Säteilyturvakeskus
Finnish Centre for Radiation and Nuclear Safety

YVL-ohje
YVL Guide

YVL 1.0

1 Dec. 1982 1 (34)

Revised translation 15 Aug. 1984

SAFETY CRITERIA FOR DESIGN OF NUCLEAR POWER PLANTS

TABLE OF CONTENTS

Helsinki 1984
Government Printing Centre

ISBN 951-46-8283-1
ISSN 0781-4321

PL-P.O.BOX 268
SF-00101 HELSINKI
FINLAND

Ydinturvallisuusosasto
Department of Nuclear Safety
Kalevankatu 44

Puh.-Tel.
(90) 616 71

Telex
122691 STUK-SF

STUK 41.01 1985 – 05

8085035600 – 12/6345/PTP

1 INTRODUCTION

This document contains the general safety criteria for the design of the structures, systems and components of a nuclear power plant equipped with a light water reactor. The objective of these criteria is to minimize the radiation exposure of the plant personnel and of the public living in the surroundings of the nuclear power plant. For this purpose, design shall be aimed at preventing incidents which could jeopardize safety and at mitigating their consequences. These incidents can include the following:

- those connected with the site of the nuclear power plant and its environment
- those caused by intentional or unintentional human actions, or
- those originating in an operational occurrence at the nuclear power plant.

To reach the above-mentioned objectives

- the design, construction and operation of a nuclear power plant with its structures, systems and components shall fulfil high quality requirements,
- the safety functions of the plant shall be performed reliably in disturbance and accident conditions; the most important of these functions are reactor shutdown, reactor core cooling and removal of residual heat,
- the plant shall be equipped with multiple barriers (fuel cladding, primary circuit and containment systems) for preventing the release of radioactive materials to the environment.

In the design of a nuclear power plant, attention shall be paid to requirements and limitations needed for assuring the safe operation of the plant. They include

- limitations concerning important operating parameters,
- operating requirements for systems important to safety and
- requirements concerning maintenance, testing and inspections, whereby it is assured that structures, systems and components operate reliably and as planned.

The Technical Specifications, to be followed when operating a nuclear power plant, will be drawn up on the basis of these requirements and limitations.

The fulfilment of the general safety criteria for design of a nuclear power plant is evaluated in the course of the design and construction of the plant. This means that these safety criteria are not applied to those nuclear power plants that have been constructed prior to the publication of this guide, but the modifications that may be needed in them will be considered case by case.

The Institute of Radiation Protection will give more detailed guides concerning the application of these design criteria.

2 GENERAL REQUIREMENTS

2.1 Radiation Protection

A nuclear power plant shall be designed so that the radiation exposure of the public and of the plant personnel is kept as low as reasonably achievable, taking into account the social and the economic factors, and so that the given radiation dose limits are not exceeded. For this purpose,

the following points shall be given consideration in the design, including maintenance, inspections, operation and accident conditions

- design, shielding, and location of systems and components containing radioactive materials,
- design of the plant spaces and passages,
- radiation control inside the plant,
- handling and cleanup of gases and liquids containing radioactive materials, as well as handling and storage of radioactive waste,
- control of releases of radioactive materials to the environment, and
- radiation monitoring in the environment.

2.2 Effects of External Events

Structures, systems and components important to safety shall be designed so that the reactor can be shut down, the primary circuit can be cooled down, residual heat can be removed, and radiation exposure of the plant personnel and releases of radioactive materials to the environment can be kept at an acceptable level, in spite of natural phenomena (e.g. earthquake, storm, flood, freezing) considered possible at the plant site on the basis of historical records, or incidents (e.g. airplane crashes, explosions, effects of poisonous gases) caused by external activities. The design shall also reflect the combinations of the effects of normal and accident conditions with the effects of the natural phenomena, as considered possible.

2.3 Physical Protection

A nuclear power plant shall be designed so that access to the plant and passages inside the plant as well as transfer of materials can be controlled. A nuclear power plant shall be separated from the surroundings in such a way that also entry to the plant site and movement there can be controlled. The aim of physical protection is to prevent activities causing damage to the plant as well as unauthorized occupation of the plant and theft of the nuclear materials.

Physical protection has to be based on the use of safety zones located one within the other, so that structures, systems and components important to safety are within the most protected area.

To implement the controls, there shall be a special control centre at the plant.

