nuclear facility.

[2019-06-15 **]**

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 system modifications. This Guide may also be applied to the design of other nuclear facilities.
[2019-06-15 **]**

3 Management of design

3.1 Organisations responsible for design

301. According to Section 7 f of the Nuclear Energy Act (990/1987), safety shall take priority during the construction and operation of a nuclear facility. The holder of a construction/operating license shall be responsible for ensuring that the nuclear facility is constructed and operated in compliance with the safety requirements. **[**2019-06-15 **]**

302. The 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. **[**2019-06-15 **]**

303. The licensee shall ensure the design integrity and safety of the facility during the design, construction, operation and decommissioning of the facility. **[**2019-06-15 **]**

304. The licensee shall have competent and experienced staff at its disposal. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

306. Management systems of organisations participating in the design of a nuclear facility and its safety-classified systems shall be in accordance with requirements 629 and 629a of Guide YVL A.3. The requirements set forth in chapter 3 of the present Guide are applicable to the design organisations. **[**2019-06-15 **]**

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.
[2019-06-15 **]**

308. If an organisation involved in the design of a nuclear facility 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 expert organisation to assess the design if necessary. **[**2019-06-15 **]**

309. Removed. **[**2019-06-15 **]**

3.2 Design processes

310. Removed. **[**2019-06-15 **]**

311. A nuclear facility 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. **[**2019-06-15 **]**

312. The design and implementation of a system 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 defining the applicable requirements to the operation stage. In the life-cycle model, the requirements shall be defined before the phase that will be steered by them. **[**2019-06-15 **]**

313. Each design and implementation stage shall be verified. The verification activities and methods shall be duly planned. **[**2013-11-15 **]**

314. Each design and implementation stage shall be reviewed before the stage is declared as complete (stage review). **[**2019-06-15 **]**

314a. Experts in various technical fields shall participate in performing phase reviews. **[**2019-06-15 **]**

314b. Nuclear safety experts of the design organisation responsible for the nuclear facility entity shall participate in verifying systems important to safety and performing related phase reviews. **[**2019-06-15 **]**

315. The licensee shall reserve the opportunity for themselves to participate in the review of any phase. The licensee shall participate in reviews significant to safety. The licensee shall assess the safety significance of issues possibly remaining open after the review and the preconditions for transitioning to the next stage of the life-cycle model. The licensee shall reserve the right for themselves to forbid the starting of a task that is part of the next phase or to interrupt a started task if it is obvious that the safety requirements are not met. **[**2019-06-15 **]**

316. The organisations involved in the design shall have defined and appropriate processes in place for the purpose of requirement management. **[**2019-06-15 **]**

317. In design tasks involving several fields of technology, appropriate procedures shall be included in the design process to ensure the correct transfer of information between the design tasks and across organisational interfaces. **[**2019-06-15 **]**

318. Removed. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

320. The configuration management processes and procedures shall cover the entire lifecycle of the facility, from design to commissioning and decommissioning. **[**2019-06-15 **]**

321. The configuration management processes and procedures shall define responsibilities and provide a description of the procedures applied in the monitoring of configuration management. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

323. The facility, entities of systems, systems, components, software, auxiliary devices, parameters (settings), interfaces and their related documentation shall be defined as hierarchical configuration units. **[**2019-06-15 **]**

324. Configuration management procedures shall be applied to configuration units and their documentation, including documentation related to verification and validation, throughout the configuration units' life-cycle. **[**2019-06-15 **]**

325. During the nuclear facility's life-cycle, the baseline configuration shall be defined for appropriate points with regard to the operation processes, starting from the design of the nuclear facility. **[**2019-06-15 **]**

326. All changes between baseline configuration levels shall be made in accordance with pre-determined change management procedures. **[**2013-11-15 **]**

327. The configuration system documentation shall be updated in connection with any modifications made. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

329. If there are several configuration management procedures in the supply chain, the licensee shall verify their acceptability and compatibility. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

330a. To allow efficient version management of software-based systems and to manage human factors, software and hardware versions shall be provided with unique identifiers. **[**2019-06-15 **]**

330b. The rooms and systems – including related components, structures and cables – shall be easy to identify. An unambiguous coding system shall be used for identification. **[**2019-06-15 **]**

3.4 Quality plans

331. Before starting the actual design work, a system-specific quality plan shall be prepared to steer the design and implementation of systems important to safety and their modifications according to requirement 628. The same quality plan may be utilised for several systems if the quality objectives, methods for attaining the quality objectives and organisation implementing the plan are the same for all the systems concerned. **[**2019-06-15 **]**

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 performers of the stage review, acceptance criteria, and the applicable decision-making procedures and responsibilities;

7. the procedures used in the management 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. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

334a. The design organisation shall perform assessments of the implementation of quality plans of systems important to safety. The assessments shall be carried out during the design and verification activities so that the implementation of the necessary corrective actions is possible. **[**2019-06-15 **]**

334b. Experts conducting quality plan assessments shall be independent of the design and implementation work and qualified for the task. Cross-technological aspects shall be taken into account in assessments in a systematic fashion. **[**2019-06-15 **]**

335. The requirements pertaining to the delivery-specific quality plan are presented in Guide YVL A.3. Quality plans required by Guides YVL A.3 and YVL B.1 can be combined in small-scale modification work of operating plants. **[**2019-06-15 **]**

3.5 Requirement specifications

336. The requirements concerning a system 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 and its components as well as their modifications throughout the life cycle of the facility. **[**2019-06-15 **]**

337. Requirements that are not considered functional requirements, such as the applicable quality requirements and standards, shall also be specified. **[**2013-11-15 **]**

338. The applicability of the standards used shall be justified in connection with the requirement specification. If an exception is made to a specified standard or guideline, such a departure

shall be justified and its effect assessed. **[**2019-06-15 **]**

339. The requirement specifications shall be unambiguous, consistent and traceable. It shall be possible to verify the fulfilment of the requirements. **[**2013-11-15 **]**

340. Experts who are independent of the design and implementation process shall assess the accuracy, completeness and consistency of the requirement specification of a system important to safety. **[**2019-06-15 **]**

341. The requirements shall be traceable in the various design stages. **[**2019-06-15 **]**

342. Moved to para 334a. **[**2019-06-15 **]**

343. Moved to para 334b. **[**2019-06-15 **]**

344. Removed. **[**2019-06-15 **]**

345. Removed. **[**2019-06-15 **]**

346. Moved to para 348a. **[**2019-06-15 **]**

347. Removed. **[**2019-06-15 **]**

3.6 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. **[**2013-11-15 **]**

348a. The licensee shall request an assessment of a safety-classified system, structure or component from an independent expert organisation if new technology is applied, or tested technology is applied on it in a new way or if its validation requires extensive experimental research. **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

351. The fulfilment of the failure criteria of systems implementing safety functions and their support systems as well as common cause failures shall be assessed by means of failure tolerance analysis when designing the systems or their modifications. If necessary, analyses shall be performed in more detail in different stages of design. **[**2019-06-15 **]**

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 or multiple failures at a time and examine their impact in terms of the operation of the system. **[**2019-06-15 **]**

353. A common cause failure analysis shall be drawn up for anticipated operational occurrences and class 1 postulated accidents. 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, their consequential effects 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. **[**2019-06-15 **]**

354. Removed. **[**2019-06-15 **]**

3.7 Documentation

355. The documentation describing the nuclear facility, 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. **[**2019-06-15 **]**

