Translated 24 May 1983

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

FAILURE CRITERIA FOR THE DESIGN OF A LIGHT-WATER REACTOR

1 GENERAL

Guide YVL 1.0 /1/ requires that the systems performing certain safety functions be designed as follows:

The systems shall have a sufficient number of redundant parts and components to ensure that the safety function of the system is accomplished also in case of a single failure. Certain systems shall meet this requirement also when any one component is concurrently inoperable.

The purpose of this quide is to provide complementary and more detailed instructions for the application of general design criteria. The guide is applied to fluid systems, to electricity supply systems, and to mechanical components which are needed for the accomplishment of the safety functions mentioned in section 3.

It is not intended that this guide be applied to protection systems starting and controlling safety systems or to systems used for over-pressure protection. Protection systems are dealt with according to Guide YVL 5.5 and the applicab-

Postadress
P.O. BOX 268
SF-00101 HELSINKI 10
FINLAND
188201754A—22

Telephone
90-61 671
90-544722 (Research Department)

Telex
122691 STL-SF
124956 STLTO-SF

le standards mentioned in it. As concerns over-pressure protection, Guide YVL 2.4 is followed.

2 DEFINITIONS

Active conponent is a component whose function is based on mechanical movement. If the safety functions mentioned in section 3 do not require that the component should move, it need not be regarded as an active component in connection with this function.

Active failure is a malfunction (not a passive failure) in an active component.

Active failures are for example: the failure of a motor-driven valve or a check valve to change its position or the failure of a pump, blower or diesel generator to start.

If a component operated by external power functions spuriously because of a failure in its automatic control, this shall be regarded as an active failure, unless the component is provided with special features or operating limitations meant to prevent this kind of spurious function. An example of spurious function is a situation where a motordriven valve receives a faulty control signal, whereby it can open or close.

Auxiliary systems are systems which help a safety system to perform its intended safety function.

For instance, the auxiliary systems of the emergency core cooling system include systems transferring heat to an ultimate heat sink, the electricity supply system, and a system cooling the pump rooms.

Initiating event is a single event which results in a si-

tuation where the plant or a part of it is no longer in normal operation. The initiating event and its eventual consequences are not a single failure defined in this guide. The initiating event can be a single component failure, a natural phenomenon or an external, man-induced hazard.

Long term is the period of operation of a safety-related system, following the short term, when the safety function of the system is required to take place.

Operator error is a single spurious or omitted action, while the operator tries to perform an operating action relative to a safety function mentioned in section 3 during normal operation, an anticipated operational occurrence or an accident situation.

Passive failure is a loss of the integrity of a component or structure, or a blocking of a process flow path. The blocking of a process flow part can be caused, for example, by the loosening of a valve head from the stem.

Safety system is a system performing a safety function mentioned in section 3 of this guide.

Short term denotes a period of time, up to 12 hours, following an initiating event. However, in the design of the emergency cooling system and the containment spray system of a pressurized water reactor, it is considered that the short term ends when these systems are switched to recirculation through the containment sump.

Single failure is a term that is used in the design and analysis of safety systems and their auxiliary systems.

It means a random failure and its consequences which are assumed to take place either in normal operation or in

addition to the initiating event and its consequences.

Unit is a nuclear reactor and associated components which are necessary for the production of electricity, and structures, systems and components which are needed to make possible the operation of the nuclear reactor without causing undue risk to safety.

3
FAILURE CRITERIA

In normal operation it shall be possible to carry out (1) removal of residual heat, (2) primary circuit cool-down and (3) heat transfer to an ultimate heat sink also in case of a single failure and when whichever active component affecting these safety functions is concurrently inoperable, for instance, due to repair or maintenance.

In normal operation it shall be possible to carry out (1) reactor shutdown (by using whichever of the two independent reactivity control systems) and (2) heat removal from the spent fuel also in case of a single failure.

After an anticipated transient leading to a reactor or turbine trip or after a postulated accident condition, it shall be possible to carry out (1) replenishment of primary coolant and emergency core cooling, (2) removal of residual heat, (3) primary circuit cool-down, (4) heat removal from the containment and (5) heat transfer to an ultimate heat sink also in case of a single failure independent of the initiating event and when whichever active component affecting these safety functions isconcurrently inoperable, for instance, due to repair or maintenance.

After an anticipated transient leading to a reactor or turbine trip or after a postulated accident condition, it shall be posible to carry out (1) reactor shutdown

(by using whichever of the two independent reactivity control systems), (2) isolation of the containment, (3) gas treatment of the containment, (4) filtering of the air to be removed from systems and rooms possibly containing radioactive substances and (5) ventilation of the control room also in case of a single failure independent of the initiating event.

If a fire in some fire zone outside the control room can prevent the accomplishment of a safety function by means of the control equipment in the control room, the suppression of the fire shall be assured with fire protection systems that can function also in case of a single fialure. Here it is no more necessary to assume a failure that is independent of the fire in the safety functions under examination (in case of further failures, the reserve control place and the local controls would still be available, as required in Guide YVL 1.0).

