

SAFETY STANDARDS
of the
Nuclear Safety Standards Commission (KTA)

KTA 3301
Residual Heat Removal Systems of Light Water Reactors
(November 1984)

Editor:

Geschäftsstelle des Kerntechnischen Ausschusses

beim Bundesamt für Strahlenschutz

Postfach 10 01 49, D-38259 Salzgitter, F.R.G.

Phone +49(0)5341/885-901, Telefax +49(0)5341/885-905

Comment:

In these English translations of KTA-Safety Standards the words shall, should and may are used with the following meanings:

- shall indicates a mandatory requirement,
- should indicates a requirement¹ to which exceptions are allowed. However, the exceptions shall be substantiated during the licensing procedure,
- may indicates a permission and is, thus, neither a requirement (with or without exceptions) nor a recommendation: recommendations are worded as such, e.g., "it is recommended that".

The word combinations basically shall/shall basically are used in the case of mandatory requirements to which specific exceptions (and only those!) are permitted. These exceptions - other than in the case of should - are specified in the text of the safety standard.

¹ Please note that in the case of IAEA NUSS standards and ANSI standards, the word "should" indicates a mere recommendation.

KTA 3301**Residual Heat Removal Systems of Light Water Reactors****Table of Contents**

| | Page |
|--|------|
| Basic Principles..... | 2 |
| 1 Scope..... | 2 |
| 2 Definitions | 2 |
| 3 Intended Uses..... | 3 |
| 3.1 Specified Normal Operation..... | 3 |
| 3.2 Plant-Internal Incidents | 3 |
| 3.3 External Events..... | 3 |
| 3.4 Other Intended Uses..... | 3 |
| 4 Design..... | 4 |
| 4.1 Boundary Conditions of the Heat Sink | 4 |
| 4.2 Residual Heat to be Removed | 4 |
| 4.3 Design of the Components | 5 |
| 4.4 Specification of the Coolant Supply Quantities | 5 |
| 5 System Concept | 5 |
| 5.1 System Function..... | 5 |
| 5.2 Failure Assumptions and Redundancy Requirements | 6 |
| 5.3 Malfunctions Inside the Systems | 7 |
| 5.4 Safe Confinement of the Primary Coolant..... | 7 |
| 6 Arrangement and Construction Measures | 8 |
| 6.1 Specified Normal Operation..... | 8 |
| 6.2 Plant-Internal Incidents..... | 8 |
| 6.3 External Events..... | 9 |
| 6.4 Heat Sink | 9 |
| 7 Operation and Monitoring | 9 |
| 7.1 Specified Normal Operation..... | 9 |
| 7.2 Plant-Internal Incidents | 10 |
| 7.3 External Events..... | 10 |
| 8 Power Supply..... | 10 |
| 8.1 Electrical Power Supply | 10 |
| 8.2 Non-Electrical Power-Supply | 10 |
| 9 Ensuring Functional Capability and Operational Availability | 10 |
| 9.1 Commissioning Tests..... | 10 |
| 9.2 Inservice Inspections | 11 |
| 9.3 Maintenance | 11 |
| 10 Reliability Analyses | 11 |
| 10.1 Objectives | 11 |
| 10.2 Extent..... | 11 |
| 10.3 Site Preparation and Specification of Boundary Conditions | 12 |
| 10.4 Calculation of Reliability Characteristics | 12 |
| 10.5 Evaluation of the Results | 12 |
| Appendix A: List of the Systems within the Scope of this Safety Standard | 13 |
| Appendix B: Regulations Referred to in this Safety Standard | 18 |

PLEASE NOTE:

Only the original German version of this safety standard represents the joint resolution of the 50-member Nuclear Safety standards Commission (Kerntechnischer Ausschuss, KTA). The German version was made public in Bundesanzeiger No. 44a on March 4, 1988. Copies may be ordered through the Carl Heymanns Verlag KG, Gereonstr. 18-32, D-5000 Köln 1.

Nuclear Safety Standards Commission (KTA)

Federal Republic of Germany

Basic Principles

(1) The safety standards of the Nuclear Safety Standards Commission (KTA) have the task of specifying those safety-related requirements which shall be met with regard to precautions to be taken in accordance with the state of science and technology against the damage arising from the construction and operation of the facility Sec. 7 para. 2 no. 3 Atomic Energy Act), in order to attain in particular the protective goals specified in the Atomic Energy Act and the Radiological Protection Ordinance.

(2) This safety standard is based on:

- a) the "Safety Criteria for Nuclear Power Plants" issued by the Federal Minister of the Interior, in particular the criteria
 - aa) for residual heat removal-during specified normal operation (Criterion 4.2),
 - ab) for residual heat removal after losses of coolant (Criterion 4.3), and
 - ac) for heat removal from the containment after loss-of-coolant incidents (Criterion 8.5);
- b) the "Interpretations of the Safety Criteria for Nuclear Power Plants, Single Failure Concept - Principles for the Application of the Single Failure Criterion";
- c) the "Guidelines for the Assessment of the Design of PWR Nuclear Power Plants against Incidents pursuant to Sec. 38 para. 3 of the Radiological Protection Ordinance - Incident Guidelines -";
- d) the "RSK Guidelines" Chapter 22, in as far as this contains system specifications.