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

1. allow verification in all design stages so that the specified requirements are duly incorporated in the final system to be commissioned; and
2. ensure that they can be assessed by an independent expert. **[**2019-06-15 **]**

357. The documentation shall be of high quality, unambiguous and traceable. **[**2013-11-15 **]**

358. Up-to-date and valid documentation shall be available to those involved in design and implementation. **[**2013-11-15 **]**

359. The documentation concerning design and implementation shall be consistent and traceable to a frozen baseline of the plant design. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

361. Moved to para 330a. **[**2019-06-15 **]**

3.8 Validation

362. Systems, structures and components important to safety shall be validated, i.e. it shall be demonstrated that they are appropriate for their purpose of use and fulfil the set safety requirements. **[**2019-06-15 **]**

363. A qualification plan shall be prepared for the system to guide the validation 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 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. **[**2019-06-15 **]**

364. The licensee shall evaluate the acceptability of the validation results and present a justified conclusion drawn from the results. **[**2019-06-15 **]**

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 practically possible* (the SAHARA principle). **[**2019-06-15 **]**

402. According to Section 11(1) of STUK regulation STUK Y/1/2018, *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.* **[**2019-06-15 **]**

403. According to Section 11(2) of STUK regulation STUK Y/1/2018, *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 a power supply, will settle in a state preferable from the safety point of view.* **[**2019-06-15 **]**

404. The design basis for all systems, structures and components of the nuclear power plant shall be the environmental conditions in which they are required to operate. Environmental conditions to be considered in the design shall include, as appropriate, vibration, temperature, pressure, electromagnetic effects, radiation, humidity, fluid properties and combinations of these conditions. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

407. Removed. **[**2019-06-15 **]**

408. In the design phase, solutions shall be preferred that can help restrict the accumulation of radioactive waste during the operation and decommissioning of the plant and facilitate the dismantling of the facility. In particular, attention shall be given to the selection of materials and system design, so that the effects of neutron activation can be limited, decontamination is

facilitated and the future amount of radioactive waste remains as small as practically possible. The design shall include the facilities required for the processing and storage of radioactive waste generated during operation, and the treatment of radioactive waste generated in the decommissioning of the plant shall also be anticipated. **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

411. If shared structures, systems and components important to safety are designed for nuclear power plant units and fuel storage facilities located at the same plant site, it shall be demonstrated that the solution is beneficial for the plants' safety. Fault propagation through shared structures, systems and components shall be prevented. The functions needed by each unit shall, when necessary, be implemented also in the event of a transient or accident occurring simultaneously at the plants. **[**2019-06-15 **]**

412. Removed. **[**2019-06-15 **]**

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.* **[**2013-11-15 **]**

414. The nuclear power plant design shall take into account events that may cause a deviation of the plant parameters from normal values and threaten integrity of the nuclear fuel or other barriers. 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. **[**2019-06-15 **]**

414a. A transient or accident occurring simultaneously at nuclear power plant units and other nuclear facilities located at the plant site shall be considered in the design of a nuclear power plant. **[**2019-06-15 **]**

415. Removed. **[**2019-06-15 **]**

416. Removed. **[**2019-06-15 **]**

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.5, B.7, B.8, A.11 and A.12. **[**2019-06-15 **]**

4.3 Application of the defence in depth principle in the design

418. According to Section 11(3) of STUK regulation STUK Y/1/2018, *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 a malfunction.* According to Section 11(5) of STUK regulation STUK Y/1/2018, *common cause failures shall only have minor impacts on nuclear power plant safety.* **[**2019-06-15 **]**

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 functional and structural safety of the plant.* **[**2013-11-15 **]**

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 9(1) of STUK regulation STUK Y/1/2018 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 facility.* **[**2019-06-15 **]**

421. According to Section 9 of STUK regulation STUK Y/1/2018, *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 facility. In accordance with the functional defence-in-depth safety principle, the design of a nuclear facility must include the following levels of defence:*
1) prevention to ensure that the operation of the nuclear facility is reliable and deviations from normal operating conditions are rare;
2) control of deviations from the nuclear facility's normal operating conditions so that the facility is equipped with systems which are able to limit the development of operational occurrences into accidents and if required can bring the facility into a controlled state;

3) control of accident situations so that the nuclear facility is equipped with systems that function automatically and reliably to prevent severe fuel damage in postulated accidents and in design extension conditions; manually actuated systems can be used to manage accident situations if it can be justified from a safety perspective;
4) confinement of a release of radioactive substances in severe reactor accidents by equipping the nuclear power plant with systems which ensure the sufficient leak tightness of the containment in severe reactor accidents so that the limits for releases in severe reactor accidents are not exceeded;
5) mitigation of the consequences by means of emergency arrangements to limit the public's exposure to radiation in situations where radioactive substances are released from the nuclear facility into the environment. **[**2019-06-15 **]**

421a. The third level of defence shall be divided into level 3a and level 3b. 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 materials. At level 3b, the objective is to control design extension conditions so that severe fuel damage can be prevented. **[**2019-06-15 **]**

421b. An anticipated operational occurrence or class 1 postulated accident involving a common cause failure in a system required to execute a safety function in safety class 2 shall be regarded as a design extension condition DEC A. **[**2019-06-15 **]**

421c. A common cause failure of any individual component type (for example, a similar check valve, same type and manufacturer) shall not prevent the nuclear power plant from being brought to a controlled state or a safe state. **[**2019-06-15 **]**

421d. Failure combinations recognised as significant based on probabilistic risk assessment shall be processed as a design extension condition DEC B. Furthermore, such failure combinations or additional failures that emerge during the initiating event, and could significantly affect the integrity of fuel, the radiological effects of the accident or primary circuit pressure shall be considered. **[**2019-06-15 **]**

422. Removed. **[**2019-06-15 **]**

423. Events that result in a release requiring measures to protect the population in the early stages of the accident shall be practically eliminated. **[**2019-06-15 **]**

423a. Events leading to a large release shall be practically eliminated. **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

4.3.1 Independence of the defence in depth levels

425. According to Section 9(3) of STUK regulation STUK Y/1/2018, *the levels of defence required under the defence-in-depth principle shall be as independent of one another as is reasonably achievable.* **[**2019-06-15 **]**

426. Independence between the levels of defence shall be based on the adequate application of functional isolation, the diversity principle and physical separation. **[**2019-06-15 **]**

427. Removed. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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 failure on one level shall not prevent the implementation of necessary functions at other levels of defence. **[**2019-06-15 **]**

430. Removed. **[**2019-06-15 **]**

431. The systems intended for reaching and maintaining a controlled state in severe reactor 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 reactor accident.
[2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

434. The redundant parts of a system performing safety functions shall be assigned to different safety divisions. **[**2013-11-15 **]**

435. The failure of a subsystem in a system executing safety functions shall not cause the failure of another redundant subsystem of the same system or the failure of several subsystems participating in the same safety function. **[**2019-06-15 **]**

436. Removed. **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

439. If the redundant parts of a safety function are interconnected for the distribution of electricity or control signals, the safety advantage as compared to a solution without such interconnection shall be justified. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

441. Removed. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

442a. The consequences caused by an initiating event to the systems needed to execute safety functions shall be identified. The failure criterion shall be applied in addition to any consequential failures possibly caused by the initiating event. **[**2019-06-15 **]**

443. More detailed requirements concerning the physical separation of systems and components are given in Guides YVL B.7 and YVL B.8. **[**2019-06-15 **]**

