Guide YVL B.1, Safety design of nuclear power plants

1 Introduction

Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2018) sets higher-level requirements on the safety design of a nuclear power plant. These requirements are specified in this Guide.

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 (earlier title “Management systems for nuclear facilities”)
- 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 Safety classification of systems, structures and components in nuclear facilities

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 in a nuclear facility
- YVL B.3 Deterministic safety analyses for a nuclear power plant
- YVL B.4 Nuclear fuel and the reactor
- YVL B.5 Primary 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 supply of a nuclear facility
- YVL E.11 Lifting and transfer equipment of a nuclear facility
- YVL E.13 Ventilation and air-conditioning equipment of a nuclear facility

The structural radiation safety of a nuclear facility and radiation safety of workers and the environment, as well as the requirements pertaining to radiation measuring instruments, are addressed in 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

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.*

A fundamental principle of the safety design of nuclear facilities with regard to preventing operational occurrences and accidents and mitigating their consequences is defence-in-depth, or the defence-in-depth safety principle. According to Section 7 b of the Nuclear Energy Act, *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.*

According to this principle, the design of a nuclear power plant shall, in order to prevent reactor damage and harmful radiation effects, be implemented by means of consecutive, redundant structures and systems. Requirements set forth in IAEA and WENRA instructions are based on the same principle. Levels of the defence-in-depth principle are laid down in STUK regulation STUK Y/1/2018, and the related requirements are specified particularly in chapter 4 of Guide YVL B.1.

The reliability of safety functions is associated with the quality of the systems performing the functions. The quality of systems, structures and components is affected by the operation of design organisations, including the licence applicant or holder, and the design process as well as the manufacture, testing and installation of components. Requirements related to these matters are presented in chapter 3 of this Guide.

In order to ensure the reliability of systems performing safety functions, threats to these systems shall be taken into consideration in the design; threats shall be managed by applying the redundancy, diversity and separation principles to design work. Requirements related to these principles are presented in chapter 4 of this Guide.

Chapter 5 lays down the requirements for the design of specific nuclear power plant systems.

Chapter 6 presents requirements related to the documents to be submitted to STUK, and chapter 7 presents requirements related to the regulatory oversight of safety design.

This memorandum presents justifications for changed requirements. In addition to the changes presented, minor further specifications and linguistic corrections have been made to some requirements.

2 Scope of application

Guide YVL B.1 presents requirements applicable to the safety design of a nuclear power plant as well as the design of systems belonging to safety classes 1–3 and EYT/STUK, and changes made to these systems. This Guide may also be applied to other nuclear facilities.

3 Justifications of the requirements

3.1 Chapter 3 Design management

Higher-level requirements for the design of nuclear power plants are provided in the Nuclear Energy Act (990/1987), whose Section 7 f sets forth:

Safety shall take priority during the construction and operation of a nuclear facility.

The holder of a construction licence, as referred to in Chapter 5 herein, shall be responsible for the nuclear facility's construction in accordance with safety requirements.

The holder of an operating licence, as referred to in Chapter 5 herein, shall be responsible for the nuclear facility's operation in accordance with safety requirements.

Furthermore, Section 9 of the Nuclear Energy Act sets forth:

The license holder shall be under an obligation to ensure the safe use of nuclear energy. This obligation may not be delegated to another party. The license holder shall ensure that the products and services of contractors and subcontractors which affect the nuclear safety of the nuclear facility meet the requirements of this Act.

Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2018) provides that:

- *The holder of the nuclear facility's construction licence shall ensure during construction that the nuclear facility is constructed and implemented in conformity with the safety requirements and using approved plans and procedures.* (Section 18(1))
- *The holder of the nuclear facility's operating licence shall ensure that the modifications to the nuclear facility are designed and implemented in conformity with the safety requirements and using approved plans and procedures.* (Section 20(5))

These requirements with regard to the licence holder and the organisations participating in the design are specified in chapter 3. The requirement level for management systems of organisations participating in the design and implementation of systems important to a nuclear power plant and its safety shall be set according to the product's safety class in accordance with requirements 629 and 629a of Guide YVL A.3. Requirements for design organisations and their processes and practices, in particular, are specified in chapter 3.

Generally, the word "nuclear power plant" has been corrected to "nuclear facility" in chapter 3 because the requirements for design management apply to them as well.

3.1.1 Chapter 3.1 Organisations responsible for design

This chapter presents requirements for the licence holder and design organisation. Requirement 309 concerning the fulfilment of requirements throughout the design

chain has been removed from the chapter because it is included in other requirements of chapter 3.

3.1.2 Chapter 3.2 Design processes

This chapter presents general requirements related to design processes, which are preconditions for demonstrating the implementation of the safety requirements.

Requirement 318, concerning reviews, has been removed and its content has been reassigned to other requirements. Requirement 314a includes a requirement on the cross-technicality of reviews, whereas the competence requirement can be considered fulfilled by means of, e.g., the requirements of the previous chapter.

Requirement 314b is new and provides that safety experts participate in verification and review processes. Depending on the stage of the facility's life cycle, the design organisation referred to in the requirement could be the licence holder itself or the plant supplier, for example.

Requirement 315 has been clarified because the completion of a phase does not have unambiguous significance. The most essential thing is to assess the impact of the matters remaining open and the conditions for starting the next design task in this regard.

3.1.3 Chapter 3.3. Configuration management

Configuration management is a process for managing the uniformity of the plant, systems, components and structures (or, more generally, products) as well as the uniformity of their documentation throughout the life cycle. Configuration management functions include identification of configuration (determining configuration units and recognising basic levels), change management (including change management of the product and operating processes), management of status information, audits and reviews of configuration management as well as interface management.