(3) The systems provided for residual heat removal in the case of incidents are part of the safety system of the reactor plant. There is a close functional connection between them and the other safety equipment, in particular the reactor protection system and the power supply system. This safety standard is therefore to be considered in connection with the Safety Standards KTA 3501, "Reactor Protection System and Monitoring of Equipment of the Safety System", KTA 37 1. "Basic Requirements for the Electrical Power Supply of the Safety System in Nuclear Power Plants Part 1: Single-Unit Plants" and KTA 3702.1, "Emergency Power Facilities with Diesel Generator Sets in Nuclear Power Plants, Part 1: Design".

1 Scope

(1) This safety standard applies to the residual heat removal systems (hereinafter referred to as "RHR systems") of stationary nuclear power plants with light water reactors (pressurized and boiling water reactors, hereinafter referred to as "PWR" and "BWR"). It contains the safety requirements for:

- a) the Process engineering design,
- b) the assembly and functional safety,
- c) the arrangement,
- d) the operation, and
- e) the monitoring and testing of the systems.

(2) The scope of this safety standard extends to the systems which are necessary, after a reactor shutdown, for residual heat removal (hereinafter referred to as "RHR") from the primary coolant system and, if required, from the containment vessel to a heat sink, in-as far as the operational main heat sink is not used for this purpose. In this context, certain parts of the primary and secondary coolant systems shall be considered as parts of the RHR systems, if their function is required for this purpose.

(3) The requirements in this safety standard shall also apply to those parts of the auxiliary, supply and energy systems, the functions of which are required for RHR purposes.

Note:

The systems within the scope of this safety standard are listed as examples in Appendix A.

The requirements for the primary side and secondary side pressure relief valves are contained in the safety standard KTA 3302 which is in preparation.

(4) Not subject to this safety standard are:

- a) the removal of residual heat from the fuel element storage pool,
- b) the incident assumptions, and
- c) the design calculations and proofs of effectiveness for emergency core cooling.

2 Definitions

(1) Active Component

An active component is a component which is operated or controlled externally and is activated either manually or automatically with the assistance of transfer and driving media (e. g. electrical current, hydraulic or pneumatic systems). A self-acting component (functioning without external power or control) shall be considered as an active component if its position is changed in the course of fulfilling its intended function (e.g. safety valve or check valve).'

(2) Failure

A failure is a component breakdown such that it can no longer fulfill one or more of its design requirements.

(3) Specified Normal Operation

Specified normal operation comprises

- a) operating procedures for which the plant, with its systems in functioning condition (undisturbed condition), has been built and is suited (normal operation),
- b) operating procedures which take place in the case of a malfunction of plant components or systems (disturbed condition), in as far as there are no safety reasons which oppose continued operation in this case (abnormal operation), and
- c) maintenance procedures (inspection, servicing, repairs).

(4) Single Failure

A single failure is a failure which is caused by a single event and includes the subsequent failures resulting from this failure.

Note:

A description of this definition is contained in the "Interpretations of the Safety Criteria for Nuclear Power Plants, Single Failure Concept - Principles for the Application of the Single Failure Criterion".

(5) Operational Availability

Operational availability is the condition of a system or part of a system (e. g. component, subsystem, train), including any necessary auxiliary, supply and energy systems, in which its intended functions can be activated and ensured on demand.

(6) Functional Capability

Functional capability is the suitability of a system, or part of a system (e. g. component, subsystem, train), including any necessary auxiliary, supply and energy systems, to fulfill its intended function.

Note:

With respect to the stress analysis of components, the term "functional capability" is further differentiated in the corresponding safety standards.

(7) Maintenance

Maintenance encompasses all procedures to preserve and restore the required condition and to determine and assess the actual condition. Maintenance is subdivided into inspection, servicing and repairs.

(8) Passive Component

A component is passive if it does not need to be operated in order to function (e. g. pipes, vessels, heat exchangers). A self-acting component (functioning without external power or control) shall be considered as passive if its position is not changed in the course of fulfilling its intended function (e. g. safety valve or check valve).

(9) Redundant

A redundant is a part of a system (e. g. component, subsystem, train) which is equivalent to other parts of the system which fulfill the same functions and which, if needed, can completely replace, or be replaced by, one of these other parts of the system.

(10) Redundancy

Redundancy is the availability of more operational technical means than are necessary for the fulfillment of the intended functions.

(11) Incident

An incident is a sequence of events on the occurrence of which the operation of the plant or the work in progress cannot be continued for reasons of safety and which was taken into account in the design of the plant or for which precautionary protective measures are provided during the work in question.

Note:

For plants in accordance with Sec. 7 of the Atomic Energy Act, "incident" shall be understood to be a sequence of events on the occurrence of which the operation of the plant cannot be continued for reasons of safety and which was taken into account in the design of the plant.

3 Intended Uses**3.1 Specified Normal Operation**

The RHR systems shall be able to cool down the shutdown reactor to a temperature which permits the handling of the fuel elements (after takeover of the shutdown procedure) and maintain the reactor at this temperature during long-term operation.

3.2 Plant-Internal Incidents**3.2.1 Incidents without Loss of Coolant**

In the case of incidents without loss of coolant which lead to a failure of the feedwater supply or of the main heat sink of the plant, the RHR system shall be able to fulfill the following functions, for the respective operational plant and system conditions:

- a) feed the steam generators (PWR),
- b) blow down the steam produced in the steam generator (PWR),
- c) maintain the level in the primary coolant system (BWR),

Note:

In the case of the PWR, the level is maintained by boron injection systems which are not within the scope of this safety standard.