2.4 Quality Assurance

All safety functions of the structures, systems and components of a nuclear power plant shall be defined, and structures, systems and components shall be classified on the basis of their inportance to safety.

Structures, systems and components important to safety shall be designed, manufactured and installed so that their quality level and the inspections and tests needed for verifying the quality level are commensurate with the importance of the safety functions to be performed.

The requirements concerning the design, manufacture, installation, inspection, testing, operation and maintenance shall be defined on the basis of the importance of the safety functions to be performed. The instructions and technical standards to be used have to be identified and

their applicability and adequacy have to be evaluated. They shall be revised, supplemented or modified as necessary to assure the fulfilment of the safety requirements.

In order to make sure that structures, systems and components important to safety meet the requirements set for them, a quality assurance program shall be established in the organizations whose activities have a direct influence on the quality. The structure, responsibility and authority of these organizations shall be in accordance with the requirements set for their activities.

Adequate records shall be compiled on the quality control, inspections and tests. The documents and records on the basis of which the quality and the reliability are assessed, and which are associated with the design, manufacture, installation, testing, inspection, operation, and maintenance of the structures, systems and components important to safety, shall be in the possession of the nuclear power plant user.

2.5 Provisions for Inspection, Testing and Maintenance

In order to assure the reliability of structures, systems and components important to safety, their structure, location and operating conditions shall be such that they can be tested, inspected and maintained prior to their commissioning and thereafter periodically during their entire operating life. If structures, systems and components important to safety cannot be tested and inspected to an adequate extent during their operation, in order to detect possible failures, the reliability shall be assured by other means, or the possibly greater failure probability of the objects shall be taken into account in the design.

2.6 Sharing of Structures, Systems and Components

Structures, systems and components important to safety

shall not be shared among nuclear power plant units, unless it can be shown that this does not significantly reduce the ability of these structures, systems and components to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cool-down of the remaining units.

2.7 Tightness and Leak Detection

Structures, systems and components important to the safety of a nuclear power plant shall be designed to meet adequate tightness requirements and they shall be equipped with suitable means for leak detection and isolation.

2.8 Heat Transfer to Ultimate Heat Sink

The plant shall be equipped with systems which transfer the heat from structures, systems and components important to safety to an ultimate heat sink in operational states and under postulated accident conditions.

The design shall assure that the safety function of the systems can be accomplished also in case of a single failure by using either one of the electric power supply systems, the onsite or the offsite, and when any one of the components affecting the safety function is simultaneously inoperable, for instance, due to repair or maintenance.

2.9 Effects of Plant Internal Events and Conditions

Structures, systems and components important to safety shall be designed to withstand the effects of the environmental conditions associated with operational states and postulated accident conditions. These structures, systems and components shall be protected against the dynamic effects of missiles, pipewhipping and discharging fluids that may result from equipment failures.

2.10 Fire Protection

Structures, systems and components important to safety shall be designed and located, as well as protected with fire resistant structures and with adequate active fire protection systems, so as to minimize the probability and effects of fires and explosions. The sustaining of safety functions during and after a fire shall be assured irrespective of the operation of the active fire protection systems.

Noncombustible and heat resistant materials shall be used, wherever practical throughout the plant, particularly in the containment and in the control room.

Fire fighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the capability of structures, systems and components important to safety to perform their safety functions.

If a fire within some fire zone outside the control room can block the control of a safety function from the control room or causes a significant release of radioactive materials into the plant spaces or to the environment, the suppression of the fire shall be assured with fire protection systems that can function also in the case of a single failure.

2.11 Precautions against Emergency Situations

A nuclear power plant shall be designed so that all functions required to cope with an emergency situation can be performed at the plant site. The plant shall have properly equipped facilities for the direction and control of emergency activities. In addition, the plant shall be equipped with sufficient alarm and communication systems for warning and instructing the personnel as well as for external con-

tacts. To facilitate coping with emergency situations, the plant shall have appropriately marked and illuminated passages.

2.12 Decommissioning

Decommissioning of the plant shall be taken into account in the design so that decommissioning and removal of contaminated or activated plant parts can be carried out in such a manner that the radiation exposure of the personnel and radioactive releases to the environment can be kept at an acceptable level.

3 REACTOR

3.1 Reactor Design

The reactor core and associated coolant, reactivity control and protection systems shall be designed with appropriate safety margins to assure that the design limits of the fuel are not exceeded in normal operation or in anticipated operational occurrences.