The products, meaning the plant, systems, components and structures, shall be divided into sufficiently small units (configuration unit) to enable their management. Each unit shall be identifiable. The KKS system is a common identification method, but others are used as well. Many kinds of documentation is associated with the configuration unit. Systems and components have requirement specifications, and a mechanical component, for example, involves construction plans, process systems involve flow diagrams and I&C equipment involves technical implementation documents and user instructions. Safety-classified configuration units are also associated with documentation submitted to the authorities as well as information related to authority approvals. During planning and development, it is important to be able to distinguish between an approved version of the product and any working copies.

Functional processes shall also be included in configuration management because any changes in the processes may affect the end result. For example, changing the method description, or functional process, related to analyses may change their results.

In a specific stage of the project or at a specific point in time, a basic level can be determined for the current configuration. According to standards, the basic level is the development stage where the configuration unit is proven to fulfil the set requirements. However, in practice, the basic level may just as likely contain the system and its documentation before starting factory tests, in which case conformity with requirements cannot yet be demonstrated as a whole. A typical project has more than one basic level, such as one basic level after the design has been completed and the as-built basic level after installation. Changes made across basic levels shall be traceable.

Change management is an important part of configuration management. It is essential to determine how to ensure that, after implementing the change, the modified product meets the set requirements.

A set of instructions describing practical measures and, if necessary, supplementary plans shall be prepared for configuration management. When preparing instructions and plans, the specifics of each field of technology shall be taken into account. Particular attention shall be paid to instructions and plans which steer changes impacting several fields of technology.

The chapter has been amended with mostly terminological changes. Furthermore, two requirements concerning configuration management have been moved to the chapter from another part of the Guide.

3.1.4 Chapter 3.4 Quality plans

Chapter 3.4 presents requirements for system-specific quality plans. Therefore, a system-specific quality plan shall be prepared and implemented for the purpose of design and implementation of systems and their changes. Requirement 331 has been modified so that it provides a point in time for preparing the quality plan and excludes the need for a quality plan in case of minor changes. The quality plan compiles topics derived from requirements concerning the organisation in charge of the design and design process; the topics are presented in requirement 332.

Requirements for quality plans have, as a rule, been prepared for construction projects of new plants. In case of operating nuclear power plants, changes ranging from very extensive to minor can be planned during the plant's service life. The number of organisations participating in the design is smaller as well, and the design may be carried out by, for example, the operating licence holder using the design organisation's quality handbook. Therefore, the quality plan may be a clarification on compliance with processes and guides and included in an applicable document.

Control rooms and I&C architecture shall be processed as systems, so quality plans are required for them as well.

Requirements for submitting quality plans are set forth in chapter 6.

Requirement 342 has been moved to this chapter and changed into requirement 334a, which addresses the assessment of quality plan implementation. At the same time, the requirement specifies that *the purposeful implementation of planning processes* refers to assessing the implementation of quality plans. Similarly, another

requirement (previously 343) was moved and became a little more specific requirement 334b concerning experts who perform assessments.

3.1.5 Chapter 3.5 Requirement specifications

Chapter 3.5 presents requirements for system requirement specifications. The definition of system requirements provides that, in practice, plant-level requirements are identified and recorded first. Some of the component-related requirements are caused by system-level design. Requirements for each stage of design shall be identified prior to beginning the design work, and the requirements shall be traceable in different stages of design. Requirements for submitting requirement specifications are presented in chapter 6 of this Guide. The component requirement specifications and related generic requirement specifications are addressed in YVL Guides of the E-series.

In the justifications for the suitability of standards in the chapter's requirement 338, *the adequacy of standards and instructions* has been replaced with justifications for the suitability of standards, because "adequacy" is an unclear concept in this context. The justifications can be added to the requirement specification or another applicable document.

Requirement 340 specifies the degree of independence. The requirement for a separate assessment report has been removed from the section. The results of the assessment can be recorded in any manner that is traceable and considered suitable for their processes by the designer.

Chapter 3.6 "Safety assessment within the design organisation" has been removed compared to guide published 2013 because the requirements have been specified and moved to suitable sections in other chapters.

3.1.6 Chapter 3.6 Substantiation of the design solutions

Chapter 3.6 presents requirements for the substantiation of design solutions. Furthermore, the chapter presents a requirement for safety assessment performed by an independent expert organisation in situations defined by requirement 348a.

The design solutions shall be justified by means of deterministic safety analyses (the requirements are provided in Guide YVL B.3) and probabilistic risk analyses (the requirements are provided in Guide YVL A.7) as well as failure tolerance analyses and common cause failure analyses, the requirements for which are provided in this chapter.

In failure tolerance analysis, the purpose of analysing functional failure dependencies is to clarify how the system operation changes when one failure at a time is postulated for it. In this case, only planned dependencies, meaning the system and its support systems, shall be observed. A support system is considered a single component. If support system failures are proven to affect system operation, a failure tolerance analysis shall be conducted for the support system as well. Its classification criteria shall include the modes of failure which were identified in the failure tolerance analysis of the main system (for example, no electricity, no flow, overvoltage, etc.). This way, a set of connectable analyses can be compiled, where the fault modes of

the support systems can be linked to the main systems. In connection with this analysis, the status of the system during maintenance of its components shall be presented as well (e.g., inoperable or brought into the safe state).

In terms of drawing conclusions related to failure tolerance analyses and common cause failure analyses, the impact of initiating events on safety functions shall also be taken into consideration. As a result of initiating events, components may be damaged on account of, e.g., the impact of a pipe break or jet force; the pump feed can be lost in the leak; or the environmental conditions may be harmful with regard to the component's functionality. Failure criteria shall be applied in addition to the consequences of the initiating event, meaning that these consequences shall be taken into account in a traceable manner in conclusions drawn from failure tolerance and common cause failure analyses.