- d) cool down the primary coolant and cool the reactor plant in the cold, subcritical state,
- e) blow-down the steam produced in the primary coolant system via relief valves into the suppression chamber (BWR),

- f) cool the suppression chamber water (BWR),
- g) cool the components required for RHR.

3.2.2 Incidents with Loss of Coolant

(1) The use of the RHR systems shall be based on all the loss-of-coolant incidents to be considered in that area of the primary coolant system which cannot be isolated.

(2) In the case of loss-of-coolant incidents, the RHR systems shall be able to fulfill the following functions for the respective operational, plant and system conditions:

- a) reflood the reactor core and maintain the level in the primary coolant system,
- b) feed back the lost coolant to the primary coolant system via the residual heat exchangers,
- c) cool down the primary coolant and cool the reactor plant in the cold, subcritical state,
- d) feed the steam generators (PWR),
- e) blow down the steam produced in the steam generator (W),
- f) blow down the steam produced in the primary coolant system via relief valves into the suppression chamber (BWR),
- g) cool the suppression chamber water (BWR),
- h) cool the components required for RHR.

3.3 External Events

(1) The following external events shall be considered:

- a) natural events (e.g. earthquake, flooding), and
- b) man-made events (e.g. aircraft crash, pressure wave from chemical reactions).

(2) In the case of external events the systems shall be able to fulfill the following functions for the respective operational, plant and system conditions:

- a) feed the steam generators (PWR),
 - b) blow down the steam produced in the steam generator (PWR),
 - c) maintain the level in the primary coolant system (BWR),
- Note:**
In the case of the PWR, the level is maintained by boron injection systems which are not within the scope of this safety standard.
- d) cool down the primary coolant and cool the reactor plant in the cold, subcritical state,
 - e) blow down the steam produced in the primary coolant system via relief valves into the suppression chamber (BWR),
 - f) cool the suppression chamber water (BWR),
 - g) cool the components required for RHR.

(3) In the case of external events with a very low frequency of occurrence, auxiliary measures may be used.

3.4 Other Intended Uses

The RHR systems may also be put to other intended uses (see Section 5.1.2), such as:

- a) recirculate the primary coolant when starting up nuclear power plants (PWR),
- b) for flooding or draining procedures when handling fuel elements,
- c) cool the suppression chamber for the maintenance of operational availability in the case of incidents (BWR),
- d) cool the fuel element storage pool,

- e) supply cooling locations in operating systems in addition to the RHR function (e. g. cooling the motors of the primary cooling pumps).

4 Design

4.1 Boundary Conditions of the Heat Sink

- (1) The boundary conditions which depend on the site of the plant and the type of heat sink which shall be taken into account.
- (2) In the case of heat discharged into bodies of water (direct cooling) it should be possible to discharge the heat, which must be removed in the case of an incident in order to maintain the plant limit values, at the maximum cooling water intake temperature which was exceeded at the site in question on a total of no more than 28 days over the immediately preceding ten years of observation, or which can be expected on the basis of the temperature forecast in a thermal load schedule. In the case of operational RHR, lower values may be assumed, e.g. the highest average monthly temperature determined over an observation period of several years.
- (3) In addition, the decisive limit values for the main water source shall be complied with, especially for:
 - a) water intake as a function of the water level,
 - b) the maximum heat output to be discharged into the body of water,
 - c) the temperature rise of the cooling water inside the plant,
 - d) the maximum allowable temperature of the cooling water on being redischarged,
 - e) the temperature rise of the main water source at the point where the heated cooling water is redischarged into it,
 - f) the maximum allowable analytical mixed temperature of the body of water after the heat has been discharged.

Note:
Statistical material regarding the temperatures of bodies of water is contained in the thermal load schedules of rivers or should be requested from the water authorities.

- (4) In the case of the discharge of heat into the atmosphere via wet cooling towers used specially for RHR, the fluctuation range of the wet bulb thermometer temperature dependent on the site shall be taken into account. RHR in the case of incidents should be based on the highest daily wet bulb thermometer temperature reached on five days per year, on an average over several years (≥ 10 a). Lower values may be assumed in the case of operational RHR, e.g. the highest daily wet bulb thermometer temperature reached on twenty days per year on an average over several years.

Note:
Statistical material on meteorological data can be requested from the headquarters of the German Weather Service In Offenbach/Main.

- (5) Design calculations using the lowest service cooling water temperature shall be carried out with respect to:
 - a) the stress affecting the strength of materials of the components of the residual heat removal chain,
 - b) the avoidance of ice formation (in the case of wet cooling towers).

