Ensuring a nuclear power plant's safety functions in provision for failures

This Guide is in force as of 1 July 1996, until further notice. It replaces Guide YVL 2.7, issued 6 April 1983.

Second, revised edition
Helsinki 1996
Oy Edita Ab
ISBN 951-712-187-3
ISSN 0783-2346

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. Original text in Finnish.

FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY
P.O.BOX 14, FIN-00881 HELSINKI, FINLAND
Tel. +358-9-759882
Fax +358-9-75988382

1 General

The Council of State Decision (395/91) presents general regulations for the safety of nuclear power plants. Guide YVL 1.0 lays down safety principles to be applied in the design of nuclear power plants and which complement the Council of State Decision.

According to the Council of State Decision (395/91), section 18, systems performing the most important safety functions must be able to carry out their functions even though an individual component in any system would fail to operate and any component affecting the safety function would be simultaneously inoperable due to repair or maintenance. These safety functions are dealt with in Guide YVL 1.0.

Section 18 of the Decision also stipulates that to ensure the most important safety functions, systems based on diverse principles of operation shall be used to the extent possible.

To complement the above general design requirements, this Guide gives instructions about the consideration of failures to ensure the safety functions of nuclear power plants. The Guide also presents the principles according to which failure criteria are to be applied to various safety functions, plus the requirements for the performance of failure analyses.

The design of primary and secondary circuit pressure control systems is dealt with in Guide YVL 2.4 and the design of protection systems which actuate safety systems and control their operation, plus the design of electrical systems, are addressed in Guide YVL 5.5.

Guide YVL 2.2 deals with transient and accident analyses to justify technical solutions at nuclear power plants. This Guide also contains requirements specifying what component failures and erroneous operator actions shall be assumed in the analyses.

2 General design principles

According to the Council of State Decision (395/91), section 13, accidents leading to extensive releases of radioactive materials shall be highly unlikely. To satisfy this requirement, the safety functions of the nuclear power plant shall be highly reliable. Design objectives ensuring the reliability of the most important safety functions are given in Guide YVL 2.8.

Both deterministic and probabilistic design principles shall be employed in the design of safety systems. When setting reliability requirements for the safety functions the likelihood of occurrence of the initiating event and the severity of its consequences shall be considered.

General design principles to ensure safety functions are given in section 18 of the Council of State Decision (395/91). From the redundancy principle follows that a safety system comprises at least two redundant sub-systems intended for the same purpose. To ensure the safety functions, the separation principle shall be so implemented that the failure of safety systems which provide back up for each other as well as the failure of redundant parts of the safety systems due to the same external common cause is unlikely.

In some cases, the option of cross-connecting otherwise independent sub-systems by operational action in the event of an abnormal event may be beneficial for system reliability. In such cases, there must be reliable checks to prevent inadvertent cross-connection.

The possibility of component common-cause failures impairs the reliability of a safety function based on the redundancy principle. Therefore, according to the Council of State Decision (385/91), section 18, systems based on diverse principles of operation shall, as far as possible, be used for the most important safety functions.

3 Application of failure criteria to safety functions

3.1 Principles of application

A single failure is a random failure and its consequent effects which are assumed to occur either during normal operation or in addition to an initiating event and its consequences.

In assessing the consequeces of an initiating event and a single failure, the possible interdependence of the system's redundant sub-systems shall be considered. In particular, cross-connections between the sub-systems and connections to systems having no bearing on nuclear safety shall be considered.

In the application of the failure criteria, two failure types shall be analysed, certain exceptions excluded. Both component functional failures i.e. active failures and passive failures which may occur when a system or a component is in the process of carrying out its safety function shall be considered.

A functional failure is a malfunction relating to the changed state of a component or its part. A component functional failure may occur e.g. when the component's functioning requires the mechanical movement of some part. Examples of typical functional failures are given in [2]. The passive failure of a mechanical component or a fluid or gas system may be the loss of component or structural integrity or the clogging up of a flow path.

The inadvertent starting of a component can be ignored as a functional failure if it can be considered highly unlikely e.g. because the component's driving power has been reliably switched off.