In practice, drawing conclusions from the fulfilment of the failure criterion in different accident situations also requires "success criteria", meaning that deterministic accident analyses are connected to failure tolerance and common cause failure analyses.

A common cause failure analysis shall be prepared for operational occurrences and class 1 postulated accidents. In the common cause failure analysis, the common cause failure is postulated for components that have a mutual characteristic, meaning the components are of a similar nature or contain significantly similar parts. If necessary, the amount of detail in the review may vary according to the equipment type.

For the purpose of common cause failure analysis, the implementation of safety functions shall be identified according to the initiating event, and the impact of the common cause failure with regard to performing the function shall be reviewed. Compliance with the diversity principle is required from functions in safety class 2 that are needed in postulated accidents, so the comparison in operational occurrence analysis shall also be related to them. Transients and accidents can be combined in the analysis when the functions needed in these situations are the same and the impact mechanisms of initiating events are similar. In the common cause failure analysis, one safety function shall be examined at a time, taking into account the systems and their support systems that implement the function. Common cause failures of any such equipment whose common cause failures may affect the implementation of the safety function shall be examined in the analysis.

The requirement for a safety assessment conducted by an independent expert organisation has been moved from the Guide published in 2013 to new chapter 3.6. The requirement has also been changed to clarify the requirements of the organisation performing the assessment, and the "considerable safety significance" described earlier has been replaced with a more specific definition. Furthermore, the requirement is more clearly targeted at the licence holder.

In relation to failure analysis, requirement 351 has been modified so that it entails the performance of failure analysis. The demonstration requirement concerning the impact of a common cause failure, presented earlier in the document, has been moved to chapter 4 and is now a more direct design requirement. Requirement 353

clarifies both the terminology and manner of application with regard to following the diversity principle. Requirement 354 has been removed because parts of it are considered to be included in failure analyses (such as maintenance errors through failure modes) and other demonstrations.

3.1.7 Chapter 3.7 Documentation

Requirements for nuclear power plant documentation are presented in chapter 3.7. In order to enable the safe construction, operation and modifications of the plant during operation, the documentation shall be comprehensive and clear. No significant changes have been made to the chapter.

3.1.8 Chapter 3.8 Validation

Chapter 3.8 presents the content required from a qualification plan. To steer the validation process, a qualification plan shall be prepared for the systems, the purpose of which is to ensure that the measures used to demonstrate the suitability of the systems for their purpose are comprehensive and completed in a timely manner. Reviewing whether systems important to safety are suitable for their purpose requires reviewing whether the safety requirements are met before and after installation. This means that the validation covers design, manufacture and deployment.

Terms in the chapter have been changed to correspond with the standard-compliant definition “validation”. However, the “qualification plan” has been left as is because the other guides refer to the requirements using this term.

3.2 Chapter 4 Design requirements for ensuring the reliability of safety functions

3.3 4.1 General design principles and requirements

Chapter 4.1 presents general design principles and requirements for safety-classified systems.

Requirement 407, concerning preparation for technological breakthroughs, has been removed from the chapter. Requirement management ensures the traceability and feasibility of changes during the life cycle of a nuclear facility. Guide YVL A.8 addresses ageing management which also takes into account technological ageing.

Requirement 412, concerning cross-connections between systems implementing the same safety function, has also been removed from the chapter due to its unclarity. Requirement 411, concerning nuclear facilities located in the same plant site and sharing common systems, has been specified in a manner that takes into account simultaneous accidents at the facilities.

A general requirement concerning preparation for disturbances and accidents at several plant units has been added as requirement 414a. Requirements pertaining to certain details have been presented in relation to the topic but, for the sake of clarity, it is also necessary to present a goal that is generic in nature.

3.3.1 4.2 Design bases of systems performing safety functions

According to Section 7 d of the Nuclear Energy Act, *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.*

The design of a nuclear power plant shall take into account events which may cause the plant's parameters to deviate from their normal values. Such events may be caused, for example, by a rupture in pressure equipment or piping; a component failure; an error in automatic control; or an internal/external threat. The events require that particular functions, or limitation and safety systems, are designed to ensure that no damage occurs to people, the environment or property on their account. These initiating events shall be classified according to the probability of their occurrence. The events may also endanger the operation of the limitation and safety systems. Requirements concerning protection are addressed in Guides YVL B.7, YVL B.8, YVL A.11 and YVL A.12.

A section concerning compromised safety functions has been removed from requirement 414. The requirement now concerns only the definition of initiating events. Requirements 415 and 416 have been removed. Requirements concerning protection from external and internal events have been addressed in other Guides and have therefore been removed from this chapter.

3.3.2 4.3 Application of the defence-in-depth principle in design

According to section 7 b of the Nuclear Energy Act, *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.*

The aforementioned requirements of Section 7 b of the Nuclear Energy Act are specified in Section 9 of the Radiation and Nuclear Safety Authority 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 power plant.*

Requirements for the safety design of nuclear power plants are based on the defence-in-depth principle whose different levels have primarily been determined by STUK regulation STUK Y/1/2018. Because of this, requirement 421 has been changed into a citation of the regulation. The design extensions have already been defined in the Nuclear Energy Decree (161/1988), but the related requirements have not been given in much detail. Levels 3a and 3b have, therefore, been defined in more detail in this Guide (new requirement 421a).