4.2 Residual Heat to be Removed

4.2.1 Contributions to Residual Heat

- (1) The following portions of residual heat may exist after the plant has been shut down:

- a) decay heat power from the fuel elements (see section 4.2.2),
 - b) decay heat from activated structural materials and coolants,
 - Note:**
This portion may be neglected in the design of RMR systems since term b) is small compared to a) in the case of light water reactors after the reactor has been shut down.
 - c) stored heat in the primary coolant system, including the secondary side of the steam generators in the case of a PWR, in each case up to the first isolation device outside the containment vessel,
 - d) fission product energy release from delayed neutrons,
 - Note:**
This term exists only briefly after a reactor scram.
 - e) reaction heat from the zirconium-water reaction between the cladding tube material and the coolant,
 - Note:**
This is only significant in the case of loss-of-coolant incidents until the reflooding of the core has been completed.
 - f) portions of residual heat arising from the operation of the RHR systems and their auxiliary and supply systems, including the electrical switch and distribution gear and the instrumentation and control equipment,
 - g) portions of residual heat arising from the operation of emergency power facilities, and
 - h) heat produced by running reactor coolant pumps.
- (2) These portions shall be taken into account in the design of the RHR systems for each intended use in accordance with the following table:

| Intended Uses | Residual Heat Portions | | | | | | | |
|--|--|---|----------------|---|---|---|----------------|----------------|
| | a | b | c | d | e | f | g | h |
| Operational RHR | x | | x | | | x | | x |
| RHR during incidents without loss of coolant or in the case of external events | x | | x ¹ | x | | x | x ² | x ³ |
| RHR in the case of loss-of-coolant incidents | x | | x | x | x | x | x ² | x ³ |
| 1 | Only to be taken into account in the case of a cooldown of the primary coolant system. | | | | | | | |
| 2 | Not applicable if the emergency power case is not taken into account. | | | | | | | |
| 3 | Not applicable if the emergency power case is taken into account or if the reactor coolant pumps are switched off. | | | | | | | |

- (3) If the cooling concept includes other operational cooling locations to be served by the RHR systems, these shall be taken into account (e.g. fuel element storage pool).

4.2.2 Calculation of the Decay Heat Power of the Fuel

- (1) The calculation of the decay heat shall be done in accordance with DIN 25463. A margin of error shall be taken into account here, i.e. in the case of incidents which are assumed to occur during power operation, this margin shall be equal to twice the standard deviation ($2 \times \sigma$), in all other cases the margin shall be once the standard deviation ($1 \times \sigma$). In the case of sequences of events with a very low frequency of occurrence, no margin of error is required.

(2) The irradiation time of the fuel elements shall be considered to be equal to their utilization time during power operation of the nuclear power plant.

(3) For RHR in the case of incidents which are assumed to occur during power operation, the reference power, for the calculation of the decay heat power shall be assumed to be the maximum power that can be achieved during operation. This is determined, by a reliably designed limitation of the reactor power, e.g. a limitation of process variables in accordance with the safety standard KTA 3501, plus instrumentation and calibration errors.

In all other cases, including the case of events with a very low frequency of occurrence, the calculation of the decay heat power may be based on the nominal reactor power.

4.3 Design of the Components

4.3.1 Pumps

(1) The heads and capacities of the pumps which feed the primary or secondary coolant system shall be specified such that when the geodetic heads and the head losses are taken into account the required injection rates are obtained as a function of the reactor, steam generator and containment vessel pressures.

(2) When determining the net positive suction head of the plant in accordance with DIN 24260, the calculated fluid temperature which can be obtained from the pressure buildup calculations for the containment vessel shall be used for pumps which take suction from the containment vessel in the case of a loss-of-coolant incident. The pressure increase in the containment vessel as a result of the incident shall not be taken into account when calculating the net positive suction head.

4.3.2 Accumulators (PWR)

Total volume coolant inventory and pressure level of the accumulators shall be specified in accordance with the design calculation data for emergency core cooling (see Section 4.4).

4.3.3 Heat Exchangers

The heat exchangers in the RHR systems shall be designed for the maximum heat power required in the case of incidents taking into account the fluid temperatures and pressures. This design shall be verified against the requirements for the intended uses during specified normal operation.

4.3.4 Safety and Relief Valves for the Primary and Secondary Coolant Systems

Response and blow-down pressures, opening and closing behavior, discharge capacity and state of aggregation of the medium to be removed as well as the physical conditions on the discharge side shall be derived from incident analyses.

4.4 Specification of the Coolant Supply Quantities

4.4.1 Pressurized Water Reactor (PWR)

(1) The coolant supply quantities required for the primary and secondary side injection shall be specified taking into account the failure assumptions and redundancy requirements specified in Section 5.2. The following requirements shall be taken into account:

- a) Specified normal operation:
Reflooding of reactor compartment and intermediate storage pool for refuelling purposes.

b) Incidents with loss of coolant:

- ba) Heat removal for the energy released in the primary circuit,
bb) RHR in the case of small leaks. Safe transfer from the secondary side to the primary side heat removal shall be possible.

c) External events:

The coolant supply quantities required for feeding into the steam generator are determined by the concept of plant protection against external events in particular by the type of supply protection and the possibility of supplementing them as well as by the intervention possibilities available to the personnel. Auxiliary measures may be used.

Note:

In accordance with Sec. 22.2 (1) of the RSK Guidelines for Pressurized Water Reactors, it shall be ensured that in the case of the inability of the control room to function, the plant will be transferred to a safe condition with the aid of the emergency system, without manual intervention, and can remain in this condition for at least 10 hours.

(2) In the case of the PWR, boric acid coolant shall be made available for injection into the primary coolant system after a loss-of-coolant incident.

Note:

The requirements for the boration of the coolant are determined by the reactivity balance.