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

444. Removed. **[**2019-06-15 **]**

445. In anticipated operational occurrences, it shall be possible to limit reactor power, if necessary, in order to ensure that the limit values set for fuel integrity, radiological consequences and primary circuit pressure during anticipated operational occurrence shall not be exceeded. The necessary limitation functions shall meet the failure criterion according to requirement 456. It shall also be possible to quickly shut down the reactor, if necessary, by a system based on solid neutron absorbers so that the acceptance criteria are fulfilled. **[**2019-06-15 **]**

445a. 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 class 1 or class 2 postulated accidents 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. **[**2019-06-15 **]**

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 in such a way that the limits set forth for fuel integrity, radiological consequences and overpressure protection in design extension conditions. The shutdown system that complies with the diversity principle shall satisfy the (N+1) failure criterion. **[**2019-06-15 **]**

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 extension conditions are not exceeded. **[**2019-06-15 **]**

448. It shall be possible to carry out fuel cooling in the reactor and the removal of residual heat from the reactor and containment in anticipated operational occurrences so that the limit values set for fuel integrity, radiological consequences and overpressure protection are not exceeded. The necessary limitation functions shall meet the failure criterion according to requirement 456. **[**2019-06-15 **]**

448a. It shall be possible to accomplish decay heat removal from the reactor and containment in postulated accidents 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 class 1 or class 2 postulated accidents 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. **[**2019-06-15 **]**

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 extension conditions DEC A 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 class 1 or class 2 postulated accidents are not exceeded, the system can also be counted among the systems that jointly meet the (N+2) failure criterion given in requirement 448. **[**2019-06-15 **]**

450. It shall be possible to carry out the removal of residual heat from the reactor to outside the containment in events involving a combination of failures (DEC B) so that the limit values set for fuel integrity, radiological consequences and overpressure protection are not exceeded under design extension conditions. Systems needed in the events shall fulfil the self-sufficiency criterion. It is not necessary to apply the single failure criterion to the arrangements. **[**2019-06-15 **]**

450a. It shall be possible to carry out the removal of residual heat from the reactor outside the containment in rare external events (DEC C) so that that the limit values set for fuel integrity, radiological consequences and overpressure protection are not exceeded under design extension conditions. Systems needed in the events shall be stationary and meet the self-sufficiency criterion. Measures related to the use of the systems and conducted at the plant site shall not require the use of vehicles during the first eight hours. Components designed for use shall be accessible even if any individual route or hatch were blocked by an external obstacle. It is not necessary to apply the single failure criterion to the arrangements. **[**2019-06-15 **]**

451. The design of a nuclear power plant shall provide for the loss of the power distribution network caused by an electrical transient or prevent it. The event shall primarily be prevented in accordance with the general DEC A design principles with electrical power distribution systems that fulfil the diversity principle and (N+1) failure criterion as well as by separating the severe reactor accident management systems from other systems. If the situation is managed through additional arrangements deviating from this, the DEC B design criteria shall be applied to the additional arrangements. Design extension condition acceptance criteria for fuel integrity, radiological consequences and overpressure protection shall be applied to the event. **[**2019-06-15 **]**

452. Removed. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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

454. The reactor shall be kept subcritical in all its possible temperatures without a scram system based on solid neutron absorbers. Subcriticality can also be ensured with merely solid neutron absorbers in situations where they are operable. The function shall fulfil the single failure criterion. **[**2019-06-15 **]**

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 common cause failure conditions (DEC A) by decay heat removal systems meeting the (N+1) failure criterion. **[**2019-06-15 **]**

455a. It shall be possible to cool the reactor from a controlled state to a safe state and keep it in the safe state on a long-term basis in events involving a combination of failures (DEC B) and rare external events (DEC C). It is not necessary to apply the single failure criterion to the required systems. **[**2019-06-15 **]**

455b. Provisions shall be made to enable the repair and servicing of the systems needed for maintaining the safe state. **[**2019-06-15 **]**

455c. After anticipated operational occurrences, postulated accidents and design extension conditions, the plant shall, in the long term, be brought into a state where fuel removal from the reactor is possible. **[**2019-06-15 **]**

4.3.5 Other redundancy requirements

456. Functions designed to mitigate the consequences of anticipated operational occurrences shall meet the (N+1) failure criterion. **[**2019-06-15 **]**

456a. The instrumentation referred to in requirement 5214 of Guide YVL B.1 shall meet the (N+1) failure criterion. **[**2019-06-15 **]**

456b. Active components of the systems designed to reach and maintain the controlled state in severe reactor accidents shall satisfy the (N+1) failure criterion. **[**2019-06-15 **]**

456c. Functions, whose purpose is to prevent the propagation of radioactive substances if the components or structures containing such substances break down or operate erroneously, shall meet the (N+1) failure criterion. **[**2019-06-15 **]**

456d. Systems necessary for maintaining safe working conditions in the control room shall satisfy the (N+1) failure criterion. **[**2019-06-15 **]**

456e. The containment isolation function shall satisfy the (N+1) failure criterion in postulated accidents in spite of possible maintenance, repair or testing operations on the I&C or other auxiliary systems needed to perform the isolation function. In design extension conditions DEC A, the I&C and auxiliary systems needed to perform the containment isolation function shall meet the (N+1) failure criterion. Design extension conditions DEC B and C do not require failure postulation. Detailed requirements concerning the containment isolation function are provided in Guide YVL B.6. **[**2019-06-15 **]**

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, YVL B.5, YVL B.6 and YVL D.3. **[**2019-06-15 **]**

4.4 Consideration of human factors relating to safety

458. According to Section 6 of STUK regulation STUK Y/1/2018, *human factors relating to safety shall be controlled with systematic procedures throughout the entire life cycle of the nuclear facility. Human factors shall be taken into account in the design of the nuclear facility and in the planning of its operations, maintenance and decommissioning in a manner that supports the high-quality implementation of the work and ensures that human activities do not endanger plant safety. Attention shall be paid to the avoidance, detection and correction of human errors and the limiting of their effects.* **[**2019-06-15 **]**

458a. In new projects, the HFE programme (Human Factors Engineering) shall be used to design the control, testing, review and maintenance of systems important to safety, with the following areas included where applicable:

1. Managing the HFE programme
2. Utilisation of operating experience
3. Analysis and allocation of functions
4. Task analyses
5. Analysis of staff members and competences
6. Processing of human tasks significant to safety
7. Design of user interfaces
8. Planning of instructions
9. Planning of training programmes
10. Verification and validation related to human factors
11. Installation and commissioning
12. Assessment and monitoring of functionality during operation. **[**2019-06-15 **]**

458b. For the purpose of designing nuclear power plant modifications, a HFE programme in accordance with requirement 458a shall be prepared in the extent appropriate for the modification. **[**2019-06-15 **]**

459. Removed. **[**2019-06-15 **]**

460. Removed. **[**2019-06-15 **]**

461. Removed. **[**2019-06-15 **]**

462. Moved to para 330b. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5102. The design of the plant shall provide a secondary ultimate heat sink for decay heat removal in the event of unavailability of the primary ultimate heat sink. The secondary ultimate heat sink shall fulfil the 72-hour self-sufficiency criterion. The prevention of the use of the heat sink can be provided for with arrangements fulfilling the DEC C requirements if residual heat removal from the reactor and containment into the final heat sink as well as cooling required by safety functions during anticipated operational occurrences or class 1 postulated accidents can otherwise be executed with functions that fulfil the diversity principle. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5106. In order to detect leaks from the primary circuit and the systems directly associated with it, procedures and systems shall be designed that provide information on the leak and its scope quickly enough and which can be used to locate the leak with sufficient accuracy. When following the Leak Before Break principle, the requirements concerning the required leakage monitoring system are presented in Guide YVL E.4. **[**2019-06-15 **]**