The reactor core and associated coolant systems shall be designed so that, in the power operating range, the net effect of the prompt inherent nuclear feedback characteristics will reduce a rapid increase in reactivity.

The reactor core and associated coolant, reactivity control and protection systems shall be designed to assure that eventual power oscillations can be detected and suppressed before they result in conditions exceeding design limits of fuel.

The internals of the reactor pressure vessel shall be designed and mounted in such a way that they withstand the loadings expected in the operational states and under

postulated accident conditions to the extent necessary to ensure reactor shutdown and core cooling.

3.2 Reactor Shutdown and Reactivity Control

The reactor shall be equipped with two independent reactivity control systems, functioning according to different design principles, to assure reactor shutdown in operational states and under postulated accident conditions.

One of the systems shall use control rods which shall be capable of reliably performing the reactor shutdown to assure that design limits of fuel are not exceeded in normal operation or in anticipated operational occurrences.

At least one of the systems shall, on its own, be capable of rendering the reactor subcritical from any normal operational state and maintaining it subcritical in all reactor temperatures.

The reactivity control systems, together with the reactor protection system, shall be designed to assure that no single reactivity control system malfunction, such as withdrawal of control rods from the core (not ejection or dropout), does not result in exceeding the design limits of fuel.

The reactivity control systems shall be designed to have a capability, in conjunction with poison addition by systems designed to cope with loss of coolant situations, of reliably controlling reactivity to assure that the effects of postulated accident conditions cannot cause:

- exceeding the design limits associated with the fuel coolability,
- damages in the reactor pressure vessel internals to such an extent as to significantly impair the capability

to cool the core, or

- exceeding the design conditions of the reactor primary circuit.

Under postulated accident conditions caused by malfunctions within the reactivity control systems themselves, the amount and the rate of reactivity increase shall remain within appropriate limits.

The design of each reactivity control system shall assure that the system safety function can be accomplished also in case of a single failure, when additionally one control rod is stuck, by using either one of the electric power supply systems, the onsite or the offsite.

3.3 Fuel Design

The design objectives are to achieve a low probability of fuel failures in normal operation and in anticipated operational occurrences and to make sure that the coolability of the fuel is maintained under postulated accident conditions. In order to take these objectives properly into account in fuel and plant design, the fuel design limits with sufficient safety margins shall be defined.

Fuel bundles shall be designed to permit adequate periodic inspections of their structure and parts.

4 REACTOR COOLANT SYSTEM

4.1 General Requirements

The reactor coolant system and associated auxiliary, control and protection systems shall be designed with sufficient safety margins in order to assure that the design conditions of the reactor primary circuit are not exceeded in normal operation or in anticipated operational occurrences.

The reactor coolant system shall be equipped with a coolant cleanup system which is capable of extracting radioactive materials from the coolant efficiently enough in normal operation and in anticipated operational occurrences.

The reactor coolant system shall be equipped with water make-up and let-down systems, which are capable of keeping the quantity of coolant within the planned limits during normal operation and which can compensate for minor coolant leakages so that the reactor core can be cooled in a normal way.

In the reactor coolant system design, the possibility of a reactor coolant leakage shall be considered. With suitable arrangements it shall be made sure, that reactor coolant leakages can be detected rapidly and located as accurately as necessary for corrective operational measures.

4.2 Primary Circuit

In the design, manufacturing, installation, inspection and testing of the reactor primary circuit, the means provided by the present state of science and technology shall be efficiently utilized for prevention of a fast growing fracture or some other serious damage.

Primary circuit components shall be designed to withstand loads and conditions in accordance with the design values. In addition, the temperatures and other conditions prevailing in operational states and under anticipated accident conditions shall be taken into account.

There shall be an adequate margin for brittle behavior of structucal materials in all operational states and anticipated accident conditions. Also uncertainty factors shall be observed when determining properties of structural

materials, irradiation of materials, effects of irradiation on material properties, stresses, and size of flaws.

The primary circuit and its components shall fulfil high quality requirements.

The primary circuit and its components shall be designed so that it is possible

- to inspect and test periodically all important sections and details in order to estimate their structural and leaktight integrity, and

- to implement a material surveillance program for the reactor pressure vessel in order to determine the effects of irradiation and the ageing of structural materials.