4.4.2 Boiling Water Reactor (BWR)

The coolant supply requirements in the case of a BWR are determined by the design concept of the pressure suppression system.

4.4.3 Water Supply for Wet Cooling Towers

The water supply in the storage pools shall be designed in connection with the available equipment for the make-up water supply such that enough water is available for the intended uses taking into account the maximum evaporation loss.

5 System Concept

5.1 System Function

5.1.1 Functionally Suitable Design of Systems and Components

(1) With respect to its division into sub-systems and their structure the circuit design concept for the RHR systems shall take into account the different intended uses and the different functional requirements resulting from them. The components required for this purpose shall be designed, structured, manufactured and assembled such that they reliably fulfill the requirements specified for them, taking into account the environmental conditions relating to each intended use. Account shall also be taken of the requirements resulting from the radioactivity and the chemical composition of the cooling media as well as from the properties of the materials.

(2) The following design principles should be applied to fulfill safety-related functions:

- a) system structure and system functions should be simply and clearly designed,
b) the necessary components should be designed and equipped such that to cope with an incident, they require the fewest possible auxiliary and supply systems,
c) the electrical loads required for residual heat removal shall be connected to emergency power facilities.

5.1.2 Coupling of Operational and Safety-Related Functions

(1) RHR during specified normal operation may be carried out by systems with purely operational function.

(2) If the requirements in both Section 5.2.2 and Section 5.2.3 are fulfilled, it is allowable to provide the same RHR systems both for normal operation and plant-internal incidents as well as for external events.

(3) In as far as the RHR systems for specified normal operation are able to cope with an incident these systems should be demanded prior to or together with the RHR systems which are especially provided to cope with incidents. However, the function of the RHR systems provided to cope with incidents shall not be detrimentally affected. Conversely the RHR systems provided to cope with incidents may be used for operational purposes if it is ensured

- a) that in the case of incidents, the RHR systems are transferred immediately and with the aid of reliable equipment into a condition which meets the safety requirements of this safety standard,
- b) that operational control signals do not detrimentally affect the safety functions, and
- c) that this does not result, in any significant influence being exerted on the unavailability and failure probability of the RHR systems after an incident has occurred.

5.1.3 Coupling of Different Safety-Related Functions

If different safety-related functions are coupled within a system, e.g. RHR and the ensuring of long-term subcriticality, the effectiveness of each of these functions in their respective intended use shall be ensured. The reliability of the safety-related functions in the case of such a coupling shall be ensured.

5.2 Failure Assumptions and Redundancy Requirements

5.2.1 Single Failure Concept

The "Interpretations of the Safety Criteria for Nuclear Power Plants, Single Failure Concept -General Principles for the Application of the Single-Failure Concept" shall apply to RHR systems. The requirements described in the following sections contain details on the single failure concept with regard to RHR systems.

5.2.2 Intended Uses During Specified Normal Operation and Plant-Internal Incidents

Note:

The requirements in this section do not apply to plant-internal events with a very low frequency of occurrence which are not design basis incidents in accordance with the Incident Guidelines pursuant to Sec. 28 para. 3 StrlSchV.

5.2.2.1 Event Combination and Redundancy

(1) The design of the systems required for RHR, including their auxiliary, supply and energy systems shall be based on the following events which may occur simultaneously or consecutively:

- a) Intended use to be coped with: Clearly defined intended uses, together with the protective or effectiveness objectives, shall be specified (See Section 3).

The failure of the power supply (emergency power case) shall be assumed if this is required in the "Incident Guidelines".

- b) Incident-induced consequential failures: Incident consequences and consequential failures in those RHR systems which are provided to cope with incidents shall be restricted such that their ability to cope with a single failure and maintenance work is still ensured.

- c) Single failure in any one component of the RHR systems but in compliance with Section 5.2.2.2: To cope with a single failure, the resulting requirement is for the RHR systems to be designed with simple redundancy ($n + 1$) of the systems related to the respective intended use. A redundant which is expected to become ineffective as a result of an initiating incident, shall not count when determining the number of redundants.

Note:

n is the number of redundants required to cope with the Intended use.

- d) Consequential failures after a single failure: Consequential failures after a single failure should remain limited to that redundant in which the single failure occurred (train separation in accordance with Section 5.2.2.4).

- e) Maintenance work: Basically the single failure criterion shall also be fulfilled during maintenance work.

Consequently, for systems in which repairs or servicing with the interruption of operational availability of a train are to be possible a double redundancy design ($n + 2$) shall basically be provided (in accordance with the specifications in Section 5.2.2.3) related to the respective intended use.

No additional redundancy need be provided to consider a functional test in a further train if the operational availability of the train can be restored in time in case of demand.

When scheduling, maintenance work in the case of a shutdown nuclear power plant, the same requirements shall basically be fulfilled. However, fulfillment of the single-failure criterion may be dispensed with if, while taking into account the temporal behavior of the plant, the system function can be restored in time in the case of an additional failure or the RHR can be otherwise ensured; auxiliary measures are also allowable for this purpose.

- (2) All the failures to be assumed in the reactor protection system shall be dealt with in accordance with the safety standard KTA 3501.

- (3) The auxiliary and supply systems within a train (e.g. lubrication oil, coolant valves of heat exchangers, hydraulic and pneumatic control equipment) should be so reliable that they have no significant influence on the unavailability and failure probability of the RHR after an incident.