5107. Removed. **[**2019-06-15 **]**

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, to compensate for any loss of coolant or to otherwise provide efficient reactor cooling in order to ensure that the design limits for fuel are not exceeded. Requirements related to residual heat removal systems apply to the emergency core cooling system. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5110. The primary circuit configuration and the positioning of the emergency cooling connections must be designed in a manner that helps steer the coolant flow into the reactor core. **[**2019-06-15 **]**

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 solid 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 and other components required for cooling, or reduce the efficiency of nuclear fuel 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.
[2019-06-15 **]**

5111a. If, as a result of an initiating event, impurities can end up in the cooling water of a residual heat removal system of the containment or another cooling system needed in the accident, solid or chemical impurities shall be considered in its design. To control solid 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 representatively aged insulation and coating materials. The following factors shall be taken into account in designing the filtering structures:
1. The quantity of impurities passing through the filters is low enough so as not to interfere with the operation of the coolant recirculation pumps and other components required for cooling.
2. The pressure loss caused by the impurities trapped by the filtering structures does not prevent the coolant recirculation system from performing as designed.
3. The filtering structures can be cleaned by means of a reversed coolant flow or gas blowdown if the pressure loss across the filters suggests a risk of excessive clogging. **[**2019-06-15 **]**

5.2 Instrumentation and control systems

5.2.1 General requirements

5201. Removed. **[**2019-06-15 **]**

5202. The same procedures shall be followed in the design of a system entity of I&C systems, meaning architecture-level design, as in the design of systems in the highest safety class which are included in the architecture. **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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 validated. Detailed requirements for the validation of tools are specified in Guide YVL E.7. Each tool version shall be specifically validated. **[**2019-06-15 **]**

5206. No solutions based on wireless data transfer may be used in the safety functions. **[**2013-11-15 **]**

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 factors. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5210. The operators in the control room shall have access to clearly presented and reliable information on the status of the nuclear power plant. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5212. In the validation 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. **[**2019-06-15 **]**

5.2.3 Instrumentation

5213. Instrumentation shall be designed to give accurate and reliable input data to the I&C systems performing safety functions. **[**2019-06-15 **]**

5214. A nuclear power plant shall have instrumentation that the operator can use to monitor the plant's status and the execution of safety functions in order to restore the controlled state and maintain it in anticipated operational occurrences, postulated accidents and design extension conditions DEC A. Such instrumentation shall include all the devices in the data transmission connection all the way from the sensor to the display unit. **[**2019-06-15 **]**

5214a. The licensee shall prepare and maintain a list of the instrumentation required in YVL B.1 requirement 5214 and YVL C.6 requirement 402a. **[**2019-06-15 **]**

5215. The nuclear reactor instrumentation 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. **[**2019-06-15 **]**

5216. Nuclear reactor instrumentation shall provide adequate information for detecting any abnormal operational conditions related to the reactor core, including indication of any incorrect positioning of the reactor internals or the fuel. **[**2019-06-15 **]**

5217. Monitoring instrumentation shall be provided for the primary circuit to detect any loose objects. **[**2019-06-15 **]**

5217a. The containment shall have instrumentation in place that can be used for monitoring the operation of the containment system. **[**2019-06-15 **]**

5218. The containment shall have instrumentation for the purpose of monitoring and controlling postulated accidents and design extension conditions in order to gain sufficient information on the state of the containment. **[**2019-06-15 **]**

5219. For the monitoring of severe reactor accidents, the containment shall be equipped with independent measuring and monitoring instrumentation that provides sufficient information on the progress of potential severe reactor accidents and any circumstances that may jeopardise containment integrity. **[**2019-06-15 **]**

5220. The measurement systems together shall be capable of performing measurements over the full range within which the parameters being measured may vary in normal operation,

anticipated operationa occurrences or accidents. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5.2.4 Operational and limitation 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’. **[**2013-11-15 **]**

5224. The operational and limitation I&C shall maintain the process parameters within a range consistent with normal operation as well as monitor the condition of plant systems, structures and components. **[**2019-06-15 **]**

5225. Removed. **[**2019-06-15 **]**

5226. A nuclear power plant shall have limitation functions which, either automatically or with the assistance of operators, launch the corrective control and adjustment measures during anticipated operational occurrences (limitation I&C). **[**2019-06-15 **]**

5227. The operating and alarm limits of the operational and limitation I&C 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 protection automation. **[**2019-06-15 **]**

5.2.5 Protection I&C systems

5228. A nuclear power plant shall be provided with a protection system that actuates the necessary systems for providing safety functions in postulated accidents and controls the operation of these systems to mitigate the consequences of postulated accidents. **[**2019-06-15 **]**

5228a. A nuclear power plant shall have a back-up protection system that launches the systems implementing safety functions during anticipated operational occurrences or class 1 postulated accidents in connection with a common cause failure of the protection system, such that the limit values set for fuel integrity, radiological consequences and overpressure protection

are not exceeded under design extension conditions. **[**2019-06-15 **]**

5229. The actuation of a safety function by the protection system 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. **[**2019-06-15 **]**

5230. If it is not possible to define two different process parameters for the detection of an event requiring actuation of a safety function according to the requirement 5229, at least two different principles of measurement shall be applied for measuring the single process parameter used for detection. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5232. It shall be possible to test the protection automation during the operation of the plant. The test concept shall be designed so that for the duration of all tests, the part of the I&C system downstream of the section being tested can be brought to a state preferable from the plant safety point of view. **[**2019-06-15 **]**

5233. The periodic tests of the protection automation shall cover the entire chain from measurements to actuators. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5.2.6 Controls of severe reactor accident management

5235a. In order to achieve and maintain a controlled state after a severe reactor accident, the nuclear power plant shall have controls that are independent of the plant's other I&C systems. The controls can be implemented with operators or automatically. The controls shall fulfil the single failure criterion. **[**2019-06-15 **]**

5235b. The instrumentation of severe reactor accidents, intended for monitoring the propagation of the accident and the state of the nuclear power plant, shall fulfil the single failure criterion. **[**2019-06-15 **]**

5235c. It shall be possible to periodically test the controls and instrumentation of severe reactor accident management. Periodic tests shall cover the entire measurement and control chain. **[**2019-06-15 **]**

5.2.7 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. **[**2013-11-15 **]**

5237. Removed. **[**2019-06-15 **]**

5238. Removed. **[**2019-06-15 **]**

5239. Removed. **[**2019-06-15 **]**

5240. The consequences of I&C failures shall be limited in accordance with the following requirements in so far as they are not already limited by other requirements:
1. A failure of class EYT I&C as an initiating event shall not lead to consequences that are worse than an anticipated operational occurrence.
2. A failure of class EYT I&C during anticipated operational occurrences and accidents shall not essentially degrade the plant state (the acceptance criterion of the event remains within the same event class).
3. A failure of safety class 3 I&C as an initiating event shall not lead to consequences that are worse than a class 1 postulated accident.
4. A failure of safety class 3 I&C in connection with an anticipated operational occurrence shall not lead to consequences that are worse than a class 1 postulated accident.
5. A failure of safety class 3 operational and limitation I&C during accidents shall not essentially degrade the plant state.

