Safety criteria for design of nuclear power plants

This Guide is in force as of 1 March 1996 until further notice. It replaces Guide YVL 1.0, issued 1 December 1982.

Third, revised edition
Helsinki 1997
Oy Edita Ab
ISBN 951-712-147-4
ISSN 0783-232X

Authorisation

By virtue of section 55, second paragraph, point 3 of the Nuclear Energy Act (990/87) and section 29 of the Council of State Decision (395/91) on General Regulations for the Safety of Nuclear Power Plants, the Finnish Centre for Radiation and Nuclear Safety (STUK) issues detailed regulations concerning the safety of nuclear power plants.

YVL Guides are rules an individual licensee or any other organisation concerned shall comply with, unless STUK has been presented with some other acceptable procedure or solution by which the safety level set forth in the YVL Guides is achieved. This Guide does not alter STUK's decisions which were made before the entry into force of this Guide, unless otherwise stated by STUK.

Translation by MSO. Original text in Finnish.

FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY
P.O.BOX 14, FIN-00881 HELSINKI, FINLAND
Tel. +358-9-759881
Fax +358-9-75988382

1 General

According to the Nuclear Energy Act (990/87), the use of nuclear energy must be safe and it may not harm man, the environment or property. A nuclear power plant's safe design, and the high quality of its components and operation contribute to the safety of the plant. The maintenance and improvement of an achieved safety level require a highly advanced safety culture.

General safety requirements for nuclear power plants are presented in the Council of State Decision (395/91). Requirements for the safety of plant structures are presented in sections 7–22 of the Decision.

According to section 3 of the Decision (395/91), *the general objective is to ensure nuclear power plant safety so that nuclear power plant operation does not cause radiation hazards which could endanger safety of workers or population in the vicinity or could otherwise harm the environment or property.* To achieve this objective, events are taken into account already in planning which may

— relate to plant operation
— arise from the plant site or the environment
— arise from unintentional or intentional human activity.

In this Guide, safety principles which supplement the Council of State Decision and which are to be used in the design of nuclear power plants are presented. Guide YVL 1.1 presents how STUK controls the design, construction and operation of nuclear power plants.

In the design of nuclear power plants, general safety requirements for physical protection and emergency response arrangements at nuclear power plants presented in Council of State Decisions (396/91) and (397/91) shall also be taken into account. Detailed requirements for physical protection and emergency preparedness arrangements are presented in Guides YVL 6.11 and YVL 7.4.

For the construction of a nuclear power plant, a decision in principle and a construction permit referred to in the Nuclear Energy Act are required. Correspondingly, to operate the plant, an operating licence as referred to in the Nuclear Energy Act is required.

According to section 9 of the Nuclear Energy Act, the licensee is responsible for the safe operation of the plant. The licensee is obliged to demonstrate that safety principles are met. The requirements for safety analyses are presented in Guides YVL 2.2 and YVL 2.8. Quality assurance is discussed in Guide YVL 1.4.

2 Radiation safety

According to section 3 of the Radiation Act (592/91), the provisions of section 2 and chapter 9 of this Act also apply to the use of nuclear energy. Worker dose limits are prescribed in chapter 2 of the Radiation Decree (1512/91).

According to chapter 7 of the Council of State Decision (395/91), *radiation exposure arising from the operation of a nuclear power plant shall be kept as low as reasonably achievable. A nuclear power plant and its operation shall also be designed so that the limits presented in this decision are not exceeded.*

Even though set limits have not been exceeded there is no justification for not implementing a solution which would essentially reduce the radiation dose of workers or the population or, environmental pollution.

2.1 Limitation of worker radiation exposure

Plant design

The quality and quantity of radioactive substances in a nuclear power plant's rooms and components shall be evaluated during the plant's design, taking into account operational conditions and accidents.

The production and transfer of radioactive substances at the plant shall be limited. The corrosion, activation and transfer of substances significantly affecting radiation doses shall be kept low by
— the choice of structural materials and solutions, and coatings
— the design of water chemistry and clean-up systems.

Structures, systems and components containing significant amounts of radioactive substances shall be placed in their own rooms in the first place, or shall be otherwise separated so that workers are not exposed to radiation originating from them while operating, inspecting or maintaining the plant. Sufficient safety margins shall be employed in radiation protection design. Passageways and any working space in regular use shall be so designed and located that the external dose rate is insignificant and the possibility of internal radiation exposure low.

The rooms of the nuclear power plant shall be classified on the basis of estimated radiation conditions. Rooms which require radiation surveillance shall be placed in an area of their own so that access there can be restricted and controlled as appropriate. Working areas in daily use are not be placed in this area without specific justification.

Such prerequisites and conditions shall be designed for the operation, inspection and maintenance of components that the number of work phases carried out while under exposure to radiation is insignificant and of short duration.

There shall be sufficient quarters and equipment at the nuclear power plant to clean, repair and service contaminated components.