5.2.2.2 Single Failure in Passive Components

- (1) No single failure needs to be assumed in passive components of the RHR systems if the requirements regarding design, structure, choice of materials, manufacture and testability are fulfilled in accordance with specifications which take the safety significance of the system parts into account.

Note:

Such specifications are, e. g. the RSK Guidelines for Pressurized Water Reactors, Sec. 4.1 for the pressure boundary and Sec. 4.2 for the external systems.

- (2) In the case of operational shutdown procedures, a failure in pipes smaller than or equal to DN 50 shall be assumed. Especially in the case of a pipe failure in the residual heat removal circuit, this means that the initial conditions shall be based on the conditions of the primary coolant at the time planned for the take-over of RHR by the RHR systems during normal operation.

- (3) After an incident, a single failure in pipes smaller than or equal to DN 50 need only be assumed in the long-term phase of residual heat removal.

5.2.2.3 Measures to be Provided for in the Case of Operational Unavailability of Redundants

- (1) In the case of the failure of a component in the RHR systems with a safety-related function, the repair of the component shall begin immediately after the failure is identified.

(2) If the fulfillment of the single-failure criterion in the remaining intact area of the system is no longer possible in the case of the operational unavailability of redundants, the operation of the nuclear power plant staff be restricted after identification of this condition (e. g. by power reduction or shutdown). If the nuclear power plant must be shut down the shutdown condition shall be selected such that the operational main heat sink is maintained as long as possible and recourse to the systems weakened by failure is avoided.

(3) In the case of the operational unavailability of a redundant which because of the short time taken to repair it has no significant influence on the unavailability and failure probability of the RHR after an incident, the independent failure of a further redundancy need not be considered.

5.2.2.4 Train Separation

(1) The RHR systems, including the associated auxiliary, supply and energy systems, which are intended for use in the case of plant-internal incidents, shall basically be constructed as separate trains. These trains shall be designed such that

- a) each train can fulfill its safety-related function independent of failures in other trains, or
- b) failures of components, which would cause the failure of more than one train, will be coped with safely.

(2) Considering the basic principles formulated in (1), connections between redundant trains and the use of components in common are allowable only if all the possible failures which are to be considered do not detrimentally affect safety-related functions. Connections between redundant trains via pipes should be closed in the standby position and shall be able to be safely isolated in the case of intended uses which are of relevance to safety.

Note:

Such connecting pipes may e. g. be the result of the operational function of a system or the attachment to a common test pipe. Connections may also be advisable in the interest of greater reliability for example in order to add components to increase redundancy.

5.2.3 Intended Uses after External Events

(1) With respect to failure assumptions and redundancy requirements external events shall basically be treated in the same way as the intended uses in accordance with Section 5.2.2.

(2) External events with a very low frequency of occurrence (e.g. aircraft crash and pressure wave of an explosion) are an exception to this rule. A single failure need not be assumed in this case. An occurrence of such an event during maintenance procedures also does not need to be assumed. In the case of the RHR systems provided for this intended use, including their auxiliary, supply, and energy systems, the following events shall therefore be assumed, which can occur either simultaneously or consecutively:

- a) the intended use to be coped with,
- b) the consequential failure of components to be assumed depending on the type of event.

5.2.4 Common Mode Failures

The following measures shall be taken against common mode failures which have a greater effect than the failure of a single train:

- a) Quality assurance in the planning, design and construction of the systems and components, in accordance with the functions to be fulfilled, taking into account all the environmental conditions to be considered,

- b) train separation and spatial separation of the redundants,
- c) choice of suitable materials and manufacturing processes,
- d) use of components of proven suitability (e. g. suitability, test or demonstration of reliable operation),
- e) testing in conditions as close as possible to those during the intended use,
- f) proper operational handling and servicing by trained personnel,
- g) in-service inspections, and
- h) quality assurance measures from the planning stage to operation.

5.3 Malfunctions Inside the Systems

Malfunctions inside the RHR systems themselves shall be coped with. The effects on other safety equipment shall be limited such that their function is not unallowably affected.

5.4 Safe Confinement of the Primary Coolant

5.4.1 Primary Coolant Confinement in the Case of Specified Normal Operation

(1) Those parts of the RHR system, which itself is attached to the primary coolant system, whose maximum allowable working pressure is below that of the primary coolant system shall be fitted with automatic isolating equipment consisting of two valves connected in series; it shall be possible to monitor these valve seats for leak tightness.

(2) The coolant injection pipes should preferably be fitted with check valves which are self-acting with respect to both injection and isolation.

(3) The isolation of the extraction pipes should be carried out with a high degree of reliability comparable to that of the injection pipes.

(4) The reactor coolant pressure boundary especially the part outside the containment vessel, shall meet high requirements with respect to leak tightness even during the intended use of the RHR system. It shall be possible to identify and isolate leaks.

5.4.2 Activity Barriers to the Heat Sink

(1) The discharge of activity via RHR systems to the heat sink shall be limited in accordance with the Radiological Protection Ordinance.

(2) Monitoring of the cooling trains for leaks and activity shall be provided for in accordance with the safety standard KTA 1504.

Note:

Basically, two activity barriers are provided. The first barrier can be a passive component (heat exchanger), the second can be a second passive component or an appropriate graduation of pressures.