4.3 Replenishment of the Coolant and Emergency Core Cooling

For loss-of-coolant situations, the plant shall be equipped with systems which replenish the lost coolant or by some other means secure an efficient cooling of the core, so that the design limits associated with the fuel coolability are not exceeded.

The design shall assure that the safety function of the systems can be accomplished also in case of a single failure by using either one of the electric power supply systems, the onsite or the offsite, and when any one of the components affecting the safety function is simultaneously inoperable, for instance, due to repair or maintenance.

4.4 Cooldown of Primary Circuit and Removal of Residual Heat

The plant shall be equipped with systems that can cool down the primary circuit and with systems that can remove the residual heat in all operational states and anticipated accident conditions.

The design shall assure that the safety function of the systems can be accomplished also in case of a single failure by using either one of the electric power supply systems, the onsite or the offsite, and when any one of the components affecting the safety function is simultaneously inoperable, for instance, due to repair or maintenance.

5 PROTECTION SYSTEM

5.1 Purpose of Protection System

The plant shall be equipped with a protection system, the purpose of which is

- to initiate automatically the operation of appropriate systems to assure that the design limits of the fuel or design conditions of the primary circuit are not exceeded as a result of anticipated operational occurrences,
- to detect accident conditions and to initiate the operation of systems important to safety, and
- to maintain the plant in a safe state in postulated accident conditions long enough to provide the operators with the time which is needed for diagnosis, choosing the appro priate measures and taking the actions.

5.2 Protection System Reliability and Testability

The protection system shall be designed for high function reliability and so that it can be tested or surveyed during normal operation. The designed redundancy and independence of the protection system shall be adequate to assure that

- a single failure does not result in the loss of a protection function, even if some part or channel is simultaneously inoperable due to repair or maintenance, and

- the effects of natural phenomena, operational states and postulated accident conditions do not result in the loss of a protection function.

Otherwise, the protection system shall be demonstrated to be acceptable on some separately defined basis.

Whenever practical, at least two different process parameters shall be monitored for each protection function. They shall both be physically dependent on operational occurrences or accident conditions and it shall be possible to choose their trip limits so that the trip occurs early enough. Otherwise, the protection system shall be demonstrated to be acceptable on some separately defined basis.

The protection system shall be designed to take the state that provides greater safety if some section of the protection system is disconnected, the energy supply is lost (e.g. electric power, instrument air) or postulated adverse environmental conditions are experienced.

The protection system shall be designed so that manual control from the control room or the function of the control system cannot prevent or stop a safety function initiated by the protection system, before the function has been accomplished (short-term actions, e.g. reactor scram or containment isolation) or before the process parameter that has activated the function has returned from the range demanding protection (long-term functions, e.g. emergency cooling).

5.3 Separation of Protection and Control Systems

Whenever practical, the protection system shall be separated from control systems. Otherwise, it shall be ensured that when an individual part or channel of the control system fails, or a part or channel of the protection system

which is common to the control and protection systems fails or is removed from service, there remains a system that fulfils all reliability, redundancy and independence requirements set for the protection system. Interconnection of the protection and control systems shall not impair safety.

6 INSTRUMENTATION AND CONTROL

6.1 General Requirements

The plant shall be provided with sufficient instrumentation to monitor operational parameters and systems in operational states and under accident conditions. Special attention shall be paid to those operational parameters and systems that can affect the fission process, core cooling, and residual heat removal as well as the integrity of fuel, primary circuit or containment. In order to keep the operational parameters and systems within prescribed operating ranges, the plant shall be equipped with suitable control devices.

By using the instrumentation, it shall be possible to record the operational parameters describing the condition of the plant and the control signals given to the systems, so that the progress of an operational occurrence or an accident can be followed during the event and the event can be analysed afterwards.

By using the instrumentation, it shall be possible to measure the operational parameters that are important to the safety of the plant. The measurement range shall cover the whole area where the measured parameter can vary in operational states and under accident conditions. To reach a sufficient accuracy, several measuring systems operating in superposed or sequential measuring ranges shall be used, if needed.

Measuring instruments that are important to safety shall be designed so that the instrument failure or the measured parameter being outside the measuring range is revealed by appropriate display or in some other reliable way.

The design shall take into account the environmental conditions in which the instrumentation is meant to function.