On level 3, provisions are made for postulated accidents with systems that are activated automatically when an accident occurs. Systems designed for such postulated accidents or safety systems include, for example, an emergency core cooling system and primary and/or secondary circuit safety valves as well as the containment isolation system. The systems are needed to mitigate the consequences

of accidents and to prevent an accident from escalating into a severe accident. Measures performed by the operator and the related systems and equipment are also belong to level 3. At level 3, provisions are also made for the failure of systems designed for these postulated accidents. At level 3b, the objective is to control design extension conditions (DEC), meaning:

A. anticipated operational occurrences and Class 1 postulated accidents that involve a common cause failure in the system designed for coping with the event concerned
B. combinations of failures selected on the basis of a probabilistic risk assessment
C. rare events that are unlikely to occur but are nevertheless considered possible, such as extreme weather phenomena or the collision of large aircraft.

Level 3b includes systems in safety class 3 that implement the diversity principle and ensure the operation of systems in safety class 2 during anticipated operational occurrences and class 1 accidents in case of any common cause failures occurring. In such situations, the plant shall be brought into a controlled state by means of systems in safety class 3 that implement the diversity principle. After this, in order to bring the plant into a safe state, the same systems in safety class 3 can be used as at the level 3a. In DEC B and C events, the same requirement level shall be applied to controlled state as is given for transitioning into a safe state.

The defence-in-depth principle is associated with “practically eliminating” (preventing with planning actions) events that lead to an early or large release (requirements 423, 423a and 424). The aim of the requirements is to ensure that the course of a severe accident can be controlled by means of systems designed for severe accidents. The purpose would be to practically eliminate any events (e.g. energetic phenomena) which could lead to a loss of the containment’s integrity or tightness or to a severe accident in the fuel storage. The loss of the containment’s integrity or tightness, occurring at an early stage of the accident, would lead to an early release, which would make it impossible to protect the public through emergency preparedness activities (level 5). A caesium-137 release exceeding 100 TBq is considered a major release in accordance with Section 22 b(5) of the Nuclear Energy Decree.

The events to be practically eliminated shall be identified and analysed using methods that are based on deterministic analyses supplemented by probabilistic risk analyses and expert evaluations. Practical elimination cannot be based solely on compliance with a cut-off probabilistic value. Although the probability of an event would, based on the analyses, prove to be very small, all measures which are practically possible shall be taken to reduce the risk. Events to be practically eliminated are, for example:

a. a rapid, uncontrolled increase of reactivity leading to a criticality accident or severe reactor accident
b. loss of coolant during shutdown leading to reactor core uncovery when the containment is not leak tight
c. a load jeopardising the integrity of the containment during a severe reactor accident (e.g. reactor pressure vessel breakdown at high pressure, hydrogen explosion, steam explosion, direct impact of molten reactor core on containment bottom or wall, uncontrolled containment pressure increase)

d. a loss of cooling in the fuel storage resulting in severe damage to spent fuel.

In chapter 4.3, requirement 421 concerning the defence-in-depth principle has been changed into a description because the requirement as such is included in Regulation STUK Y/1/2018. However, the chapter now includes a general requirement concerning the considering of a common cause failure any system performing a safety function or in its support system as a design extension condition DEC A. The intention was to clarify that the requirement for following the diversity principle applies to the entire system aggregate needed to perform the function, similarly to the failure criterion (442). Similarly, requirement 421d has been added to address DEC B situations. Various failure combinations at the plant, particularly those highlighted during PRA, are to be considered as DEC B events. Typically, it has been required to consider various combinations of failures that could significantly affect matters such as releases when combined with the initiating event. Examples of such events include a stuck-open steam generator safety valve during a steam generator pipe leak, the rupture of several pipes or, for example, events referred separately in Guides YVL B.5, B.6 and B.8.

Example cases presented in requirement 424 concerning practical elimination have been moved from the requirement to the explanatory memorandum. Requirement 423a, concerning limiting a major release in accordance with the Nuclear Energy Decree, has been added to the chapter. In practice, the requirement is not new because it has been included in the examples of requirement 424.

4.3.1 Independence of the defence-in-depth levels

According to Section 9 of 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.*

The independence of the levels of defence shall refer to systems operating at different levels of defence that have been functionally and physically isolated from each other to ensure that they cannot fail in consequence of the same event or cause during an accident. In addition to the functional and physical separation, compliance with the diversity principle can be considered as part of the independence. Its purpose is to prevent failures for the same reason. An acceptable level of independence may vary across various lines of defence and fields of technology.

In practice, normal operating systems and limitation systems, or defence levels 1 and 2, are not separated comprehensively. It may not necessarily even be possible or necessary to separate them comprehensively. Limitation functions can be implemented in the plant’s functional architecture by applying them in different ways when other requirements related to, e.g., safety class and failure criterion are fulfilled. At defence level 3, systems can be used when another system at level 3 fails if it can be proven that both of them shall not fail during the event. The levels of defence 3a and 3b are, therefore, not necessarily completely isolated across the plant; the independence of measures needed for different situations shall be demonstrated on a case-by-case basis. In this regard, different fields of technology have differences; for example, the independence of process system functions can typically be more easily demonstrated, whereas backup I&C systems shall be implemented as separate lines

of defence. Management of severe reactor accidents shall be separated more clearly from other levels of defence, and the starting point shall be the assumption that the chain leading to a severe reactor accident cannot necessarily be defined.

Functional isolation shall refer to the separation of inter-connected systems from one another to prevent the impact of a system's operation or failure on another system. Functional separation shall also include electrical separation and separation related to the communication of information. Functional separation helps make provisions for failures that are caused by transients caused by external or internal factors and could proceed from one system to the next or across the interfaces of subsystems.