6. A failure of safety class 3 back-up protection system or safety class 3 severe reactor accident I&C shall not essentially degrade the plant state In postulated accidents. **[**2019-06-15 **]**

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 concerning failures. **[**2019-06-15 **]**

5242. The interfaces between systems shall be defined as part of the design of the I&C architecture. **[**2013-11-15 **]**

5243. The data communications systems of the I&C systems important to safety shall satisfy the response time requirements during normal operation, anticipated operational occurrences and accidents. This shall be demonstrated for all conceivable load conditions. **[**2019-06-15 **]**

5244. Moved to Guide YVL A.12. **[**2019-06-15 **]**

5245. Moved to Guide YVL A.12. **[**2019-06-15 **]**

5246. Detailed information security requirements are provided in Guide YVL A.12. **[**2019-06-15 **]**

5247. Removed. **[**2019-06-15 **]**

5248. Removed. **[**2019-06-15 **]**

5249. Removed. **[**2019-06-15 **]**

5250. Removed. **[**2019-06-15 **]**

5251. Removed. **[**2019-06-15 **]**

5252. Moved to Guide YVL E.7. **[**2019-06-15 **]**

5253. Removed. **[**2019-06-15 **]**

5254. Removed. **[**2019-06-15 **]**

5255. Removed. **[**2019-06-15 **]**

5256. Removed. **[**2019-06-15 **]**

5257. Removed. **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

5302. Due consideration shall be given to human factors and organisational circumstances right from the outset when designing the control room operations or modifications affecting the control room. **[**2019-06-15 **]**

5303. The control room operations, the procedures required for the control of the nuclear power plant and competence of the operators shall form an ensemble, whose appropriateness shall be ensured using the plant simulator. Similarly, the appropriateness of any modifications to the control room procedures and significant ergonomic changes shall be ensured in advance by means of tests carried out in the plant simulator. **[**2019-06-15 **]**

5304. The parts of the instrumentation and controls of protection I&C and severe reactor accident management that implement the redundancy principle shall be separated from each other functionally within control rooms. **[**2019-06-15 **]**

5305. The control room, emergency control room, command centre for emergency preparedness and other rooms needed under accident conditions 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 and ventilation, noise abatement, radiation protection and access control. **[**2019-06-15 **]**

5306. The main control room and the emergency control room shall be physically separated to ensure they aren't damaged due to the same internal or external event. **[**2019-06-15 **]**

5.3.2 Main control room

5307. According to Section 16(1) of STUK regulation STUK Y/1/2018, *a nuclear facility shall contain equipment that provides information on the operational state of the facility and any deviations from normal operation.* **[**2019-06-15 **]**

5308. According to Section 16(3a) of STUK regulation STUK Y/1/2018, *in order to control the nuclear power plant and enable operator actions, the nuclear power plant shall have a control room, in which the majority of the user interfaces required for the monitoring and control of the nuclear power plant are located. The scope of monitoring and control duties performed outside the control room shall be designed according to their feasibility.* **[**2019-06-15 **]**

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. The support function shall also include the management of accidents during outages. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5311. The displays for measurement and status data of instrumentation needed by the operator during transients and accidents, and referred to in requirements 5214 in Guide YVL B.1 and requirement 402a in Guide YVL C.6, shall be visually distinguishable from other displays. **[**2019-06-15 **]**

5312. The main control room shall provide facilities for monitoring the state of the off-site grid. **[**2013-11-15 **]**

5313. A qualification plan shall be provided for the control room and the other necessary monitoring and control posts when the application for a construction license is filed. **[**2019-06-15 **]**

5.3.3 Emergency control room

5314. According to Section 16(4) of STUK regulation STUK Y/1/2018, *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 the nuclear reactor and for removing decay heat from the nuclear fuel in the reactor and the spent nuclear fuel stored.* **[**2019-06-15 **]**

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. **[**2019-06-15 **]**

5316. A safe passage shall be provided from the main control room to the emergency control room. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5318a. Requirements pertaining to the design of the control room and emergency control room are specified in Guide YVL A.11. **[**2019-06-15 **]**

5.4 Electrical power systems

5401. According to Section 11(6) of STUK regulation STUK Y/1/2018, *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.* **[**2019-06-15 **]**

5401a. The same procedures shall be followed in the design of a system entity of electrical systems, meaning architecture-level design, as in the design of systems in the highest safety class which are included in the architecture. **[**2019-06-15 **]**

5402. The plant shall be provided with systems permitting power supply from the main generator to the plant systems in case the connection to the off-site grid is lost. **[**2019-06-15 **]**

5403. The off-site and on-site system 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. **[**2019-06-15 **]**

5404. Removed. **[**2019-06-15 **]**

5405. Cross-connections between the redundant parts of safety-classified electrical systems shall be avoided unless they are demonstrated to improve the safety of the nuclear facility. **[**2019-06-15 **]**

5406. 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. **[**2019-06-15 **]**

5407. The propagation of faults from one redundant electrical system part to another via cross-connections shall be reliably prevented. **[**2019-06-15 **]**

5408. Plant-specific frequency and voltage variations caused by an external grid, and those caused by electrical components or failures of the plant, shall be analysed. **[**2019-06-15 **]**

5409. Frequency and voltage fluctuations analysed according to the requirement 5407 shall not endanger the safety functions during normal operation, anticipated operational occurrences or accidents. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5412. Removed. **[**2019-06-15 **]**

5413. Removed. **[**2019-06-15 **]**

5414. Electrical systems and equipment utilizing software-based technology shall fulfill the requirements of Section 5.2. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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). **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5418. The independent off-site grid connections according to 5417 shall be designed to ensure that a simultaneous failure of both connections due to the same cause remains unlikely. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5421. Removed. **[**2019-06-15 **]**

5422. The plant shall be provided with a reliable switch-over automation to permit automatic switch-over between the off-site grid connections. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2019-06-15 **]**

5425. Removed. **[**2019-06-15 **]**

5.4.2 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. **[**2013-11-15 **]**

5426a. The design of on-site emergency power supply shall provide for a common cause failure in the supply system during operational occurrences and class 1 postulated accidents when off-site electrical power supply is lost. DEC A design requirements and acceptance criteria shall be applied to the situation. The provisions can be implemented by complying with the diversity principle in the emergency power supply system, for example, or by designing an independent emergency power supply system in accordance with the diversity principle. **[**2019-06-15 **]**

5426b. In order to manage severe reactor accidents, an on-site emergency power supply system shall be available that fulfils the (N+1) failure criterion and is independent of systems designed for normal operation, anticipated operational occurrences, postulated accidents and design extension conditions. **[**2019-06-15 **]**

5427. The on-site emergency power supply systems shall fulfil the 72-hour self-sufficiency criterion in postulated accidents and design extension conditions. **[**2019-06-15 **]**

5427a. It shall be possible to provide emergency power supply during severe reactor accidents without water, fuel or any other material replenishments external to the plant for 72 hours. **[**2019-06-15 **]**

5428. Removed. **[**2019-06-15 **]**

5429. It shall be possible to actuate the on-site emergency power supply systems manually from the main control room. **[**2019-06-15 **]**

5430. It shall be possible to switch from the on-site emergency power supply referred to in requirements 5426 and 5426a back to the regular off-site electrical power supply using the manual controls in the main control room provided that the regular off-site electrical power supply is available. **[**2019-06-15 **]**

5431. The on-site emergency power supply systems 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). **[**2019-06-15 **]**

5432. The quality of the alternating current supplied by the on-site emergency power supply systems shall be consistently maintained to ensure that the operability of the supplied

components is not endangered. [2019-06-15]