The instrumentation important to safety shall be designed to permit periodic testing of its appropriate operation. If testing of some instrument is not possible under some normal operating conditions or if the operation of the instrument is particularly important, the appropriate operation shall be assured by using several redundant instruments or some other reliable method.

6.2 Control Room

The plant shall be provided with a control room from which necessary actions can be taken to maintain the nuclear power plant unit in a safe condition in operational states and under postulated accident conditions. However, operational actions for which there is enough time can be planned to be taken outside the control room, provided this does not impair safety.

The control room shall be located and protected so that the effects that may result from equipment failures do not endanger working in the control room. Continuous electric power supply for the control room equipment shall be assured from the onsite electric power sources. Control room ventilation system and radiation protection shall be designed so that also in accident situations the control room is accessible and the radiation exposure of the personnel working there remains within acceptable limits during an accident.

The physical working conditions of the control room shall be appropriate.

Display instruments for functionally interconnected process variables and for control devices affecting these process variables shall be properly grouped.

The control room shall be equipped with devices that at all times give enough information about the operational state and function of the plant. Furthermore, the control room shall be equipped with alarm equipment which indicate deviations from the normal operating condition, and with appropriate, properly assured data collecting, processing and display equipment assisting the operators during operational occurrences and under accident conditions.

At appropriate locations outside the control room there shall be equipment for performing

- a reactor scram; the equipment shall include necessary instrumentation and control devices to maintain the plant in a safe condition during hot shutdown,
- thereafter, cooldown of the reactor into cold shutdown through the use of suitable procedures, and
- cooling of the spent fuel.

These control equipment outside the control room shall be separated from the control equipment in the control room so that no single incident, e.g complete loss of components within one fire zone, can damage the control equipment in such a way that accomplishment of the above-mentioned functions is unachievable.

7 ELECTRIC POWER SYSTEMS

7.1 Electric Power Supply Systems

The plant shall be equipped with both onsite (independent of main generator) and offsite electric power supply systems which assure the function of systems important to safety. Furthermore, the plant shall be equipped with systems which make possible electric power supply from the main generator if the connection to the offsite transmission network is lost. The onsite and the offsite electric power supply systems shall each provide sufficient capacity to assure that

- the reactor can be shut down, the primary circuit cooled down and residual heat removed, as necessary,
- the design limits of the fuel and the design conditions of the primary circuit are not exceeded as a result of anticipated operational occurrences, and
- cooling of the fuel and other essential safety functions as well as the containment integrity are maintained under postulated accident conditions.

The onsite electric power supplies and the onsite electric distribution system shall have sufficient independence, redundancy, and testability to assure that the safety functions they are supporting can be accomplished also in case of a single failure and when any one mechanical or electric component is simultaneously inoperable, for instance, due to repair or maintenance. The onsite electric power supplies shall assure a continuous power supply to the necessary equipment in operational states and under postulated accident conditions.

For power supply from the offsite grid to each redundant section of the onsite electric distribution system, there

shall be two independent and separate grid connections (not necessarily on separate rights of way) designed and located so as to minimize the likelihood of their simultaneous failure in operational states and under postulated accident conditions. Both grid connections shall be designed to be available even with the main generator disconnected from the grid.

In operational states, it shall be possible to place the stand-by grid connection in service soon enough after losing the other connection so that the design limits of the fuel and the design conditions of the primary circuit are not exceeded, regardless of the function of the onsite a.c. power supply sources.

Under postulated accident conditions, it shall be possible to establish one grid connection so rapidly that the core is cooled and containment integrity can be maintained.

It shall be assured that losing of the remaining power sources as a result of, or coincident with, the loss of one power supply is most unlikely.

8 CONTAINMENT SYSTEM

8.1 Purpose of Containment

To keep the releases of radioactive materials to the environment within acceptable limits in accident conditions, the plant shall be provided with a reactor containment. The containment and associated systems shall form a practically leak tight barrier against the release of radioactive materials to the environment.

8.2 Design Principles of Containment

The reactor containment and associated systems shall be designed so that the containment structure and its internal

compartments can accommodate, with a sufficient safety margin and without exceeding the design leakage rate, the pressure and temperature conditions resulting from postulated accident conditions as well as the reaction forces and missile impacts estimated to be possible under these conditions.