If only one barrier is available (e. g. while discharging steam from the steam generator into the atmosphere), the acceptability of this measure will be demonstrated with respect to limiting the possible release of radioactive substances.

5.4.3 Isolation of Pipes in the Case of a Loss-of-Coolant Incident

(1) The isolation of those pipes in the RHR systems, which have no emergency cooling function in the case of a loss-of-coolant incident and which penetrate the containment vessel, shall be dealt with in accordance with Criterion 8.4 of the Safety Criteria.

Note:

Further specifications are contained in the safety standard KTA 3404.

(2) Pipes without an emergency cooling function, which are attached to parts of the RHR systems outside the containment vessel which can carry incident-induced radioactively contaminated coolant, shall be constructed such that they can be isolated by two isolation devices, one behind the other, as close as possible to the point of attachment.

(3) In the case of the pipes of RHR systems which have an emergency cooling function and penetrate the containment vessel the emergency cooling function shall be ensured with priority. A failure of these pipes outside the containment vessel shall only be assumed in accordance with the single failure concept in Section 5.2.2.2 (3). Similarly, no isolating devices are required in the injection pipes from the system to the primary coolant system on the penetration of the containment vessel if there are separate isolating devices for the primary coolant system, which close reliably in the case considered, and if consequential failures between the primary coolant system isolation and the containment vessel can be excluded. The same criteria shall apply to the extraction pipes from the primary coolant system.

(4) Those parts of the primary side RHR systems with a direct open connection to the atmosphere outside the containment vessel, e.g. the reflooding tanks or reflooding pools, shall be constructed such that they can be safely isolated from the incident-induced radioactively contaminated coolant by at least two isolating devices, one behind the other.

6 Arrangement and Construction Measures

6.1 Specified Normal Operation

The measures to be taken in this case are contained in the "Guideline for Radiological Protection Planning".

6.2 Plant-Internal Incidents

6.2.1 Measures for the Prevention of Consequential Failures

(1) Suitable measures shall be planned against the incident-induced stresses to be considered (e.g. reaction, jet and missile forces, flooding and fire, vibration and pressure wave) and against changed environmental conditions (e.g. humidity, pressure, temperature, radioactive radiation). Such measures are, e.g.:

- physically separated arrangement of the redundants,
- construction measures (e.g. pipe whip restraints, covers, reinforcements, shock arresters),
- structural measures, (e.g. compartmentalization, walls, raised foundations),
- component design adapted to the load.

(2) These measures shall also apply to the auxiliary, supply and energy systems as well as to the instrumentation and control equipment of the RHR systems.

6.2.2 Containment Vessel Sump

6.2.2.1 General Requirements

(1) It shall be ensured through the design the containment vessel and its internals that, in the case of a loss-of-coolant incident, the water escaping from the break reaches the containment vessel sump.

(2) Impurities in the containment vessel shall be kept as low as possible by the choice of suitable materials and design measures. For this purpose, the following aspects should be considered:

- insulation of the pipes and vessels such that material can only come off in the immediate vicinity of the break and the insulation cannot fray,
- use of insulation material with a density distinctly different from that of water,
- use of insulation material with short fibres, and
- use of firmly adhesive paints on structural components.

6.2.2.2 Intake Openings

(1) The flow paths to the intake openings in the RHR system shall be designed such that they can neither be so damaged by debris nor so obstructed by entrained materials that their functioning is unacceptably affected.

(2) The following precautions shall be taken to ensure that this requirement is met:

- Sum grids to hold back coarse debris and sump screens to hold back fine debris shall be provided, and both sump grids and sump screens should be arranged vertically. Gratings may also be used if appropriate for this purpose.
- The surface area of the sump grids shall be determined under consideration of the quantity of impurities likely to accumulate.
- The mesh size of the sump screens shall be specified such that pumps and valves are not endangered and the flow channels not obstructed.
- The intake openings shall be located above the level of the sump floor.
- The sump grids and screens as well as the intake openings shall be protected against consequential failures (e.g. as a result of jet forces).
- The design of the sump grids and screens shall take the flow forces and differential pressures due to pressure equalization processes into account.
- The intake openings shall be spatially separated.
- The sump grids and intake openings shall be designed such that they are accessible for inspections.

6.2.2.3 Intake Pipes

The intake pipes from the containment vessel sump to the first valve outside the containment vessel shall be designed such that the possibility of water being lost in incident conditions can be excluded. For this purpose, technical precautions shall be taken considering the requirements of Section 5.2.2.2 (3).

6.2.3 Measures to be taken for Long-term Operation

Through the arrangement of the RHR systems and the detailed design of the plant together, if necessary, with the use of temporary measures and additional special measures to protect the personnel, e.g. the use of heavy respiratory equipment, it shall be ensured that:

- access to the failed system parts can be restored,
- flooded compartments can be pumped free, and
- leaks can be sealed off,

to permit maintenance work on essential active components. The provisions of the "Guideline for Radiological Protection Planning", the "Guideline for Radiological Protection Measures" and the "Maintenance Guideline" shall be complied within this context.

Note:

Further specifications are contained in the safety standards KTA 1301.1 and KTA 1301.2.

6.3 External Events

The RHR systems required to cope with external events shall be designed to withstand the loads resulting from such events. Spatial separation shall be considered sufficient protection if the loads remain limited to partial areas of the plant.