The nuclear power plant shall be so designed that it is possible to work long-term in the control room and that the components required to restrict radioactive releases can be operated and serviced even during accidents.

Detailed instructions as to how to take radiation safety into account in nuclear power plant design can be found in Guide YVL 7.18.

Radiation monitoring

To ensure radiation monitoring, there shall be a sufficient number of fixed and portable radiation measurement devices at the plant for determining the external dose rate and what radioactive substances there are in the air, systems or on surfaces. There shall also be appropriate laboratory facilities and equipment for sample analysis and equipment for individual dose monitoring.

Furthermore, alarming measurement devices shall be used for radiation monitoring in such a way that, during the nuclear power plant's operational conditions, nobody is exposed to radiation without knowing it and in a degree harmful to health.

When designing radiation monitoring, provision shall also be made for accidents. It shall be possible to take at least the following measures during accidents:
— measurement of dose rate inside the containment
— determination of the concentration of radioactive substances in gas phase inside the containment
— determination of the concentration of radioactive substances in the coolant.

Detailed requirements for the radiation protection of nuclear power plant workers are presented in Guide YVL 7.9. In Guide YVL 7.10, requirements for worker radiation dose monitoring and dose reporting are presented. Guide YVL 7.11 deals with radiation monitoring systems and equipment.

2.2 Limitation and monitoring of radioactive discharges

According to section 26 of the Council of State Decision (395/91), *releases of radioactive materials from a nuclear power plant*

and their concentrations in the environment shall be effectively monitored.

Systems and components containing radioactive substances shall be designed in such a way that releases of radioactive substances and the radiation exposure of the population living in the vicinity of the plant can be kept low. Systems which are capable of cleaning fluids and gases containing radioactive substances shall be designed. These systems shall effectively restrict radioactive releases and the radiation exposure arising from them in the environment.

The plant shall be provided with systems which monitor all planned release pathways of radioactive substances. These systems shall be designed to measure and record data about the amount of radioactive substances to be released to the environment during operational conditions and accidents. Release limits shall be defined for the various release pathways and also the necessary measures to restrict the releases if these limits are exceeded.

It must be possible to monitor the releases of radioactive substances along planned pathways also in the event of a single failure during operational conditions and accidents.

In the plant's vicinity, a sufficient number of automated, continuous-monitoring measurement stations for external radiation shall be placed which indicate possible radioactive releases harmful to the environment, if any. Reliable, real-time assessment of the spreading of radioactive substances into the environment must be possible by meteorological measurement devices.

Detailed requirements for the limitation of a nuclear power plant's radioactive discharges into the environment are presented in Guide YVL 7.1. Requirements for the measurement of releases are presented in Guide YVL 7.6. Radiation monitoring in the plant's environment is dealt with in Guide YVL 7.7 and meteorological measurements in Guide YVL 7.5.

2.3 Ventilation

The rooms of the plant where significant amounts of airborne radioactive materials may occur shall be provided with ventilation and filtering systems which

— reduce the concentrations of airborne radioactive substances within the plant
— prevent the spreading of radioactive substances within the plant
— limit the releases of radioactive substances into the environment.

These ventilation and filtering systems shall operate at planned capacity even in the event of a single failure during operational conditions and postulated accidents.

A filtered inlet air system shall be designed for the nuclear power plant's control room, fallout shelter and the rooms required for accident management measures. These systems shall be capable of carrying out their safety functions even in the event of a single failure during operational conditions and accidents.

Detailed requirements for the nuclear power plant's ventilation systems are presented in Guide YVL 5.6.

2.4 Nuclear waste handling and treatment systems

A nuclear power plant shall have adequate rooms for the handling, treatment and storage of low and medium level radioactive waste. Systems shall be designed for these rooms to safely handle, treat and transfer waste and to measure the amount and quality of radioactive substances in the waste.

Detailed requirements for radioactive waste handling and storage at the nuclear power plant are presented in Guide YVL 8.3.

2.5 Decommissioning

Provision for a nuclear power plant's decommissioning shall be made already during the plant's design phase. One criterion

when deciding the plant's materials and structural solutions shall be that the volumes of decommissioned waste are to be limited. It shall be possible to decommission the plant and remove radioactive structures and components in such a way that the radiation exposure of workers and the environment remains low.

3 Nuclear safety

The safety level of a nuclear power plant shall be raised as high as practicable to achieve the objectives presented in section 6 of the Nuclear Energy Act and in section 3 of the Council of State Decision (395/91). The more severe an accident's consequences to man, the environment and property could be, the smaller the likelihood of its occurrence shall be.

According to section 13 of the Council of State Decision (395/91), *in design, construction and operation proven or otherwise carefully examined high quality technology shall be employed to prevent operational transients and accidents (preventive measures).*

A nuclear power plant shall encompass systems by the means of which operational transients and accidents can be quickly and reliably detected and the aggravation of any event can be prevented. Accidents leading to extensive releases of radioactive materials shall be highly unlikely (control of transients and accidents).