Prevention of fault propagation is an integral part of system and equipment separation and is related to the interfaces of systems or system parts in different safety classes. Interfaces of systems in different safety classes shall be designed in a manner that ensures that a connection between them shall not compromise the operation of systems performing a safety function. In particular, the failure of a system, structure or component in a lower safety class shall not cause the failure of a system, structure or component in a higher safety class.

Electrical separation shall refer to, i.a. galvanic separation.

Physical separation shall refer to separating items from each other with sufficient barriers, distance or placement or combinations thereof with the aim of preventing damage to the separated items on account of the same external or internal event. Physical separation is realised through structures and/or placing the items sufficiently far apart in order to prevent the consequences from spreading. The structure may be a separate building or room, or a wall or similar structure in a certain area.

The need for physical, electrical and functional separation depends on the relevant internal or external threat and shall be assessed with comprehensive analyses. The separation shall also take into account the consequences of failures. The aim is to achieve sufficient independence between the various subsystems of safety systems as well as systems at different levels of the defence-in-depth principle.

Requirement 427 has been removed from the chapter because it is included in other requirements. Requirement 430 has also been removed from the chapter because sufficient independence is also required from levels of defence by Regulation STUK Y/1/2018. Independence shall also entail the necessary physical separation in a situation where, for example, an initiating event or a single failure occurring during or in consequence of the event could result in the loss of systems/equipment needed to implement functions on another level of defence. In addition to this, requirement 430 may lead to an excessively strict interpretation of physical separation (in other words, different lines of defence should be strictly separated in different safety blocks, in addition to which other requirements based on fire protection should be complied with). The level of defence categorically separated from the others is the management of severe reactor accidents in accordance with requirement 431. Requirement 431 takes into consideration the change in Regulation STUK Y/1/2018, and the requirement has been limited to apply to a controlled state in a severe reactor accident.

4.3.2 Strength of individual defence-in-depth levels

This chapter presents requirements for the strength of individual defence-in-depth levels of the defence-in-depth safety principle. This shall refer to the manner of making provisions for failures of systems performing safety functions by means of the principle of redundancy by dividing them into two or more redundant systems or subsystems in order to implement the safety function in question, even if any of these were inoperable.

Furthermore, there is a requirement that, in order to decrease the frequency of initiating events, 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.

The chapter also presents general requirements for the separation of systems and subsystems. A key factor in the strength of the defence-in-depth levels is the functional and physical separation of various subsystems from each other. The purpose is to ensure that the failure of one subsystem shall not compromise the operation of other subsystems or that the plant's internal events shall not spread from one safety block to the other, harming more than one subsystem. Separation into safety blocks also helps in some external events.

In some cases, however, there are valid reasons for connecting various subsystems of the same system to each other or connecting various subsystems of functional chains. Typical examples include isolation functions in which, in order to increase the reliability of isolation, the control and operational force of two consecutive isolation valves located in the same process subsystem shall be implemented through subsystems of different I&C and electrical systems. Such situations may also include voting implemented in I&C systems. In these exceptional situations, safety benefits shall be assessed and the prevention of fault propagation, in particular, shall be ensured. Requirement 439 has been specified.

More detailed regulations concerning the physical separation of systems and components are provided in Guides YVL B.7 and YVL B.8.

Requirements 436 and 441 have been removed from the chapter because they have been covered by other requirements. A new requirement 442a has been added to the chapter, addressing the identification of the consequences of initiating events and taking them into account in the design of systems performing safety functions. The requirement was previously included in YVL Guides but, in connection with structural changes, was removed for all events except for postulated accidents. Requirement 435 has been specified.

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

This chapter presents the failure tolerance and self-sustainment requirements for systems performing safety functions that are needed to bring the plant into a controlled state during operational occurrences, postulated accidents or design extension conditions in a manner that the corresponding acceptance criteria for fuel integrity are not exceeded.

Requirements concerning operational occurrences, postulated accidents and design extension conditions have been distinguished from each other more clearly.

In case of operational occurrences referred to by requirement 432, the objective is to ensure that there is no need to start systems designed for managing of postulated accidents in consequence of a single failure. This situation has also been recognised by requirements 445 and 448. On the other hand, events where the system causing the initiating event fails more extensively that intended in requirement 432 shall also be considered as operational occurrences. To manage such an operational occurrence, it is also possible to use systems designed for managing postulated accidents for shutting down the reactor, controlling reactivity and removing residual heat. In both cases, the limit values set for fuel integrity, radiological effects and primary circuit pressure shall be fulfilled for operational occurrences. More specific requirements for failure postulations regarding different types of operational occurrences have been set out in Guide YVL B.3.

The requirement concerning reactor shutdown when the control rod-based system fails has been relaxed so that it corresponds with the international requirement level.

Requirements for DEC B and C situations are presented as separate requirements because the situations are different in nature.

External events and conditions are required to be considered as DEC C situations. All external conditions or events do not necessarily cause an initiating event at the plant. The definition of events is addressed in more detail in Guide YVL B.7.

Requirement 451 has been simplified to apply to the definition of an initiating event and the related acceptance criterion. The requirement can be taken into account in the design of a new nuclear power plant by complying with the general design requirements presented in chapter 4, meaning that electric power distribution systems are designed in accordance with the diversity principle and the residual risk related to the propagation of the initiating event is controlled by separating severe accident management systems from other plant systems in order to prevent the propagation of the transient. In this case, this is considered a common cause failure in the design of electrical systems, and the failure criterion of a system or part of a system compliant with the diversity principle shall be N+1 according to the general principle. Because common cause failures of electric power distribution systems may be difficult to identify, it is essential to separate severe reactor accident control systems from the rest of the electric power distribution by preventing the propagation of the electrical transient.