Under accident conditions leading to core meltdown, the containment shall maintain its integrity until the major part of iodines and radioactive aerosols released in the core meltdown has departed from the containment atmosphere and the population in the surroundings of the plant has had enough time to get prepared for possible releases of radioactive materials. Containment damage due to dynamic loads (missiles, explosions) shall be most unlikely. Accommodation of pressure loads shall be ensured for a sufficiently long period of time also in case the systems that are designed for heat transfer from the containment have lost power supply. The formation of gas and vapour caused by the molten core penetrating the basemat of the containment shall be taken into account, and the basemat shall be designed such that it resists the penetration of the molten core.

The primary containment building shall be entirely surrounded with a secondary containment building so that under all postulated accident conditions the space between the two buildings can be kept in underpressure compared with the outside atmosphere. Exhaust air from the space between the buildings shall automatically be transferred to flow through filters under accident conditions. The design of the underpressure system shall assure that the safety function of the system can be accomplished also in case of a single failure by using either one of the electric power supply systems, the onsite or the offsite. Deviations from the above principles can be allowed if it can be demonstrated that some other containment design is safe enough.

8.3 Containment Penetrations and Access Openings

The pipe and cable penetrations of the containment shall be designed according to the containment design requirements. The reaction forces stemming from pipe movement as well as loads possibly occurring under postulated accident conditions, such as thermal loads, jet forces, pipe-whips and missile impacts, shall be taken into account in the design of penetrations. Piping systems penetrating the containment shall be provided with leak detection and isolation capabilities having redundancy, reliability and performance capabilities which reflect the importance to safety of isolating each piping system. The piping systems shall be designed with a capability to test periodically the operability of the isolation valves and associated apparatus and to determine valve leakage.

Personnel and equipment access to the containment shall be through airlocks. Their design shall assure that at least one of the doors is closed during operation.

8.4 Containment Isolation Valves

Each pipeline that is part of the reactor primary circuit or connects directly to the containment atmosphere and penetrates the containment shall be provided with two independent, reliably functioning isolation valves. Each isolation valve shall either function automatically or shall be locked closed. One of the isolation valves shall be placed inside and the other outside the containment. The design shall assure the containment isolation also in case of a single failure.

Each pipeline that penetrates the containment and is neither part of the primary circuit nor connected directly to the containment atmosphere shall have at least one isolation valve outside the containment. The isolation valve shall be either automatic, or locked closed, or

capable of remote manual operation.

The isolation valves outside the containment shall be located as close to the containment as practical. The position of the isolation valves shall be indicated in the control room. A check valve may not be used as an isolation valve outside the containment.

Deviations from the above requirements can be allowed if it can be demonstrated that some other method of isolation is acceptable and that the application of the requirements is unfavorable to safety functions.

8.5 Provisions for Containment Inspection and Testing

The reactor containment and the equipment which can be subjected to testing conditions of the containment shall be designed in such a way that, prior to commissioning of the plant, it is possible to perform a leak test at design pressure and a pressure test at a pressure which is the design pressure added with a sufficient safety margin.

Additionally, the containment shall be designed so that it is possible:

- to perform periodically a leak test at such a pressure that it is possible to determine the leakage corresponding to design pressure with sufficient accurary,
- to perform a pressure test, if necessary,
- to inspect periodically the points that are important to leaktightness and strength
- to survey the condition of the containment during operation, and

- to test periodically the leaktightness of penetrations which have resilient seals or expansions bellows.

8.6 Heat Removal from Containment

The plant shall be provided with systems which remove heat from the containment in operational states and under postulated accident conditions. The system safety function is to reduce the containment pressure and temperature and to maintain them at acceptably low levels.

The heat removal systems of the containment shall be designed so that their inadvertent operation does not endanger the integrity of the containment. Additionally, the effect of the systems on the progress of accident situations leading to core melt shall be considered and it shall be noted that the operation of the systems may increase the risk of containment failure.

The design shall assure that the safety function of the system can be accomplished also in case of a single failure by using either one of the electric power supply systems, the offsite or the onsite, and when any one of the components affecting safety function is simultaneously inoperable, for instance, due to repair or maintenance.

8.7 Gas Treatment in Containment

The containment shall be provided with systems which remove fission products from the containment atmosphere, and with systems which can reduce the concentration of oxygen or of the combustible gases which may be released into the containment in an accident situation, or in some other way prevent uncontrolled gas fires.