Effective technical and administrative measures shall be taken for the mitigation of the consequences of an accident. Countermeasures for bringing an accident under control and for preventing radiation hazards shall be planned in advance (mitigation of consequences).

According to section 14 of the Council of Decision (395/91), *dispersion of radioactive materials from the fuel of the nuclear reactor to the environment shall be prevented by means of successive barriers which are the fuel and its cladding, the cooling circuit (the primary circuit) of the nuclear reactor and the containment building.* Sufficient safety margins shall be used in design to maintain the integrity of these successive technical barriers.

According to section 18 of the Council of State Decision (395/91), *in ensuring safety functions, inherent safety features attainable by design shall be made use of in the first place. In particular, the combined effect of a nuclear reactor's physical feedbacks shall be such that it mitigates the increase of reactor power.*

If inherent safety features cannot be made use of in ensuring a safety function, priority shall be given to systems and components which do not require an off-site power supply or which, in consequence of a loss of power supply, will settle in a state preferable from the safety point of view.

Systems which perform the most important safety functions shall be able to carry out their functions even though an individual component in any system would fail to operate and, additionally, any component affecting the safety function would be out of operation simultaneously due to repairs or maintenance (redundancy principle).

Safety systems which back up each other as well as parallel parts of safety systems shall be separated from each other so that their failure due to an external common cause failure is unlikely (separation principle).

In ensuring the most important safety functions, systems based on diverse principles of operation shall be used to the extent possible (diversity principle).

Detailed requirements for the application of failure criteria and the diversity principle can be found in Guide YVL 2.7.

3.1 Reactor

Fuel and reactor design

According to section 15 of the Council of State Decision (395/91), *the probability of significant degradation of fuel cooling or of a fuel failure due to other reasons, shall be low during normal operational conditions and anticipated operational transients.*

During postulated accidents, the rate of fuel failures shall remain low and fuel coolability shall not be endangered.

The possibility of a criticality accident shall be extremely low.

The reactor and related systems must not contain specific features which could cause a significant reactivity increase in connection with an anticipated operational transient or postulated accident and thus aggravate the consequences of an event.

The structure of the fuel and reactor internals shall be designed compatible so that when the reactor is assembled, each component fits reliably in the right place and position. After reactor loading, it must be possible to check that the fuel and reactor internals have been correctly positioned.

The reactor pressure vessel internals shall be so designed and installed that they maintain position during operational conditions and postulated accidents, and that they withstand all loads encountered during these conditions without endangering reactor shutdown or cooling.

According to section 18 of the Council of State Decision (395/91), *in particular, the combined effect of a nuclear reactor's physical feedbacks shall be such that it mitigates the increase of reactor power.*

Furthermore, the reactor core and related cooling, protection and reactivity control systems shall be so designed that

— reactor power is stable during normal operation
— potential power oscillations can be detected and suppressed before fuel design limits are exceeded.

Detailed requirements for fuel design and design limits are presented in GuideYVL 6.2.

Reactivity control and reactor shutdown

The plant shall be provided with two independent reactivity control systems with diverse operating principles. Each of them shall be separately capable of shutting down the reactor during operational conditions. At least one of these systems alone must be capable of maintaining the reactor in a shutdown state at any reactor temperature.

The reactivity control systems shall be designed to have a capability of their own or a combined capability together with the poison added by the emergency core cooling system of reliably maintaining the reactor in a shutdown state in postulated accidents.

The reactivity control systems shall be so designed that a reactor which has sustained damage in a severe accident, or its debris, are maintained sub-critical.

One of the reactivity control systems shall be based on fixed absorbators, such as e.g. control rods.

The reactivity control systems together with the protection system shall be designed to assure that a single malfunction of the reactivity control systems, such as control rod withdrawal at normal speed, does not result in the exceeding of the fuel design limits.

In postulated accidents caused by the failure of the reactivity control systems (e.g. control rod ejection or drop, or the sudden reduction of some other absorbing material from the reactor core), the degree and speed of reactivity increase shall be limited in such a way that the design limits for fuel coolability are not exceeded and that the number of fuel failures possibly occurring in consequence of the accident is kept small.

The reactivity control systems shall be designed to assure that both systems are capable of accomplishing their safety functions even in the event of a single failure.

If only one of the two reactivity control systems is capable of maintaining the reactor in a shutdown state at any temperature, it must be capable of carrying out its safety function even in the event of a single failure, although any device affecting the safety function would be inoperable due to repair or maintenance.

The reactivity control systems shall be designed to assure that a single failure of the control system or a single control error does not cause a power increase reaching a limit which requires the reactor to be shut down.

3.2 Reactor primary circuit and cooling systems

Ensuring the integrity of the reactor primary circuit

According to section 16 of the Council of State Decision (395/91), *the primary circuit of a nuclear reactor shall be so designed that the stresses imposed upon it remain, with sufficient confidence, below the values defined for structural materials for preventing a fast growth crack during normal operational conditions, anticipated operational transients and postulated accidents. The possibility of a primary circuit break due to other reasons shall be low, too.*

During the design, manufacture, installation, inspection and testing of the reactor primary circuit, state-of-the-art know-how and technology shall be effectively used to prevent a fast growth crack and any other serious failure. An attempt shall be made especially to limit frequently occurring loads and stress peaks transferred to the circuits' components, and the number of welded seams in the circuit.