If a fire can cause a significant release of radioacitve substances inside the plant or into the environment, the suppression of the fire shall be assured with fire protection systems that can function also in case of a single failure.

In short-term considerations, the single failures that are taken into account can be limited to active failures.

In long-term considerations, the limiting failure can be either active or passive.

A passive failure that is taken into account in design shall be determined by analyzing the failure mechanisms regarded as posible, so that the operating conditions and potential failure and leak modes are given due consideration. The analysis may result in the definition of the worst failure, for instance, as a seal failure in a pump

or in a valve or as a rupture of a small-diameter pipe, if it can be demonstrated, on the basis of the operating conditions of the system and the proper execution of the design, manufacture and inspections of the components and structures, that there is no real risk of failures worse than that.

The operator errors that may occur during the operation of the plant shall be regarded as active failures.

If there are enough time and means for the detection, investigation and repair of a single failure, the actions of the operating personnel at the unit can be taken into account in performing the single failure analysis required in section 6.

4 EXEMPTIONS FROM THE APPLICATION RULES

If it can be demonstrated that the active function of a component is correct in all credible situations, it is not necessary to assume an active failure in the component. The opening of a check valve of a certain type can serve as an example of such a function. If an exemption of this kind is made, it shall be justified.

A passive failure or a leak exceeding the limit used as a design basis for the containment need not be assumed in the containment or in its penetrations, nor in those sections of the piping penetrating through the containment which are left between the penetration and the isolation valve (including the isolation valves). This exemption is not applied to the emergency core cooling system piping, where a damage would result in a loss of the emergency core coolant during recirculation phase.

The requirements presented in section 3 concern the design

of a unit. If, during the operation of the unit, there should arise a situation where the requirements are not met, actions are taken in accordance with the Technical Specifications approved for use at the unit.

Passive failures causing a limited leak need not be taken into account in the single failure analysis required in section 6 if the unit is designed in such a way that the failure does not result in the loss of the required safety functions.

In making the single failure analysis required in section 6, it is not necessary to assume the initiating event to be a fault in safety systems that are needed in normal operation and that are given consideration in single failure analyses concerning normal operation. For example, it is not necessary to assume that the initiating event be a failure in a residual heat removal pump or in an auxiliary feed water pump during cool-down of the unit or the loss of one line in the intermediate cooling circuit during the power operation of the unit. These failures are dealt with in a single failure analysis where the initial condition is the normal operation of the unit. However, this exemption is not applied to failures which would require the starting of other safety systems. For instance, a pipe rupture in the residual heat removal system resulting in a non-isolable leak of the primary coolant would require the starting of the emergency cooling system, and thus it should be assumed as an initiating event.

In making the single failure analysis required in section 6, it is not necessary to assume the intiating event to be a fault in systems that are not needed in normal operation and whose failure does not cause automatic protective actions.

5
DESIGN REQUIREMENTS

It shall be possible to perform the safety functions mentioned in section 3 by using either one of the power supply systems of the unit, the onsite or the offsite. The onsite power supply and distribution system of the unit shall alone, as part of each safety function mentioned in section 3, meet the failure criteria set for the function.

The systems performing the safety functions mentioned in section 3 shall be designed in such a way that their condition can be controlled through periodic inspections.

The systems performing the safety functions mentioned in section 3 shall be designed in such a way that the operability of their active components can be ascertained through periodic tests.

To provide for events after which it can take a long time before normal operation is restored, e.g. LOCA, it shall be ensured that the components outside the containment are accessible and reparable in case that they fail during the recovery period. The actions to be taken in this respect include: the separation of redundant systems from each other with sufficient radiation shields, the possibility of flushing rooms, the possibility of draining and flushing lines containing radioactive substances in rooms that must be entered, and safe passages to the components. In justified situations it can be assumed that offsite power supply, components classified non-nuclear safety, and additional equipment acquired outside the unit are available.

When planning how to contain radioactive substances inside the unit after an accident, the amount and radioactivity content of the substance released as a consequence of a

single failure shall be estimated conservatively taking into account the releases that have occurred both before and after isolation. The duration of the release shall be determined conservatively, taking into account the potential for detecting, locating and isolating the leak.

6 ANALYSIS REQUIREMENTS

The safety functions mentioned in section 3 shall undergo single failure analyses to demonstrate that the requirements presented in this YVL guide are met. The results of the single failure analyses are presented as part of the preliminary and final safety analysis reports or in topical reports supplementing the safety analysis reports.

A single failure analysis performed for the normal operation of the unit and for each initiating event shall cover, besides the safety systems, all auxiliary systems that they need. It is not necessary to assume concurrent or successive failures in the safety system or in the needed auxiliary systems (except for those that come about as consequences of the initiating event or the assumed single failure). For instance, if it is assumed that a diesel generator has failed while the emergency core cooling system is needed, then there is an active failure. Other failures may result from this failure or initiating event, but besides these, no other failures affecting the emergency core cooling need be taken into account either in short or in long term.

7 REFERENCES

1. YVL 1.0 Safety Criteria for Design of Nuclear Power Plants