Feeding through a motor generator is considered an acceptable way to separate control systems for severe reactor accidents. A sufficient level of separation can also be ensured by dimensioning components of severe reactor accident control systems to withstand double overvoltage compared to what a transient coming from the plant’s main generator could, in an extreme case, be expected to be.

If these principles cannot be followed comprehensively, they can be supplemented with methods such as the following:

- electrical isolation of safety functions as well as the plant status control and supervision functions from the plant's electrical grid
- safety functions independent of the electrical supply and distribution to manage the situation, and electrically isolated plant status control and supervision functions.

It is no longer practically possible to perform extensive modifications to the architecture of electrical power distribution at an operating nuclear power plant. Therefore, examples such as the aforementioned can be used to fulfil the requirement.

Requirements for fuel storages have been moved to Guide YVL D.3.

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

Systems which implement safety functions and are needed to reach a safe state as well as to keep the reactor subcritical and cool it down shall, as a rule, fulfil the single failure criterion (N+1). In DEC B and C events, the same requirement level shall be applied to controlled state as is given for transitioning into a safe state. If it is not possible to reach the safe state right away or within the time period required to fulfil the self-sufficiency criterion, it shall be possible to maintain the plant in a controlled state for as long as is needed to ensure the operability of the equipment needed to restore the safe state.

The order of the functions has been changed in requirement 454. The requirement was previously written in a way that takes into account the special characteristics of reactor types; in other words, besides the system based on solid absorbers, the pressurised water reactor also needs a system using boron diluted in the coolant, whereas solid absorbers can be used in the boiling water reactor to keep the reactor subcritical at all temperatures. However, in boiling water reactors, also the system based on an absorber diluted in the coolant must be able to bring the reactor into a cold state to ensure that this is successful also in case the solid absorbers fail (ATWS).

Furthermore, the requirement concerning the reparation of systems required to achieve a safe state as well as the requirement concerning design extension conditions DEC B and DEC C have been clearly separated as individual requirements. Because of this, requirement 455 has been divided into three parts. Requirement 455c, concerning the possibility to remove fuel from the reactor after operational occurrences, postulated accidents or design extension conditions, has been moved from Guide YVL B.3 because it is not a requirement applicable to analyses.

Chapter 4.3.5 Other redundancy requirements

In order to ensure adequate functional reliability, the safety-relevant systems presented in the Guide shall fulfil the (N+1) failure criterion.

Requirement 456 has been divided into parts, and requirements already laid down in other Guides have been removed. Requirement 456c, concerning functions needed

to prevent the dispersion of radioactivity, has been specified so that it applies to functions instead of systems. Requirement 456e concerning I&C functions and other support functions needed to isolate the containment has also been specified so that the failure criterion is provided in accordance with the event classification.

3.3.3 4.4 Taking into account human factors

Requirement concerning the HFE programme has been moved to this chapter from chapter 5.3 that addresses the control room, and any overlapping requirements have been removed. Some parts of the requirement for the HFE programme have been specified. Requirements concerning the new plant and modifications to the operating plant have been presented separately.

3.4 Chapter 5 Design of specific nuclear power plant systems

3.4.1 Chapter 5.1 Reactor cooling and decay heat removal systems

The requirement concerning the removal of decay heat into the ultimate heat sink has been changed in the update of the Guide. The diversity principle shall be followed in accordance with chapter 4 in designing systems participating in decay heat removal. In addition, preparations shall also be made for the interruption of the use of the ultimate heat sink. Heat transfer to a secondary ultimate heat sink can be implemented in accordance with the DEC C rules if the diversity principle has been followed in transferring heat to a primary heat sink. On the other hand, it also possible to design the use of the secondary heat sink as a function that entirely complies with the diversity principle, meaning that it meets the DEC A requirements. When assessing the effects of the loss of the ultimate heat sink, one shall take into account that some of the safety functions may be seawater-cooled.

Requirement 5106 has been changed so that procedures and indirect methods related to leak monitoring are taken into account. A reference to the LBB requirements has been added to the requirement; there are separate criteria for systems related to these requirements.

Requirement 5111a has been added to the chapter based on requirement 5111. Requirement 5111 applies to the operation of emergency cooling systems in a situation where insulation impurities and other materials are released into the containment as a result of a pipe break. The nuclear power plant may have other systems which, similarly, recycle water within the containment; this has been taken into account in requirement 5111a.

3.4.2 Section 5.2 I&C systems

Requirements concerning instrumentation and automation/control systems have been presented in chapter 5.2. Due to the complexity of the requirement, background information on requirement 5240 has been provided in the explanatory memorandum to clarify the requirement.

Requirement 5240 with its subsections

The requirements are design requirements, meaning that provisions shall be made for I&C failures when designing I&C systems for the plant. The extent of the impacts of failures shall be limited with design solutions. The simplest way to accomplish this is by identifying the functions whose simultaneous active and/or passive failure could compromise the safety of the nuclear power plant and by separating such a functionality in a manner that would make a simultaneous failure highly unlikely.

The extent of the failure shall be justified in the analysis performed on the basis of the requirements. Assumptions regarding the extent of the failure shall be based on verifiable design solutions. For example, the typical extent of the failure could be limited to one system, particularly when the system has a limited number of interfaces to other systems. When the analysis is limited to system level, possible failures of interfacing systems or system parts containing similar technology (platform/application system software) shall be assessed.

Failure refers to the simultaneous failure of a functionality of a part of I&C architecture, reviewed under requirement 5240, so that the most harmful failure mode given the situation shall be inspected. Failure can, therefore, be passive (a function does not start), active (unexpected operation) or a combination of these failure modes. With regard to the most critical or complex functions, the partial implementation of these functions shall also be assessed. An example of this is the halting of a diesel sequence or the freezing of a signal. The conservative failure type may vary depending on the initiating event combined with the postulated failure.