In designing the primary circuit, radiation-induced and chemical effects and also thermal, hydraulic and mechanical loads shall be taken into account in such a way that fracturing of the pressure vessel and of other components of the primary circuit is highly unlikely.

The safety margin for operational conditions and postulated accidents must be sufficient as regards the brittle behaviour of structural materials. Uncertainty factors shall be taken into account during design when the properties of structural materials, irradiation of the materials and the effects of irradiation on material properties, stresses and flaw sizes are determined.

The primary circuit and its components shall be so designed that
— important areas and details can be periodically inspected and their structural integrity and leaktightness evaluated
— the periodic reactor pressure vessel materials testing programme to determine the effects of radiation and the ageing of structural materials can be implemented.

Detailed requirements for the inservice inspections of the reactor pressure vessel are presented in Guide YVL 3.8.

Reactor coolant system

The reactor coolant system and the associated auxiliary, control and protection systems shall be so designed that the design bases of the reactor primary circuit are not exceeded during operational conditions.

The shape and construction of the reactor coolant system shall be such that
— the possibility of coolant leaks below the top of nuclear fuel is extremely small during operational conditions
— measures affecting the primary circuit during an outage do not essentially increase the risk of a coolant leak.

The reactor pressure control shall be so designed that, during normal operational conditions, pressure can be maintained within the limits required by normal cooling even in the event of a single failure in some pressure regulating component or control system. The

design basis shall specifically include that during operational conditions there is no need
— to remove primary coolant outside closed systems, with the exception of a possible brief discharge to manage a transient
— to operate a safety valve.

During accidents, the pressure control system must take care of the reactor coolant system's overpressure protection and pressure reduction in case of failures specified in detail in Guide YVL 2.4. Pressure reduction shall be so planned that a severe accident at high pressure can be reliably prevented.

Control of the reactor coolant volume shall be so designed that the coolant volume in the primary circuit can be kept within the limits required for normal cooling even in the event of a single failure in some component or control system affecting the volume control.

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

A reactor coolant clean-up system shall be designed to remove radioactive substances and other impurities from the coolant during operational conditions.

An emergency cooling system shall be designed for coolant leaks which cannot be taken care of by normal reactor volume control systems or which otherwise ensures efficient reactor cooling so that the design limits for fuel coolability are not exceeded. In designing the emergency cooling system, various leak sizes shall be considered so that the largest leak equals to a complete, sudden rupture of the largest primary circuit pipe. Furthermore, the possibility to operate the system long enough shall be ensured.

The operability and efficiency of the emergency cooling function during postulated leak conditions shall be ensured by primary circuit configuration and the appropriate location of emergency cooling connections. The emergency cooling system shall be capable of carrying out its function also in the event of a single failure even if any component affecting the safety function would be simultaneously inoperable due to repair or maintenance. Furthermore, the diversity principle shall be observed in the design of the emergency coolant system.

Primary circuit cooling and decay heat removal

The nuclear power plant shall be equipped with systems which cool down the primary circuit during operational conditions. These systems shall be operable also in the event of a single failure.

It must be possible to accomplish reactor decay heat removal and heat transfer to the final heat sink during operational conditions and postulated accidents even in the event of a single failure although any component affecting these safety functions would be simultaneously inoperable due to repair or maintenance. The reactor decay heat removal and heat transfer to the final heat sink shall be arranged in compliance with the diversity principle. In the plant's design, provision shall be made against interruption in the use of the final heat sink normally used.

3.3 Containment function

Containment

A nuclear power plant shall be designed a leaktight containment which limits radioactive releases during operational conditions and accidents.

According to section 17 of the Council of State Decision (395/91), *the containment shall be designed so that it will withstand reliably pressure and temperature loads, jet forces and impacts of missiles arising from anticipated operational transients and postulated accidents.*

Furthermore, the containment shall be designed so that the pressure and tempera-

ture created inside the containment as a consequence of a severe accident will not result in its uncontrollable failure.

The possibility of the creation of such a mixture of gases as could burn or explode in a way which endangers containment integrity shall be small in all accidents.

The hazard of a containment building failure due to a core melt shall also be taken into account in other respects in designing the containment building concept.

The containment shall be encased in a secondary containment building so that any radioactive substances which leak from the primary containment can be collected and treated as appropriate. In case the primary containment must be made non-leaktight due to reactor reloading or maintenance, the secondary containment shall be designed to function as an efficient technical barrier to the spreading of radioactive substances in accidents assessed possible under these operational conditions.