5433. More detailed requirements regarding the equipment used for emergency power supply at nuclear power plants are specified in Guide YVL E.10. [2013-11-15]

5434. The on-site emergency power supply systems 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. [2019-06-15]

5435. It shall be possible to safely isolate redundant parts of the on-site emergency power supply systems from other electrical systems or system parts for the purpose of functional testing, maintenance and repairs. [2019-06-15]

5436. Removed. [2019-06-15]

5437. Removed. [2019-06-15]

5438. Removed. [2019-06-15]

5439. Removed. [2019-06-15]

5440. Removed. [2019-06-15]

5.4.3 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. [2013-11-15]

5442. Battery sets, charging devices and any converters shall be dimensioned so as to assure the operability of components requiring uninterrupted power supply in accordance with the specified operating time requirements. [2019-06-15]

5443. The battery sets supplying loads important to safety shall be dimensioned to provide at least two-hour discharge time under the highest conceivable load. [2019-06-15]

5444. The battery sets supplying severe accident management systems shall be dimensioned to provide a 24-hour discharge time under the highest conceivable load. [2013-11-15]

5445. The dimensioning criteria for the safety-classified start-up batteries of combustion engines and special-purpose batteries shall be substantiated for each location of use. [2019-06-15]

5446. Removed. [2019-06-15]

5447. The charging devices of the battery sets important to safety and related to uninterruptible power supply systems shall be dimensioned to operate even under extreme load conditions (e.g. charging of discharged battery sets and simultaneous supply of loads following a power failure) and operating conditions. **[**2019-06-15 **]**

5448. The safety classified uninterruptible power supply devices shall be capable of supplying the necessary direct current to the components being supplied s even if the battery set is disconnected so that their operability of components is not endangered. **[**2019-06-15 **]**

5449. In the event that uninterruptible power supply is provided while the battery sets are disconnected, the electricity shall be of sufficiently high quality not to cause any disruptions to the components being supplied. **[**2019-06-15 **]**

5450. The uninterruptible power supply systems important to safety shall be designed to reliably prevent the transmission of potential disruptions in the supplying alternating current power grid to the final consumers. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5.4.4 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 receiving unit can be maintained in a controlled state in case of loss of electrical power. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5.4.5 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. **[**2013-11-15 **]**

5456. Electrical and I&C 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. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5458. Detailed EMC requirements shall be defined in the requirement specifications for safety-classified electrical and I&C systems and components. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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). **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5462. A radio frequency table shall be created for the nuclear power plant in support of the preparation of EMC specifications and qualification. **[**2013-11-15 **]**

5463. The radio frequency table shall list all the radio frequencies allowed on the nuclear power plant site, including the highest permissible field intensities. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5.4.6 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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5.4.7 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. **[**2013-11-15 **]**

5471. Fault currents shall be cut off quickly enough to avoid hazards and to minimise disruptions. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5473. Adequate alarms shall be provided to ensure that any electrical failures can be promptly detected, located and repaired. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5475. The operation of the protection devices of safety-classified electrical power systems shall be capable of being tested across the entire protection chain. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5478. Removed. **[**2019-06-15 **]**

5479. Any protection devices placed in service to safeguard components during testing shall be designed in such a way that their operation does not endanger the operational capability of the system during an actual event. **[**2019-06-15 **]**

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
1. reduce the concentrations of airborne radioactive substances within the plant;
2. prevent the spread of radioactive substances to other areas within the plant; and
3. limit the release of radioactive substances to the environment. **[**2019-06-15 **]**

5502. The ventilation and air conditioning systems shall maintain and ensure such ambient conditions in all the rooms of a nuclear power that the components and structures important to safety are kept in good condition and operate flawlessly. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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). **[**2013-11-15 **]**

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 when necessary. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5507. Safety divisions shall have separate ventilation and air conditioning systems. Rooms containing parts of several safety divisions in the containment and control room constitute an exception. The exhaust ducts of safety divisions in the controlled area can be combined outside the safety divisions right before the ventilation stack when the ducts are equipped with sufficient smoke and fire isolation. **[**2019-06-15 **]**

5508. The ventilation and air conditioning systems shall perform their functions, determined for the situation in question, during normal operation, anticipated operational occurrences and accidents. Conditions to which systems may be exposed during the situation shall be used as the design basis for the ventilation and air conditioning systems designed to operate during accidents or thereafter. **[**2019-06-15 **]**

5509. A definition of room conditions shall be made for rooms with equipment important to safety. The definition of room conditions shall cover the factors most important to the design of air conditioning and ventilation systems; such as temperature, humidity level, radiation level, thermal loads and pressure differences as well as leak tightness and insulation requirements. Based on the definition of room conditions, dimensioning criteria for different rooms with regard to air conditioning and ventilation shall be provided. **[**2019-06-15 **]**

5510. The rules and regulations issued by the Ministry of the Environment and the Ministry of the Interior concerning the design and operation of ventilation systems, and the related fire

protection design bases shall be met. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5511a. High-efficiency filters shall be placed in ventilation and air conditioning system ducts in connection with the activated-carbon filter in order to prevent the dispersion of coal dust from the filters. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

5513. When classifying rooms into zones, due consideration shall be given to:
1. the amounts and forms of radioactive substances potentially released from the plant systems and components in the event of leaks; and
2. the accessibility of the rooms during normal operation and accidents. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5520. The availability of supply air shall be ensured in circumstances in which it may be adversely affected by snow or ice. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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 leak tightness of the ducts. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

5524. Any combustible, toxic or otherwise hazardous gases and vapours released into the plant rooms shall be removed by the ventilation system. **[**2013-11-15 **]**

5525. If the exhaust air from plant rooms contains or may contain radioactive substances (in gaseous, particulate or droplet form) in amounts significant in terms of environmental radiation exposure, the exhaust air shall be sufficiently filtered or efficiently delayed. **[**2019-06-15 **]**

5526. The filtering and cooling of the air in the rooms shall be arranged with room-specific equipment if it is necessary to restrict the flow of exhaust air to reduce releases in the event of an accident. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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 license 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 license application; as a rule, the documents are to be submitted at the time of filing of the license application. If, exceptionally, some documents are submitted during the processing of the license 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 license. **[**2019-06-15 **]**

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

602. According to Section 24(2) 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, among others,

1) an outline of the technical principles of the planned nuclear facility;

2) a description of the safety principles that will be observed. **[**2019-06-15 **]**

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/events;
e. the preliminary plans to cope with an aircraft crash;
f. a summary of performed safety analyses for a standard or reference plant 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 license applicant's own assessment of how the plant satisfies the most essential Finnish safety requirements affecting design. **[**2019-06-15 **]**

603a. Guide YVL A.1 includes further requirements on the documentation required for the decision-in-principle. **[**2019-06-15 **]**

6.1.2 Preliminary Safety Analysis Report

604. According to Section 32 of the Nuclear Energy Decree (161/1988), the application for a construction license shall be accompanied by, among others,
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. […] **[**2019-06-15 **]**

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 license 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. […] **[**2019-06-15 **]**

606. The information enclosed with the application for a construction license 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. **[**2013-11-15 **]**