Some of the restrictions of the consequences of failures are included in other requirements. Requirement 5240 specifies the requirements concerning consequences of failures in so far as these are not presented elsewhere. According to requirement 432, the failure of an individual operating component shall not lead to a postulated accident. Provisions shall be made for the common cause failure of the protection system with functions that meet the DEC criteria in accordance with requirements 421b and 5228a. According to requirement 440, a functionality in a lower safety class shall not prevent the implementation of functions in a higher safety class, and a separate requirement 5231 has been given for the functions of protection I&C systems. Furthermore, the management of severe accidents (including the operation of the dedicated I&C systems) shall be independent of the other functionalities of the plant or the impacts of failure in accordance with requirement 431.

The failure of EYT I&C systems shall not cause an initiating event that is worse than an operational transient. Furthermore, according to requirement 440, the failure of EYT I&C systems shall not prevent the implementation of functions in a higher safety class; in this requirement, this is laid down in Section 2.

In safety class 3, the acceptance criterion presented for initiating events caused by I&C system failures is a postulated accident in class 1. The objective is, in part, to limit the implementation of functionality in I&C systems belonging to safety class 3 in a manner that ensures that the extent of the impacts of its failure would not reach a postulated accident in class 2. For example, the control of pressuriser safety valves

or similar pressure reduction lines shall be reliable in a manner that makes it impossible to cause a situation similar to a large pipe break. Furthermore, one shall take into account that I&C systems in safety class 3 shall not prevent the operation of the protection system in accordance with requirements 5231 and 440 and based on the independence targets of the lines of defence.

A criterion is presented for the failure of operational and limitation I&C systems. In I&C architecture, the operational I&C system can also be separated from the limitation I&C system. In this case, depending on the isolation solutions, the operational I&C system and the limitation I&C system may be considered as entities failing separately.

If I&C systems in safety class 3 fail during operational occurrences, it can be assumed that it may not be possible to comply with the criteria for operational occurrences because the purpose of limitation I&C systems is, in these cases, to prevent the aggravation of the event. A protection system belonging to a higher safety class shall however, operate in such a situation, and thus a class 1 postulated accident has been set as the criterion. According to the same principle, the failure of a back-up protection system, control systems of severe reactor accidents or other I&C systems in safety class 3 shall not lead to a situation that is worse than a class 1 postulated accident.

When combined with a separate postulated accident in class 2, the failure of an I&C system in safety class 2 is may to lead to a severe accident. The back-up protection system has been designed to handle postulated accidents in class 1, which means that the more significant initiating events may be beyond the abilities of the back-up protection system. The functions of the back-up protection system would, however, be similar in cases such as leaks of various sizes.

In postulated accidents, the status of the plant shall not be worsened by the failure of the back-up protection system or I&C systems in severe reactor accidents. The failure of the back-up protection system, combined with a DEC situation, is positioned in the residual risk area; in other words, it is assumed that the situation could lead to a severe reactor accident.

The section discussing technological breakthroughs has been removed from requirement 5203, related to the architecture requirement specification, because predicting technological breakthroughs at the level of requirement specifications and in a verifiable manner is impossible.

The definition of essential accident instrumentation has been removed, so that requirement 5214 has been rephrased and targeted at operational occurrences, postulated accidents and design extension conditions. The section addressing containment instrumentation has been moved to the chapter, and it has been specified.

Terminology related to systems implementing limitation functions as well as protective I&C systems has been clarified. Requirements for different systems have been distinguished from each other more clearly.

Diverse instrumentation (5229, 5230) is connected to the primary protection system, which can be considered a change from the previous version of the requirement. The fulfilment of the diversity principle was more extensively required from the instrumentation connected to the protection I&C system.

A requirement concerning the failure criterion for management of severe reactor accidents and instrumentation has been added to the chapter. In its current form, the requirement can be derived from other requirements. This makes it a clarification and the requirement level is not affected. In addition, a requirement for enabling and performing periodic testing has been added to the chapter. Previously, these requirements were targeted at the management of severe reactor accidents and instrumentation through requirements set for protection I&C systems. Therefore, the requirement is not affected except in so far as the Regulation STUK Y/1/2018 enables the transition to a safe state after a severe reactor accident also by other means than entirely independent systems.

Sections already presented as general requirements elsewhere have been removed from requirement 5233. Furthermore, the scope of the periodic tests has been specified.

Requirement 5240 concerning the failure of I&C systems has been corrected so that it is in line with the other requirements, and duplicates have been removed. Updated background information on applying the requirement has been provided previously in this chapter.

Requirements concerning information security have been moved from the chapter to Guide YVL A.12. Testing requirements have also been removed because such requirements are presented in Guide YVL E.7.

3.4.3 Chapter 5.3 Control rooms

Requirements for control room design are presented in this chapter.

The requirement concerning the HFE programme has been modified and moved to chapter 4.4 which addresses human factors.

3.4.4 Chapter 5.4 Electrical power systems

Requirements for electrical power systems are presented in this chapter.

A new requirement has been added to the beginning of the chapter, entailing that the level of architecture of electrical power systems shall be processed as a system, meaning that the processing shall be considered comparable to the processing of I&C. The requirement is new and may affect procedures.

Requirement 5405 entails that, when making a cross-connection, safety improvements at the plant shall be examined instead of examining the reliability of an individual system. This may affect procedures.

The section discussing a back-up control room has been removed from requirements 5424, 5429 and 5430 due to its excessive amount of details.