The primary containment and the secondary containment protecting it shall be so designed that the external events presented in subsection 3.14 do not jeopardise the operability of the containment systems and the primary containment leaktightness in accidents. These buildings shall also be so designed that they form an adequate physical shield against external events for the reactor and the systems relating to it.

It must be possible for systems ensuring containment leaktightness in connection with a severe accident to carry out their safety function also in the event of a single failure.

Penetrations, access openings and isolation

The location, structure, protection and sealing materials of containment penetrations, access openings and isolation valves shall be so designed that they maintain operability and leaktightness during operational conditions and accidents. Particular attention shall be paid to the long-term durability of the sealing materials in severe accidents. In the design of the penetrations, loads transferred from piping shall be observed.

As containment access openings, air locks shall be used the structure of which is such that at least one door is always closed when the air lock is in use. There shall be at least two access openings. These shall be located sufficiently much apart from each other so that during any event at least one of them provides an emergency exit from the containment. Both shall also be manually operable.

A minimum of two isolation valves which operate independently of each other shall be designed in every pipe which is part of the primary circuit or directly connecting to the containment inner space and which penetrates the containment. Each isolation valve shall be either automatic or locked-closed. Any automatic containment isolation valve must be controlled by the plant protection system or shall self-close (check valve) if flow is lost. Primarily, there shall be one isolation valve inside the containment and one outside it.

Every pipe penetrating the containment and which is not part of the primary circuit and not directly connected to the containment inner space shall have at least one isolation valve outside the containment. The isolation valve must be either automatic, locked-closed or remotely operable by hand.

The containment external isolation valves shall be as closely located to the containment as possible. It must be possible to observe their position from the control room, with the exception of manually operated valves which are locked-closed. A check valve shall not be used as a containment external isolation valve.

The containment isolation valves shall be so designed in the first place that they close independently if power supplied to their actuators is lost.

It must be possible to isolate the containment during accidents even in the event of a single failure.

In GuideYVL 2.8, requirements are set for the reliability of containment isolation. Guide YVL 5.3 handles nuclear power plant valves.

Pressure and temperature management

The nuclear power plant shall be provided with systems which remove decay heat from the containment during accidents. These safety function of these systems is to reduce containment pressure and temperature and keep them sufficiently low. The systems shall be so designed that their operation or inadvertent start-up does not endanger containment integrity or other safety functions during operational conditions or accidents.

Containment heat removal in postulated accidents must be possible even in the event of a single failure, although any component affecting the safety function would simultaneously be inoperable due to repair or maintenance.

To ensure containment integrity in severe accidents, systems, structures and components shall be designed which are independent of systems designed for plant operational conditions and postulated accidents. When analysing pressure and temperature loads, the below facts in particular shall be considered

— decay heat yielded by the reactor and its debris
— total volume of uncondensed gases
— heat loads arising from combustible gases.

When evaluating the volume and timing of non-condensable gases released during severe accidents, particular attention shall be paid to how overheated reactor internals and fuel react with water. In estimating the volume, it shall be assumed that 100% of easily oxidising reactor core materials react with water. Furthermore, radiation-induced disintegration of water, chemical reactions considered possible in the containment and the primary circuit, and melted core-concrete interaction on the containment floor if the core melt has penetrated the reactor pressure vessel shall also be analysed.

The release into the environment of a steam-gas mixture accumulated in the containment shall not be designed as the primary measure of preventing containment pressurisation. A containment filtered venting system shall be designed which can be used to remove any overpressure caused by non-condensable gases possibly released in a later phase of an accident.

The effects of the core melt possibly discharged from the high-pressure primary circuit to the containment in consequence of a severe accident shall be taken into account in the containment design.

Treatment of combustible gases

Containment systems shall be designed to reduce the concentrations of oxygen or combustible gases formed in accidents, or to prevent in some other way gas explosions or uncontrollable gas fires which may jeopardise containment leaktightness or the operability of accident management equipment inside the containment.

The treatment of combustible gases inside the containment shall be possible during postulated accidents even in the event of a single failure.

For the reduction of combustible gases, systems and components shall be used in the first place which do not rely on external power supply.

Containment bypass prevention and control

In the design of the containment function, particular attention shall be paid to the prevention of containment bypass during operational conditions and accidents. In this Guide, containment bypass means loss of integrity or operability, or wrong position, of

a structure or component designed to isolate the containment in the consequence of which the containment is not leaktight anymore.

The containment shall be provided with monitoring equipment by which any containment bypass and non-leaktightness which has bearing on environmental radiation exposure during accident conditions can be detected during operational conditions.

Pressure management during PWR primary-to-secondary leaks shall be so arranged that no coolant discharges to the environment are required.

Pipelines connecting to the primary circuit shall be so designed that they withstand the same pressure as the primary circuit, unless it can be demonstrated that these systems can be reliably isolated from the primary circuit under any condition. The primary cooling systems shall be so designed that no single component failure leads to containment bypass or to coolant water ending up outside emergency cooling circulation.

Management of the reactor debris

The containment lower space shall be so designed that a core melt possibly formed in a severe accident with high certainty does not cause a containment melt-through.