The systems intended for controlling oxygen and combustible gases shall be designed in such a way that the integrity of the containment is not endangered due to a gas fire

in accident situations and that components important to safety do not lose their ability to perform their functions. Both the rapid formation of hydrogen in the metal-water reaction caused by the heated reactor core and the formation of hydrogen and other combustible gases when the molten core reacts with the reactor pressure vessel and the basemat of the containment shall be taken into account in the design. It shall be possible to measure the concentrations of oxygen and combustible gases as needed for planned operation of the systems intended for controlling the concentrations.

The design shall assure that the safety function of the systems can be performed also in case of a single failure by using either one of the electric power supply systems, the offsite or the onsite.

9 FUEL HANDLING AND STORAGE

9.1 Fresh Fuel Handling and Storage

The plant shall be equipped with suitable facilities and systems for handling and storage of fresh fuel. Especially the following points shall be taken into account in the design:

1. Criticality shall be prevented with sufficient safety margins, preferably by use of suitable storage structures.

2. Possibility of the fuel dropping or becoming damaged in some other manner shall be extremely small.

3. Suitable facilities and equipment shall be reserved for inspection of received fuel.

9.2 Spent Fuel Handling and Storage

The plant shall be provided with suitable facilities and systems for handling and storage of spent fuel. Especially the following points shall be taken into account in the design:

1. Critically shall be prevented with sufficient safety margins, preferably by use of suitable storage structures.

2. The plant site shall contain enough storage capacity so that the fuel bundles in the reactor can be moved into storage pools, if necessary. Moving of the fuel bundles from any storage pool into other storage pools shall be possible, unless it can be reliably demonstrated that the repair of the pool is possible even when it has not been emptied of spent fuel.

3. Fuel storage facilities shall be equipped with cooling, coolant cleanup and leak collection systems and with systems which control the coolant temperature and level.

4. The possibility of heavy objects dropping on fuel shall be extremely small.

5. The possibility of the fuel dropping or becoming damaged in some other manner shall be extremely small.

6. There shall exist suitable facilities and equipment for periodic inspection of spent fuel and for handling and storage of damaged fuel.

The design shall assure that the safety function of the fuel cooling system can be accomplished also in case of a single failure by using either one of the electric power supply systems, the onsite or the offsite.

10 RADIATION PROTECTION

10.1 Radiation Protection Principles in Plant Design

The plant facilities and passage routes shall be designed such that the external radiation dose rate in them is acceptable and the possibility for internal radiation exposure is small.

Rooms shall be classified on the basis of estimated radiation conditions. The personnel and material traffic inside the plant, the passage restrictions within radiologically controlled area and the necessary passage control arrangements shall be taken into account in the design of rooms.

Systems and components containing radioactive materials shall be designed, located and protected in such a way that the release of radioactive materials to the environment can be kept acceptable and the necessary operational, maintenance, repair and inspection measures can be taken so that the radiation exposure of the personnel remains at an acceptable level.

The availability of the control room and the sufficient maintainability of equipment necessary for keeping the plant safe under accident conditions shall be assured.

Proper facilities and equipment shall be reserved for decontamination of the personnel and equipment and for repair and storage of the radioactive components.

10.2 Radiation Monitoring

Means shall be provided to ensure adequate radiation monitoring at the plant in all operational states and under accident conditions. The plant shall have at least the following radiation measuring instruments:

1. Stationary dose rate meters for external radiation.

2. Instruments for measuring the concentration of radioactive substances in the atmosphere.

3. Instruments for determining the concentration of radioactive materials in the plant fluid systems, and proper laboratory facilities and equipment for measuring the samples.

4. Portable instruments for measuring external radiation dose rate and radioactive surface contamination.

5. Instruments for measuring external contamination of persons.

6. Equipment necessary for personal dose control.

In designing the equipment, provision shall be made for accident situations. It shall be possible to take at least the following measures under accident conditions:

- radiation dose rate measurement in the containment,
- determining the concentration of radioactive materials in the atmosphere of the containment, and
- determining the concentration of radioactive materials in the primary coolant.

10.3 Handling and Storage of Radioactive Wastes

The plant shall be provided with adequate systems for treatment of the radioactive gaseous and liquid effluents in order to restrict releases of radioactive materials.

The plant shall be provided with special facilities and systems for the handling and storage of radioactive wastes.

The plant shall have equipment by the help of which it is possible to determine the radioactive materials and their amounts in the wastes with sufficient accuracy.