There are passive failure types relating to electrical engineering components and systems. When applying the failure criteria to electrical and automation systems or to the instrumentation systems of safety systems, however, no difference is made between functional and passive failures. As prescribed in section 6, both functional and passive failure types shall be examined in the failure analyses performed for these systems.

A design basis passive failure shall be defined by analysing the possible failure and leak modes in such a way that a system's operational conditions are appropriately taken into account. For example, the failure of a pump or a valve sealing, or the rupture of a small-diameter pipe can be defined as the most design basis passive failure if, based on a system's operational conditions plus the design, manufacture and inspection of components and structures, it can be demonstrated that failures worse than these are highly unlikely.

A passive failure can be completely ignored if its probability can be demonstrated as being sufficiently low. In assessing the application of passive failures, even the post-initiating event period during which a component or structure must operate shall be taken into account, and also the impact of the failure on the accomplishment of a safety function and on the plant total risk shall be considered.

A prerequisite for ignoring a passive failure is that a component is designed, manufactured and inspected according to high quality requirements and that an equal quality level is preserved by maintenance during operation. Possible items fulfilling these prerequisites are e.g. buildings, water tanks and support structures of components. The potential non-application of a passive failure as regards the above factors and prerequisites shall be justified in a failure analysis, as prescribed in section 6.

When the failure criteria are applied to systems and components performing safety functions it is assumed that the operability of the systems and components can be periodically tested. The requirements relating

to this testing shall be considered during a system's design. A failure which cannot be reliably observed in periodic tests or inservice inspections and which does not cause an alarm or any other indication in the plant main control room is to be considered a hidden failure. If the possibility of such a hidden failure is detected the primary mode of action is to alter the system's design or testing procedures to facilitate failure detection. If this is impossible, the possibility of a hidden failure shall be considered in failure analyses, as prescribed in section 6.

The operation of auxiliary systems required in the initiation or operation of safety functions is considered to be part of the safety functions and, therefore, their reliability shall be equivalent to that of the safety functions.

When applying the failure criteria to safety functions, deviations from the above application principles are allowed for a specific reason. Any deviations shall be justified in a failure analysis, as prescribed in section 6. For example, the non-meeting of the failure criteria may be well founded in connection with the consequences of highly rare initiating events.

3.2 Rules of application

This section presents how to apply the failure criteria laid down in the Council of State Decision (395/91), section 18, to various safety functions in compliance with the requirements of Guide YVL 1.0.

The reactivity control systems shall be so designed that they both accomplish their safety function even in the event of a single failure.

If only one of the two reactivity control systems is capable of alone maintaining the reactor shut down at all temperatures, it shall also be capable of accomplishing its safety function even in the event of a single failure although any component affecting the safety function would simultaneously be inoperable due to repair or maintenance.

The reactivity control systems shall be so designed that a control system single failure or a single operator error does not bring about a power increase reaching a limit requiring reactor shutdown.

It must be possible to accomplish the removal of reactor residual heat and the transfer of heat to the final heat sink during operational conditions 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.

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

The reactor emergency cooling system shall be able of accomplishing its function even in the event of a single failure although any component affecting the safety function would simultaneously be inoperable due to repair or maintenance.

The accomplishment of containment heat removal shall be possible during 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.

The treatment of combustible gases inside the containment shall be possible during 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.

The cleaning of the containment gas space shall be possible during accidents even in the event of a single failure.

The protection system initiating the safety functions shall operate 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.

The onsite electrical power supply system providing for the safety functions shall be capable of accomplishing its tasks 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.

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

To detect reactor cooling system leaks, a system shall be designed to transmit data about a leak and its size promptly enough even in the event of a single failure and by which the leak can be localised quickly enough.

The reactor coolant volume control shall be so designed that the coolant volume in the primary circuit is maintained within the range required by normal cooling even in the event of a single failure of a component or control system affecting the volume control.

Nuclear power plant systems shall be designed to cool the primary circuit during operational conditions. These systems shall operate even in the event of a single failure.

Containment isolation shall be possible during accidents even in the event of a single failure.

Ventilation and filtering systems which reduce the concentrations of radioactive substances in the plant atmosphere, prevent the spreading of radioactive substances to other plant quarters or restrict the environmental releases of radioactive substances shall be capable of operating at their design power even even in the event of a single failure during operational conditions and postulated accidents.