Requirement concerning the fulfilment of the diversity principle in designing on-site emergency power supply has been added as requirement 5426a. The purpose of this is to enable the fulfilment of the diversity principle in many ways according to the principles outlined in chapter 4; the internal diversity of the system may also be a solution. Requirements 5436–5440 concerning categorically separate and independent emergency power supply have been removed, and requirements concerning system properties have been combined with the others presented in the chapter.

A requirement concerning emergency power supply in severe reactor accidents, which shall be single failure tolerant, has been added as requirement 5426b. The system shall also be independent from other levels of defence in accordance with chapter 4 and requirement 5415. With the addition, requirements concerning the properties of emergency power supply sources can also be targeted at the emergency power supply system in severe reactor accidents.

The requirements concerning the diversity principle can be considered less strict than before. Regarding systems related to severe reactor accidents, a requirement concerning material reserves in the plant area has been added.

Requirements 5445, 5448, 5450 have been clarified so that they are applicable to safety-classified systems.

Overlapping requirements have been removed from the chapter.

3.4.5 Chapter 5.5 Ventilation and air conditioning systems

Requirements concerning ventilation and air conditioning systems have been presented in this chapter. Furthermore, 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 as well as the related fire protection design bases shall be complied with in design work.

Requirement 5507 has been clarified with regard to applying the separation principle so that the requirement cannot be interpreted to entail that subsystems should have separate ventilation stacks. The requirement level has not been changed.

Two new requirements concerning filters have been added to the chapter. Furthermore, a reference to delaying exhaust air when necessary has been added to requirement 5525. Reference 5510 to the rules and regulations issued by the Ministry of the Environment and the Ministry of the Interior has been specified so that it is considered necessary to follow these rules also in connection with system changes.

3.5 Chapter 6 Documents to be submitted to STUK

Requirement 612a, concerning the submission of system quality and qualification plans and requirement specifications along with similar system documentation related to the preliminary safety analysis report, has been added to the chapter. Previously, parts of the requirement were included in Guide YVL E.7 but, in terms of Guide YVL B.1, the issue at hand was only described in the explanatory memorandum. Therefore, the requirement level has not been changed in a substantial manner, but it

clarifies and harmonises expectations concerning the processing of the documentation.

Sections concerning supplier organisations have been modified in requirements 607 and 618.

For the sake of clarity, a reference to buildings has been added to requirements 609, 611, 620 and 622 concerning system descriptions presented in the preliminary and final safety report, because a system description is also required from the buildings. Previously, the requirement for descriptions was only included in requirement A01 of the appendix.

Requirements concerning conceptual plans and pre-inspection documentation prepared for modifications of operating plants have been updated. Requirement 627 now includes a definition of situations where a conceptual plan shall be prepared; requirement 627a defines the content of the conceptual plan. Requirements concerning pre-inspection documentation have been separated under the same principle, meaning that requirements 628 and 628a determine in which cases pre-inspection documentation concerning modifications shall be submitted for approval or for information. The content requirement has been presented in requirement 628b. Requirements for implementing requirement specifications as well as quality and qualification plans have been presented in requirements 628c and 628d.

A subchapter has been added to the chapter, addressing the evaluating system changes made after granting the construction licence but before the handling of the operating licence. Detailed design was previously addressed in requirement 619, in the chapter concerning operating licence applications, and the maintenance of a safety report during construction was addressed in the chapter addressing system changes. On that basis, it was not unambiguous which procedure should be followed between the processing of the construction licence and operating licence.

Other minor corrections and specifications were made to the chapter and some parts were removed on account of overlaps.

3.6 Chapter 7 Regulatory oversight of safety design

Requirements overlapping with other guides or requirements have been removed from the chapter.

4 International regulations concerning the scope of the Guide

WENRA reference levels and requirements for new nuclear power plants as well as IAEA requirements have been taken into account in the preparation of the Guide, in accordance with the Guide’s list of references.

In other respects, changes to international requirements have not caused significant changes to the content of the Guide. The requirement concerning the common systems of nuclear power plants and fuel storage facilities has been specified particularly with regard to simultaneous accidents occurring at plant units.

5 Impacts of the Tepco Fukushima Dai-ichi accident

Due to the changes in WENRA reference levels, experiences of OL3 and the accident at Tepco Fukushima Dai-ichi, requirements concerning design extension conditions and plant self-sufficiency have been added to the version of Guide YVL B.1 published in 2013.

6 Needs for changes taken into account in the update

The needs for changes due to changes made to international and national laws/regulations and the change proposals made in connection with the preparation of the YVL Guide implementation decisions (SYLVI) together with others recorded in STUK's change proposal database have been considered when updating the requirements. In addition, the possibilities to reduce the so-called administrative burden have been considered.

Comments given to reduce the administrative burden have previously been given also in connection with implementing the Guide published in 2013. The aim was to use consistent terminology and clarify connections between quality plans (incl. possibilities for combination) when updating Guide YVL B.1 and other guides that discuss quality plans. Requirements concerning conceptual plans and pre-inspection documentation prepared during modification work of operating plants has been corrected and specified; in addition, smaller changes where documentation is not required for approval have been defined. Submission times for requirement specifications concerning quality and qualification plans have been added.

In terms of safety assessments, the document primarily the requirements concerning the planner's "safety assessment" have been detailed. In other words, a report that is generally considered a safety assessment is not required; an assessment of the implementation of the design process is. This removes duplicate assessments. In other respects, the modifications take into account various specification needs that have emerged during the implementation as well as in other instances of applying the guides. Duplicates have been removed and therefore some subchapters have been entirely removed. The amendments have been presented in more detail in chapter 3 "Justifications of the requirements".