Provision shall be made for the cooling of the reactor debris on the bottom of the containment in such a way that radioactive substances released into the containment air space can be effectively restricted and that the radiation heat emitted by the reactor debris does not break the containment integrity.

The management of hot gases formed in severe accidents shall be so planned that the gases do not break the containment integrity via the steam generators or otherwise.

Cleaning of the gas space

Containment systems shall be designed to remove radioactive substances from the gas space during accidents. In designing these systems, special attention shall be paid to radioactive iodine and radioactive substances in the form of solids and also to events including a containment leak during an accident.

It must be possible to clean the containment gas space during accidents even in the event of a single failure.

3.4 Protection systems

The nuclear power plant shall be equipped with a protection system which during anticipated operational transients automatically initiates the appropriate safety functions to assure that fuel design limits and the primary circuit design conditions are not exceeded. The protection system shall also detect any accidents at the plant and initiate the necessary safety functions.

According to paragraph 2 of section 22 of the Council of State Decision (395/91), *a nuclear power plant shall contain automatic systems that maintain the plant in a safe state during transients and accidents long enough to provide the operators a sufficient time to consider and implement the correct actions.* The sufficiency of this time shall be assessed based on analyses performed on plant operational transients, accidents and human operations. It must be possible for the operators to initiate the safety functions necessary during any specific event even earlier if they consider it necessary for ensuring safety.

Manual initiation of the protection system shall be implemented using technology as reliable as possible. In addition to the manual initiation of individual devices, it shall also be possible to manually trip protective signals, if necessary.

The protection system shall be so designed that any operation performed by the operators in the control room or any control system operation cannot prevent or stop a safety function initiated by the protection system

before the function has been completed (reactor scram, containment isolation) or before the plant parameters indicate there is no need for protection anymore (emergency cooling).

The protection system shall be so designed that in case of its failure it settles in a state preferable from the plant safety point of view.

The protection system which initiates the safety functions shall operate during anticipated operational transients and postulated accidents even in the event of a single failure, although any component affecting a safety function would simultaneously be inoperable due to repair or maintenance. Also the diversity principle shall be complied with in the design of the reactor protection system.

In the first place, the protection system shall be separated from the control system and other automation systems. Any possible interdependence between the protection, control or other automation systems shall not endanger safety.

Detailed design requirements for the design of the protection system are presented in Guide YVL 5.5.

3.5 Electrical systems

According to paragraph 4 of section 18 of the Council of State Decision (395/91), *a nuclear power plant shall have on-site and off-site electrical power supply systems. The execution of the most important safety functions shall be possible by using either of the two electrical power supply systems.*

In addition to these systems, the plant shall be provided with systems which enable power supply from the main generator to the plant's safety significant systems in case the connection to the external transmission grid is lost.

The on-site electrical power supply system serving the safety functions shall be capable of carrying out its functions during anticipated operational transients and postulated accidents even in the event of a single failure, although any component affecting the safety function would simultaneously be inoperable due to repair or maintenance.

For electrical power supply, there shall be two separate, independent grid connections from the external grid to each parallel section of the on-site electricity distribution system. These grid connections shall be so designed that during operational conditions and postulated accidents, the simultaneous loss of both is unlikely. It must be possible to start operation of both grid connections quickly enough after the plant main generator has been separated from the grid.

The plant's electrical power supply units shall be so designed that the loss of the remaining power supply units in case of the loss of a single power supply unit or caused by the same reason is highly unlikely.

In nuclear power plant design, the possibility of the on-site and off-site power supply units being simultaneously lost shall be considered. As provision against such a situation, the plant shall have available a power supply unit which is independent of the electrical power supply units designed for operational conditions and postulated accidents. It must be possible to introduce this power supply unit into operation quickly enough and its capacity shall be sufficient to remove reactor decay heat, to ensure primary circuit integrity and to maintain reactor sub-criticality.

Batteries backing up the operation of electrical systems important to safety shall maintain their capability to operate at least for two hours under any circumstances.

Detailed requirements for plant electrical systems are presented in Guide YVL 5.5.

3.6 Monitoring and control

Instrumentation and control

The reactor and other structures, systems and components of the nuclear power plant shall

be provided with sufficient instrumentation for monitoring the process parameters and the operation and condition of systems. The plant shall have reliable control systems for keeping the process parameters and systems within the specified operating range. Together with the systems and components they control, these control systems shall ensure that during operational conditions or in the event of a single failure of the control systems there will be no need to start safety systems designed for postulated accidents.

For the purpose of accident monitoring and management, appropriate measuring and monitoring instrumentation shall be designed for the plant by which the operating personnel obtains sufficient data for event assessment and for the planning and implementation of countermeasures.

Monitoring equipment shall be designed for the nuclear power plant to manage and monitor the progress of severe accidents and to give data about
— the possible re-criticality of the reactor or its debris
— the threat of a reactor pressure vessel melt-through
— the location of the reactor debris
— other factors possibly endangering containment integrity.