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 on the essential standard series used in system design and manufacture
3. A description of the nuclear power plant and its safety-classified systems; the general architecture of the systems
4. A description on the operating principles of the plant
5. A description of how the following factors have been taken into consideration in the general design of the plant and the design of safety-classified systems:

a. the implementation of the defence-in-depth principle and the independence of different levels of defence in the general design of the plant

b. the implementation of the redundancy principle, principle of physical and functional separation and diversity principle in all plant systems implementing safety functions that are required in different operational situations at the plant

c. the placement of systems and structures and components associated with them

d. protection from internal and external hazards/events

e. plans for protection against aircraft collisions

f. principles related to the management of human factors

g. a summary of the results of deterministic and probabilistic safety analyses, including the estimated environmental consequences of severe reactor accidents

6. The most important organisations related to the design of the plant and its system as well as a clarification on how they meet the requirements set for design organisations in chapter 3 of this Guide
7. A summarised description of the management systems of the key organisations participating in the implementation of the project
8. The license applicant’s own assessment of how the plant and participating organisations

meet the Finnish safety and quality requirements. **[**2019-06-15 **]**

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 license 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 requirement 609, and that the requirement specifications can be made for the purpose of procuring components and structures. **[**2019-06-15 **]**

609. At minimum, the following information shall be provided in the system descriptions of systems belonging to safety classes 1, 2 and 3, and in system descriptions drafted for buildings:
1. A description of the system, system functions and interfaces with other systems; at least the information presented in appendix A01 shall be provided
2. The 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 the various operational states of the plant
b. ambient conditions and the design criteria derived from them
c. internal and external hazards/events affecting the system
d. safety classification of the system and its structures and components
e. the failure criteria and 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 qualification of the system and its structures and components
g. requirements for maintenance, inspections and testing in various operational states of the plant
h. the requirements concerning 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 the plant's various operational conditions:
a. normal operational conditions
b. system fault conditions
c. anticipated operational occurrences and accidents
4. Methods used for the physical separation of the system and its equipment

(compartmentation, separation by distance, protection), and the preliminary positioning of the equipment 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 human factors have been taken into account in design
8. A preliminary safety assessment independent of the designer, drawn up by the license applicant
9. A list of equipment and its design requirements, presented in a meaningful fashion for the equipment type. **[**2019-06-15 **]**

610. The information listed in requirement 609, to the extent necessary, shall be provided on systems assigned to Class EYT/STUK. **[**2019-06-15 **]**

611. Other class EYT systems and buildings shall be described in system descriptions to the extent necessary for the assessment of the plant's overall operation. For systems, at the least tasks relevant for the plant's various operating conditions as well as a description of the functions and interfaces to other systems shall be provided. **[**2019-06-15 **]**

612. Analyses drawn up to justify design solutions shall be presented in the preliminary safety analysis report, such as deterministic analyses of postulated operational occurrences and accidents, failure tolerance and common cause failure analyses as well as analyses of internal and external threats. The main results of the structural analyses of the primary circuit and the containment shall also be presented in the preliminary safety analysis report. **[**2019-06-15 **]**

612a. The quality plans, qualification plans and requirement specifications of systems shall be submitted to STUK for information when submitting the system description of the corresponding system. **[**2019-06-15 **]**

613. Removed. **[**2019-06-15 **]**

614. Removed. **[**2019-06-15 **]**

6.1.3 Detailed design and changes during construction

614a. Change documentation related to changes to systems important to safety or detailed design after the granting of the construction license shall be submitted to STUK for approval, if the detailed design or change

- affects the nuclear power plant's functional architecture, i.e. it changes the design basis, operating principle, task or dependencies of the system(s)
- may affect the execution of the safety functions of the system(s).

The change documentation shall consist of descriptions of the purpose and main points of the modification as well as the system descriptions of modified systems. **[**2019-06-15 **]**

614b. Analyses drawn up to justify design solutions shall, when necessary, be submitted as part of the change documentation referred to in requirement 614a, such as deterministic analyses of anticipated operational occurrences and accidents, failure tolerance and common cause failure analyses as well as analyses of internal and external threats. **[**2019-06-15 **]**

614c. System descriptions of the safety analysis report shall be updated after the granting of the construction license so that sufficient understanding of the plant's configuration is maintained for the purpose of approving system modifications as well as components and structures. **[**2019-06-15 **]**

6.1.4 Final Safety Analysis Report

615. According to Section 34 of the Nuclear Energy Decree (161/1988), the application for an operating license shall be supplemented with, among others,
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. **[**2019-06-15 **]**

616. According to Section 36 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 an operation license is filed
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. […] **[**2019-06-15 **]**

617. The final safety analysis report shall describe a completed plant. In the operating license stage of the new plant, the final safety analysis report shall describe the plant as it is before nuclear fuel is loaded to the reactor. **[**2019-06-15 **]**

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/events;
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. **[**2019-06-15 **]**

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 analysis report or, alternatively, summarised in the safety assessment report and detailed in separate topical reports supplementing it. **[**2019-06-15 **]**

620. In addition to the requirements concerning the content of the preliminary safety analysis report specified in requirement 609 and Annex, at least the following information shall be

provided in the final safety analysis report on any systems or buildings assigned to Safety Classes 1, 2 or 3:

1. A detailed description of the implemented system;
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. **[**2019-06-15 **]**

621. The information listed in requirement 620, to the extent necessary, shall be provided on systems assigned to Class EYT/STUK. **[**2019-06-15 **]**

622. Other class EYT systems and buildings shall be described in system descriptions to the extent necessary for the assessment of the plant's overall operation. For systems, at the least tasks in the plant's various operating conditions as well as a description of the functions and interfaces to other systems shall be provided. **[**2019-06-15 **]**

623. Analyses drawn up to justify design solutions shall be presented in the final safety analysis report, such as deterministic analyses of anticipated operational occurrences and accidents, failure tolerance and common cause failure analyses as well as analyses of internal and external hazards/events. The main results of the structural analyses of the primary circuit and the containment shall also be presented in the final safety analysis report. **[**2019-06-15 **]**

624. Removed. **[**2019-06-15 **]**

625. Removed. **[**2019-06-15 **]**

6.2 System modifications

626. Removed. **[**2019-06-15 **]**

627. Regarding modifications made to safety-classified systems during the operation of a nuclear power plant, a conceptual plan shall be submitted to STUK for approval if the modification affects the functional architecture of the nuclear power plant, i.e. it changes the design basis, operating principle, task or dependencies of the system(s). A conceptual plan shall also be drawn up for a new system important to safety (EYT/STUK) and submitted for information. **[**2019-06-15 **]**

627a. The conceptual design plan shall include
1. a general description of the modification and systems to be modified
2. initial requirements for the design of system-level modifications with regard to performance, safety classification, defence-in-depth, redundancy, physical separation, functional isolation, diversity principle, layout, protection against internal and external threads and information security
3. description of the effects of the modification on the plant's operating principles and accident situations
4. a description of the deterministic and probabilistic analyses to be prepared or updated or other safety justifications considered necessary (such as tests)
5. a description of the modification schedule. **[**2019-06-15 **]**

628. During the operation of a nuclear power plant, pre-inspection documentation related to the modifications made to safety-classified systems shall be submitted to STUK for approval if a conceptual design plan has been prepared for the modification or if the modification may affect the execution of the safety functions of the system(s).
Information on equivalent changes to systems in class EYT/STUK shall be provided for information. **[**2019-06-15 **]**

628a. Concerning modifications other than those modifications of safety classified systems referred to in requirement 628, a description of the modification shall be submitted to STUK for information. The description shall include the purpose and main characteristics of the modification. **[**2019-06-15 **]**

628b. Where applicable to the modification, descriptions corresponding with the content of requirement 609 shall be presented in the system pre-inspection documentation. The pre-inspection documentation shall also include any separate justifications, such as deterministic

accident analyses, to demonstrate the safety of the modification. **[**2019-06-15 **]**