The inlet air filtering system of the nuclear power plant's control room, air raid shelter and the rooms required for the conduct of operations during accidents shall be capable of accomplishing its safety function even in the event of a single failure during operational conditions and accidents.

The measuring systems intended for accident monitoring and management shall operate even if a single failure occurs.

It shall be possible to monitor radioactive discharges along planned release pathways even in the event of a single failure during operational conditions and accidents.

Systems ensuring containment integrity in connection with a severe accident shall be capable of accomplishing their safety functions even in the event of a single failure.

3.3 Special requirements for fire protection

As the initiating events of anticipated operational transients referred to in sub-section 3.2, also fires confined to a single fire compartment shall be examined. The failure criteria are then applied as such according to sub-section 3.2.

If it can be justifiably demonstrated that a fire confined to a single fire compartment does not bring about an initiating event, the fire and the failure of safety-related systems caused by it are considered a single failure. The failure criteria in sub-section 3.2 are then as such applied to operational conditions.

If a fire breaking out in some fire compartment could cause a significant release of radioactive substances to the plant's rooms or to the environment, fire detection and extinguishing in that compartment shall be ensured by fire protection systems which are capable of accomplishing their functions even in the event of a single failure.

Design requirements concerning fire protection are addressed in more detail in Guide YVL 4.3.

4 The diversity principle

Common-cause failures of components in redundant parts of the safety systems may compromise the reliable operation of a system. Common-cause failures may be due to e.g. deficient component design, testing or maintenance. Also, the ambient conditions of components may bring about common-cause failures.

Attention shall be paid to the avoidance of common-cause failures in the design, operation and maintenance of safety systems. Methods based on quality assurance, component qualification and the separation principle to prevent common-cause failures are given in [2]. The possibility of common-cause failures shall be taken into account, however.

By virtue of the Council of State Decision (395/91), section 18, systems based on diverse principles of operation shall be used to the extent possible to ensure the most important safety functions. The diversity principle shall be observed if high reliability is required of a safety function in Guide YVL 2.8, or if there are specific grounds to suspect that a safety function's reliability could be impaired by common-cause failures.

The assessment of the likelihood of a common-cause failure may be based on operational experience, qualitative analysis of the failure mechanisms of components and the results of probabilistic safety assessment. Below are presented, and to some extent, specified, the safety functions for which, according to Guide YVL 1.0, systems based on the diversity principle shall be used.

Two independent reactivity control systems shall be designed which have different operating principles; each system must be separately capable of shutting down the reactor during operational conditions.

If protective actions based on the active functioning of components are required to prevent a reactivity accident, high reliability and the diversity principle shall be applied to these actions, too.

The diversity principle shall be complied with in the design of the reactor protection system. It is specifically required that the reactor protection system measures at least two different process parameters which are both physically dependent on a transient or accident and whose trip limits can be so chosen that they are reached early enough. If this is not possible for all protection functions, different measurement principles shall be used in the measuring of the process parameter in question.

In the design of residual heat removal from the reactor and heat transfer into the final heat sink the diversity principle shall be applied. In the plant's design, specific provision shall be made for an interruption in the use of the final heat sink normally used.

In the design of the reactor cooling system pressure control, the diversity principle shall be complied with according to Guide YVL 2.4.

The diversity principle shall be complied with in the design of the reactor emergency cooling system.

As far as possible, the diversity principle shall be complied with in the design of control room systems which display the overall plant status and alarm data during transients and accidents.

In the design of the nuclear power plant, the possibility shall be taken into account that the plant's onsite and offsite AC power supply units are simultaneously lost. According to the diversity principle, the plant shall have available a source of AC supply which is independent of the power supply units designed for operational conditions and postulated accidents.

5 Application of failure criteria in compliance with the diversity principle

When the diversity principle required in section 4 is complied with, the failure criteria are applied to safety functions according to sub-section 3.2 but in such a way, however, that any requirement concerning simultaneous maintenance or repair applies to the entire safety function. It is also required that all sub-systems having different operating principles are capable of accomplishing their functions even in the event of a single failure.

A source of independent AC power supply need not meet the failure criteria if electrical systems having bearing on the safety functions fulfil the requirements of sub-section 3.2.