The measurement systems designed for accident monitoring and management shall maintain operability even in the event of a single failure.

The measurement systems shall be capable of measuring accurately enough over the entire range within which the measured parameters vary during operational conditions or accidents. As far as possible, the measurements shall be so planned that the operators will easily see if the measurement fails or the measurement range is exceeded.

The control equipment shall be designed to record process parameters indicating plant state and also system control signals so that the plant's operational events can be analysed afterwards.

Requirements for electrical and automation systems and components are presented in Guide YVL 5.5. Guide YVL 7.11 applies to radiation measurements.

Control rooms

According to paragraph one of section 22 of the Council of State Decision (395/91), *a nuclear power plant's control rooms shall contain equipment which provide information about the plant's operational state and any deviations from normal operation as well as systems which monitor the state of the plant's safety systems during operation and their functioning during operational transients and accidents.*

The control room shall be so designed that the measures necessary to control the plant can be performed there during operational conditions and accidents.

The structures and safety systems of the control room shall be so designed that safe working is possible there even during accidents.

According to paragraph 3 section 22 of the Council of State Decision (395/91), *there shall be an emergency control post at a nuclear power plant which is independent of the control room and the necessary local control systems by the means of which the nuclear reactor can be shut down and cooled and residual heat from the nuclear reactor and spent fuel stored at the plant can be removed.*

The emergency control post shall be so designed that the reactor can be shut down from there and the plant can be brought to stable shutdown state.

The control systems of the emergency control post outside the control room shall be separated from the control systems of the control room in such a way that if the equipment in one fire compartment are entirely destroyed by fire this does not harm both control systems so much that safety functions could not be carried out.

Ergonomic principles which apply to control room work and which make possible the reliable performance of control measures shall be considered in the design of the control room, the emergency control post and local control posts. Particular attention shall be paid to the design of control panels, alarm systems and computer-based display systems so that, in the event of a transient or accident the operators can obtain a good overall picture of the plant state and that data most important for the plant's safety are clearly displayed.

If possible, the diversity principle shall be complied with in the design of systems which give an overall picture of the plant state and provide data relating to alarms.

Detailed requirements for control room design are presented in Guide YVL 5.5, those relating to requirements for control room radiation protection in Guide YVL 7.18 and requirements for control room ventilation systems in Guide YVL 5.6.

3.7 Fire protection

According to paragraph 2, section 20 of the Council of State Decision (395/91), *structures, systems and components important to safety shall be designed and located, as well as protected by means of structural fire barriers and adequate fire fighting systems so that the likelihood of fire and explosions is small and their effect on plant safety insignificant.*

Fire protection shall be based on room arrangements and fire compartments in the first place. Each parallel sub-section of the plant systems performing safety functions shall be placed in a separate fire compartment. No other systems or components shall be placed in these rooms which would essentially increase the fire load or the threat of a fire breaking out. These rooms shall be placed sufficiently far from such other systems and rooms as could endanger the operation of the safety systems.

The fire classification of buildings containing systems important for nuclear power plant safety shall be fire-resistant. As far as possible, incombustible and heat-resistant materials shall be used everywhere at the plant, particularly in the containment and the control room.

The fire protection systems shall be so designed that their breaking or inadvertent operation does not significantly reduce the capability of structures, systems and components important to safety to carry out their safety functions.

If a fire in some fire compartment may cause a significant release of radioactive substances into the plant rooms or to the environment, fire detection and extinguishing within the compartment shall be ensured by fire protection systems capable of performing their functions even in the event of a single failure.

In Guide YVL 4.3, detailed requirements for fire protection at nuclear power plants are presented.

3.8 Fuel handling and treatment systems

The nuclear power plant shall have sufficient rooms and systems for the safe handling, treatment, storage and inspection of fresh and spent fuel.

Fuel criticality shall be prevented primarily by the use of appropriate storage structures. Appropriate technical and administrative arrangements shall be made during fuel storage or transfer to prevent fuel damage.

There shall be so much storage space for spent fuel at the plant site that all fuel assemblies in the reactor can be transferred to the storage pools and that fuel in any storage pool can be transferred to other storage pools.

Spent fuel cooling must be possible even in the event of a single failure.

Detailed requirements for the storage, handling and treatment of fresh and spent fuel are presented in Guide YVL 6.8.

3.9 Safety classification

According to section 21 of the Council of State Decision (395/91), *the functions important to the safety of the systems, structures and components of a nuclear power plant shall be defined and the systems, structures and components shall be classified according to their safety significance.*

The systems, structures and components important to safety shall be designed, manufactured, installed and operated so that their quality level and the inspections and tests required to verify their quality level are adequate considering any item's safety significance.

Detailed requirements for safety classification are presented in Guide YVL 2.1.

3.10 Provision made for inspections, testing and maintenance

The nuclear power plant's systems, structures and components shall perform reliably. To ensure this, it must be possible to service, inspect and test plant systems, structures and components over the entire design service life of the plant.