628c. The licensee shall submit the system requirement specifications related to the modification to STUK for information in connection with the system modification documentation. **[**2019-06-15 **]**

628d. The licensee shall submit system-specific quality and qualification plans to STUK for information in connection with the system modification documentation. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

630. Moved to para 627a. **[**2019-06-15 **]**

631. Requirements concerning the risk assessment, submitted as part of the conceptual plan and pre-inspection documentation in connection with system changes, have been provided in Guide YVL A.7. **[**2019-06-15 **]**

632. Moved to para 628b. **[**2019-06-15 **]**

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 alternative, 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 license applicant's request, give its preliminary opinion on issues concerning the application of safety principles or specific technical solutions. **[**2019-06-15 **]**

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 license 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. **[**2019-06-15 **]**

7.2 Processing of the preliminary safety analysis report in connection with the construction license application

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 license, 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 license 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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

706. Removed. **[**2019-06-15 **]**

707. When reviewing the PSAR and related design documentation submitted for the construction license, STUK verifies that the design of the plant and its systems can be used as a design basis for structures and components. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

709. Removed. **[**2019-06-15 **]**

710. Removed. **[**2019-06-15 **]**

7.3 Processing of the final safety analysis report in connection with the operating license application

711. Removed. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

713. Removed. **[**2019-06-15 **]**

714. Removed. **[**2019-06-15 **]**

7.4 System modifications at nuclear power plants during construction and operation

714a. STUK shall review the documentation referred to in requirements 614a and 614b before approving the component documentation related to the modifications. **[**2019-06-15 **]**

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 approving the related component documentation. **[**2019-06-15 **]**

8 Appendix Detailed requirements for system descriptions

A01. Description of the systems and buildings 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; 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.

2a. For HVAC systems: the main parts and components of the system; interfaces with other systems; process and instrumentation diagrams; auxiliary systems required for the operation of the system; monitoring and control of the system functions; operating parameters in different operational conditions (e.g. volumetric flow rates, cooling capacities, leak tightness requirements, filter efficiency and type); 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 software-based 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. **[**2019-06-15 **]**

9 References

1. Nuclear Energy Act (990/1987). **[**2013-11-15 **]**

2. Nuclear Energy Decree (161/1988). **[**2013-11-15 **]**

3. Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2018). **[**2019-06-15 **]**

4. Radiation and Nuclear Safety Authority Regulation on the Security in the Use of Nuclear Energy (STUK Y/3/2016). **[**2019-06-15 **]**

5. Radiation and Nuclear Safety Authority Regulation on the Emergency Arrangements of a Nuclear Power Plant (STUK Y/2/2018). **[**2019-06-15 **]**

6. Radiation and Nuclear Safety Authority Regulation on the Safety of Disposal of Nuclear Waste (STUK Y/4/2018). **[**2019-06-15 **]**

7. IAEA, Fundamental Safety Principles, Series No. SF-1, November 07, 2006. **[**2013-11-15 **]**

8. IAEA, The Management System for Facilities and Activities Safety Requirements, Series No. GS-R-3, July 21, 2006. **[**2013-11-15 **]**

9. IAEA, Safety Assessment for Facilities and Activities General Safety Requirements Part 4 Series, No. GSR Part 4, May 19, 2009. **[**2013-11-15 **]**

10. IAEA, Safety of Nuclear Power Plants: Design, Series No. SSR-2/1 (Rev.1), February 2016. **[**2019-06-15 **]**

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. **[**2013-11-15 **]**

12. IAEA, Design of Instrumentation and Control Systems for Nuclear Power Plants, SSG-39, 2016. **[**2019-06-15 **]**

13. Removed. **[**2019-06-15 **]**

14. Removed. **[**2019-06-15 **]**

15. Removed. **[**2019-06-15 **]**

16. IAEA, Ageing Management for Nuclear Power Plants Safety Guide, Series No. NS-G-2.12, February 06, 2009. **[**2013-11-15 **]**

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. **[**2013-11-15 **]**

18. IAEA, Design of Electric Power Systems for Nuclear Power Plants, SSG-34, 2016. **[**2019-06-15 **]**

19. IAEA, Modifications to Nuclear Power Plants Safety Guide, Series No. NS-G-2.3, October 23, 2001. **[**2013-11-15 **]**

20. Removed. **[**2019-06-15 **]**

21. WENRA Safety Reference Levels for Existing Reactors, 24th September 2014. **[**2019-06-15 **]**

22. WENRA, Safety of new NPP Designs, 2013. **[**2019-06-15 **]**

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. (STUK Y/1/2018)

Separation principle

Separation principle shall refer to physical separation and functional isolation. (STUK Y/1/2018)

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. (STUK Y/1/2018)

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. (STUK Y/1/2018)

Ventilation

Ventilation shall refer to maintaining and improving the quality of indoor air by circulating it; in some rooms of a nuclear facility, 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 is normally used as a synonym for “validation” in YVL-guides. Qualification shall refer to confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

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.

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. (STUK Y/1/2018)

Criticality accident

Criticality accident shall refer to an accident caused by an uncontrolled chain reaction of nuclear fissions. (STUK Y/1/2018)

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

Anticipated operational occurrence 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. (Nuclear Energy Decree 161/1988)

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 facility 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, 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, which can be assumed to occur less frequently than once during any one thousand operating years. (Nuclear Energy Decree 161/1988)

Design extension condition

Design extension condition 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;
b. an accident caused by a combination of failures identified as significant on the basis of a probabilistic risk assessment; or
c. an accident caused by a rare external event and which the facility is required to withstand without severe fuel failure.
(Nuclear Energy Decree 161/1988)

Power supply system

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.

Accident

Accident shall refer to postulated accidents, design extension conditions and severe accidents. (Nuclear Energy Decree 161/1988)

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 facility that may have an adverse effect on the safety or operation of the plant.

Protection I&C systems

Protection automation shall refer to I&C systems that control systems needed to manage postulated accidents and design extension conditions in order to reach a controlled state and maintain it. Protection I&C systems also include I&C systems that control systems needed for accident management during possible I&C common cause failures.

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, PRA

Probabilistic risk assessment (PRA) shall refer to quantitative assessments of hazards, probabilities of event sequences and adverse effects influencing the safety of a nuclear power plant. (Nuclear Energy Decree 161/1988)

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. (STUK Y/1/2018)

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. (STUK Y/1/2018)

System/structure/component important to safety

System/structure/component important to safety shall refer to systems, structures or components in safety classes 1, 2 and 3 and systems in class EYT/STUK.

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. (STUK Y/1/2018)

External events

External events shall refer to exceptional situations or incidents occurring in the vicinity of a nuclear facility 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. (STUK Y/1/2018)

Failure criterion (N+1)

(N+1) failure criterion shall mean the same as the single failure criterion.

Single failure criterion (N+1) 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 the most important safety functions necessary to bring the plant to a controlled state and to maintain it must be ensured in postulated accidents even if any individual component of a system providing the safety function is inoperable and even if any other component of a system providing the same safety function or of a supporting system necessary for its operation is simultaneously inoperable due to the necessity for its repair, maintenance or testing.

Annual dose

Annual dose shall refer to the sum of the effective dose arising from external radiation within the period of one year, and of the committed effective dose from the intake of radioactive substances within the same period of time. (Nuclear Energy Decree 161/1988)

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.

Single failure criterion

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