In the application of the failure criteria, only safety-classified systems designed to carry out the functions in question can be taken into account. In the application of the diversity principle, if a system primarily intended for a safety function is alone sufficient to meet the requirements of sub-section 3.2, the other system can be assigned to a lower safety class, but not below class 3, however.

6 Failure analyses

It shall be demonstrated by failure analyses that the failure criteria in section 3 and the related requirements are met and that the safety functions can be accomplished. The failure analyses are conducted as part of the safety assessment of the plant and its systems. Although a probabilistic safety assessment is performed, the requirement of having to perform failure analyses is not removed but such a safety assessment can justify deviations relating to the application of the failure criteria and the consideration of common-cause failures.

The failure types assessed possible for each component shall be examined by analysis until all components having bearing on the safety function have been analysed. In the analysis, one random failure and its consequences are considered at a time. The failure analysis shall cover safety systems associated with the safety functions plus the auxiliary systems they require.

A failure analysis can be performed as follows:

1. The plant's design basis initiating events are defined in connection with which a safety function mentioned in sub-section 3.2 is required to ensure plant safety, and the consequences of these initating events are assessed.

2. Systems and components relating to safety functions are identified which must function faultlessly in connection with every initiating event.

3. Assumptions according to sub-sections 3.1 and 3.2. are made of random failures and of the maintenance and repair of components relating to the safety functions. The consequences of random failures are assessed. The possibility of hidden failures is examined and if these cannot be reliably prevented assumptions are made concerning them. It is demonstrated that a safety function can be accomplished in connection with normal operation or initiating events when these assumptions prevail.

4. The actions of the operating personnel which affect the safety functions are identified and the effect of human error on a safety function is analysed. In a failure analysis, only operator errors in the control room are addressed, such as not performing an action required in the procedures, or erroneous action. Operator errors relating to event identification or decision-making are addressed in a probabilistic safety assessment. A control

error is handled as a single failure. The accomplishment of a safety function shall be demonstrated according to the previous section.

System-specific summaries of the outcome of failure analyses shall be presented in the preliminary and final safety analysis reports and detailed analyses shall be included in the topical reports attached to the safety analysis report.

As regards the common-cause failures and hidden failures of components relating to a safety function, the topical report attached to the safety analysis report shall assess possible failures of this kind relating to each system and shall state how the diversity principle is to be observed to ensure the safety function's reliability.

7 Definitions

An **initiating event** is a single event in the consequence of which the facility deviates from its normal operational state. An initiating event can be an onsite or offsite incident such as a component failure, a natural phenomenon or a hazardous situation due to human action. The definition of initiating events is addressed in App of [1].

The **diversity principle** means the use of redundant systems or components to accomplish the same safety function in such a way that these systems or components have one different feature, such as an operating principle, a manufacturing method or physical parameters.

An **operator error** is a single erroneous action or the omission of an action while an operator attempts to perform a control action relating to a safety function.

A **passive failure** means the loss of integrity of a component or structure or the blockage of the flow path of a process.

A **hidden failure** means an identified failure which does not activate an alarm and which is not detected in tests or inspections performed according to plans.

A **random failure** is a failure whose occurrence is statistically independent of the failure of other components of a similar type. Statistical variations in material, manufacturing method, operating condition, maintenance and testing may cause a component to behave in a manner which deviates from other components of a similar type.

A **functional failure** (also called an active failure) is a malfunction relating to a change in the operating mode of a component or its part. Examples of typical operational failures are given in [2].

A **safety system** is a system performing some of the safety functions mentioned in chapter 3 of this Guide.

A **common-cause failure** means the failure of several components or structures in consequence of the same single event or failure.

A **single failure** is a random failure plus its consequent effects which are assumed to occur during either a normal operational condition or in addition to an initiating event and its consequent effects.

8 References

1 IAEA Safety Series No. 50-C-D (Rev. 1), Code on the Safety of Nuclear Power Plants: Design, 1988

2 IAEA Safety Series No. 50-P-1, Application of the Single Failure Criterion, 1991.

3 IAEA Safety Series No. 50-SG-D1, Safety Functions and Components Classification for BWR, PWR and PTR, 1979.