3.11 Shared systems, structures and components

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

If cross-connections are designed between systems of different nuclear power plant units performing the same safety function, it shall be demonstrated that these make the safety functions more reliable than they would be without the connections.

3.12 Environmental conditions

All nuclear power plant structures, systems and components shall be so designed that they perform reliably under design-basis environmental conditions. During design, it shall be defined under what environmental conditions the structure, system or component shall be capable of operating. The operability of a structure, system or component under the environmental conditions in question shall be demonstrated by the necessary tests and analyses.

Requirements for the environmental qualification of electrical and instrumentation components are presented in Guide YVL 5.5 and the environmental qualification of other structures and components is prescribed in YVL Guides which apply to these structures and components.

3.13 Human errors

According to section 19 of the Council of State Decision (395/91), *special attention shall be paid to the avoidance, detection and repair of human errors. The possibility of human errors shall be taken into account both in the design of the nuclear power plant and in the planning of its operation so that the plant withstands well errors and deviations from planned operational actions.*

The avoidance of human error shall be specifically taken into account in control room design and when planning control room activities. The planning of control room activities shall be based on sufficient procedural and task analyses.

To avoid maintenance errors, attention shall be paid to the physical work environment and component accessibility. A clear marking system shall be planned to identify components. Safety-related operator and maintenance staff operations shall be task-analysed to plan the necessary actions to avoid or reliably detect human error.

In failure analyses required in Guide YVL 2.7, human error shall be considered and it shall be demonstrated that individual errors do not prevent safety functions. The possibility of multiple human error shall be assessed in the plant probability safety assessment (PSA) and the necessary measures to avoid or reliably detect errors shall be planned.

3.14 External events

According to paragraph one, section 20 of the Council of State Decision (395/91), *the most important nuclear power plant safety functions shall remain operable in spite of any natural phenomena estimated possible on site or other events external to the plant. In addition, the combined effects of accident conditions induced by internal causes and simultaneous natural phenomena shall be taken into account to the extent estimated possible.*

Natural phenomena include at least freezing which hinders the operation of the final heat sink or blockage due to some other reason, thunderstorm, earthquake, storm wind, flooding, exceptionally cold or warm weather, exceptionally hard rain or drought and exceptionally low sea level. Other events external to the plant are at least electromagnetic disturbances, oil leaks, crashing aeroplanes, explosions, releases of poisonous gases and unauthorised plant site entry.

Guide YVL 2.6 deals with how earthquakes are taken into account in nuclear power plant design.

3.15 Ageing of components and materials

In nuclear power plant design, the service life and the effect of their ageing on the safety of all safety significant structures, components and materials shall be assessed using sufficient safety margins. Furthermore, provision shall be made for the surveillance of their ageing and, if necessary, their replacement or repair.

4 Definitions

Operational conditions

Operational conditions mean a nuclear power plant's normal operational conditions and anticipated operational transients.

Final heat sink

The final heat sink means the atmosphere, the ground and also surface water and groundwater to which heat from various sources is transferred during operational conditions and accidents.

Normal operational conditions

Normal operational conditions mean the nuclear power plant is operated according to the Technical Specifications and operational procedures. These also include tests, plant start-up and shutdown, maintenance and refuelling.

Anticipated operational transients

An anticipated operational transient means such a deviation from normal operational conditions as is milder than an accident and which may be expected to occur once or several times over a period of a hundred operating years.

Accident

An accident means such a deviation from normal operational conditions as is not an anticipated operational transient. There are two classes of accident: postulated accidents and severe accidents.

Postulated accident

A postulated accident means such a nuclear power plant safety system design-basis event as the nuclear power plant is required to manage without any serious damage to the fuel, and discharges of radioactive substances

so large that in the plant's vicinity, extensive measures should be taken to limit the radiation exposure of the population.

Fuel design limits

Fuel design limits mean the limits to prevent fuel failures during operational conditions and to ensure fuel coolability in postulated accidents.

Primary circuit

The primary circuit means pressure-retaining components of the reactor cooling water system, such as pressure vessels, piping, pumps and valves or other components connecting to the reactor cooling water system. The boundaries of the primary circuit are defined in Guide YVL 2.1.

Structures, systems and components important to safety

Structures, systems and components important to safety are such that
— their malfunction or breakage can significantly increase the radiation exposure of the plant's workers or the environment
— they prevent the occurrence and propagation of transients and accidents
— they shall mitigate the consequences of accidents.

Safety system

A safety system is a system which carries out a certain safety function.

Safety functions

Safety functions are safety-significant functions to prevent the occurrence or propagation of transients and accidents or to mitigate the consequences of accidents.

Severe accident

A severe accident means an event during which a significant part of the fuel in the reactor sustains damage.

Single failure

A single failure means a random failure and its consequent effects which are assumed to occur either during a normal operational condition or in addition to the initial event and its consequent effects. More detailed instructions concerning single failures are given in Guide YVL 2.7.