10.4 Ventilation

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

- prevent radioactive materials from spreading within the plant,

- reduce the concentrations of airbone radioactive materials within the plant, and

- prevent radioactivity releases to the environment.

The ventilation systems shall be so designed that the concentrations of airbone radioactive materials within the plant remain acceptable in normal operation and in anticipated operational occurrences.

For preventing radioactive materials from spreading within the plant, the pressure differences shall be such that the air flows towards the more active areas.

To restrict radioactive releases, the exhaust air systems shall be provided, if necessary, with proper filtering equipment.

The control room shall be provided with a filtered inlet air system. This system, as well as the other ventilation systems planned to be operated under accident conditions, shall be designed to assure that the safety function of the system can be accomplished also in case of a single failure by using either one of the electric power supply systems, the offsite or the onsite.

10.5 Monitoring Radioactivity Releases

The plant shall be provided with systems for monitoring all discharge paths of planned radioactivity releases as well as with systems for measuring and registering the amounts of radioactive materials to be released to the environment in operational states and under accident conditions.

Provisions shall be made for environmental radiation monitoring in operational states and under accident conditions. The plant shall be provided with meteorological measuring devices with a display unit in the control room.

DEFINITIONS

Accident Conditions

Accident conditions denote substantial deviations from normal operation, including postulated accident conditions and such events that can lead to severe damages of the reactor core, up to and including core melt, or to radioactive releases exceeding the prescribed limits.

Anticipated Operational Occurrences

Anticipated operational occurrences denote such deviations from normal operation that are anticipated to occur one or more times during the operating life of the nuclear power plant, but are not accident conditions.

Design Limits of Fuel

The design limits of fuel denote limits that are meant to prevent fuel failures in operational states and to assure the coolability of the fuel under postulated accident conditions.

Design Conditions

Design conditions denote loads which form the basis for the design of, for instance, a structure or a component. The design values may be different for normal operation, for anticipated operational occurences and for postulated accident conditions.

Loss of Coolant Situations

Loss of coolant situations mean such postulated accident conditions where, due to a leak in the reactor primary circuit, coolant is lost at a rate in excess of the capability of the make-up water system designed for normal operation.

Normal Operation

Normal operation means the operation of the nuclear power plant in accordance with the Technical Specifications and the operating instructions, including testing, shutdown, start-up, maintenance and refuelling.

Operational States

Operational states mean the normal operation of a nuclear power plant as well as anticipated operational occurrences.

Postulated Accident Conditions

Postulated accident conditions mean accident conditions that are used as the design basis of the plant. They may result from such initiating events as:

- a leak in any system containing liquid, steam or gas. The size of the leak may vary between a small leak and a leak caused by the breaking of the largest pipe in the system.

- loss of the onsite or the offsite a.c. power supply sources

- earth fault in any electric station

- ejection or dropout of a control rod

- failure of a trip signal in connection with an anticipated operational occurrence

- failure of any component performing mechanical activities or its malfunction as a consequence of the most severe adjustment error that it credible.

- a sequence of accidents where one of the above-mentioned initiaiing events can with a considerable probability cause other faults.

Primary Circuit

Primary circuit means pressure-bearing parts that are an integral part of or directly connected with the reactor coolant system, such as pressure vessels, piping, pumps and valves.

Safety Functions

Safety functions are functions of systems and components important to safety which are needed to prevent the exceeding of design limits and values or to mitigate the consequences of operational occurrences and accident conditions.

Single Failure

Single failure is a term that is used in the analysis of systems important to safety. Single failure means

a random failure and its consequences which are presumed to occur either in normal operation or after the initiating event of an operational occurrence or a postulated accident condition. More detailed instructions concerning single failures are given in a separate guide published by the Institute of Radiation Protection.

Structures, Systems and Components Important to Safety

Structures, systems and components important to safety are items

- in which malfunction or failure can significantly increase the radiation exposure of the plant personnel or the public,
- which prevent the anticipated operational occurrences from leading to accidents, or
- which are meant to mitigate the consequences of accident conditions.

Ultimate Heat Sink

The ultimate heat sink means the atmosphere, the ground, and the surface and ground waters into which heat is transferred from different sources in normal operation, in anticipated operational occurrences and under postulated accident conditions.

In the event of any differences in interpretation of this guide, the Finnish version shall take precedence over this translation.