6.4 Heat Sink

6.4.1 General Requirements

The equipment for RHR to a heat sink (such as the release of heat by discharging main steam into the atmosphere, the discharge of heat into bodies of water by means of direct cooling, the release of heat into the atmosphere via wet cooling towers) shall be designed and arranged to ensure RHR during specified normal operation, in the case of incidents and in the case of external events to be considered for the location of the plant (e.g. floods, drought, ice formation, washed-up flotsam, shell incrustation, earthquakes, aircraft impact, gas-cloud explosion).

6.4.2 Requirements for the Design of Intake Structures

Intake structures, including the purification equipment, shall be designed for the intake of cooling water from the main water course in accordance with the respective redundancy requirements. For RHR with river or sea water the following requirements shall be fulfilled:

- a) Precautions and measures shall be taken to hold back flotsam, algae, hay, shells, etc. and thus ensure the intake of the required cooling water. To prevent the adhesion of deposits in the RHR systems (e.g. shellfish larvae) operational measures (e.g. heating the affected train, intermittent chlorination) shall be taken,
- b) freezing up shall be prevented,
- c) unallowable reflux of the heated cooling water into the cooling water inlet shall be prevented, and
- d) the design shall be in accordance with the plant protection concept for coping with external events.

6.4.3 Requirements for the Design of Outlet Structures in the Case of River or Sea Water Cooling

Outlet structures shall be designed for the outlet of cooling water into the main water source during specified normal operation and in the case of plant-internal incidents. If outlet structures fail as result of external events, it shall be possible to discharge the cooling water by other means after it has been used to cool the plant.

6.4.4 Requirements for the Design of Wet Cooling Tower Facilities

Wet cooling tower facilities for RHR, including the associated water reservoirs, shall be designed and arranged in accordance with the respective redundancy requirements such that the following requirements are fulfilled in the case of their intended uses:

- a) Operation shall be ensured in the case of frost (prevention of ice formation) during any of the intended uses including functional tests, in particular by means of the appropriate arrangement of the storage pool and by other precautions and measures (e.g. by graduated admission into and ventilation of the cooling cells, by heating contact surfaces, by keeping the cooling tower internals free of snow).
- b) Precautions shall be taken against pollution and fouling by algae (e.g. intermittent chlorination).
- c) The design shall be in accordance with the plant protection concept for coping with external events.

7 Operation and Monitoring

7.1 Specified Normal Operation

7.1.1 Mode of Operation

(1) Manual control of the RHR systems is allowable. Control may be for individual components - individual operation - and, in the case of functionally associated groups of components, for groups - group operation.

(2) Routine periodic functional procedures should be automated in view of relieving the operating personnel.

(3) It shall be ensured by means of operational procedures that the limits specified for the cooldown rates intended for the protection of the components of the primary coolant system, as well as any other specifications to be considered (see Section 4.1), can be complied with during the shutdown procedure.

(4) The actuation elements for RHR operation shall be provided in the control room. The actuation elements for carrying out functional tests shall preferably be provided in the control room, but are also allowable at local control stations.

Direct intervention in the mechanical components by the operating personnel on location should remain restricted to maintenance.

(5) In the case of a failure of the power supply during residual heat removal, it shall be ensured via the instrumentation and control equipment that the components required for RHR can be supplied with emergency power and that RHR can be recommenced immediately.

7.1.2 Monitoring

(1) Important parameters (e.g. pressure, temperature, flow rate, water level) shall be displayed or recorded in the control room so that the condition of the systems can be quickly and correctly identified. In the case of unallowable deviations, hazard alarms shall be set off in the categories specified in the safety standard KTA 3501.

(2) Equipment for the protection of components shall be installed and set such that unallowable system conditions are avoided, even in the case of malfunctioning components or an error in the operation or a component (e.g. setting of safety valves and response values of the protection interlocks).

(3) To avoid activity discharges, provision shall be made for monitoring in accordance with the safety standard KTA 1504.

(4) The water quality to be is specified or the individual systems shall be maintained and monitored. Sampling points representative shall be located at points.

7.1.3 Precautionary Measures

(1) All the systems provided to cope with incidents shall be monitored and kept ready for use or in operation for as long as incidents can be expected. In general, this requires that

- a) the systems be filled with the fluids required for their operation,
- b) the necessary coolants be held ready in the design quantities and in their specified normal condition, and
- c) the auxiliary fluids be available in the required quantities and for an adequate duration of operation (e.g. lubricating oils).

(2) Remotely actuated valves should, as far as possible be in their specified position of readiness to cope with incidents and be fitted with a position monitor. Incorrect positions shall be indicated by signals in the control room.

- (3) Manually operated valves relevant to safety shall be secured against incorrect positioning.

7.2 Plant-Internal Incidents

7.2.1 Mode of Operation

The following modes of operation are allowable:

- a) the self-acting functioning of components, without control by instrumentation and control equipment and without external power, solely as a direct effect of process sequences,
- b) automatic activation and control,
- c) control by manual intervention from the control room or from local control stations in the case of pending safety hazard alarms in accordance with the safety standard KTA 3501. These manual interventions shall be specified in the operating handbook.
- d) control by manual intervention from the control room or from local control stations for long-term RHR. These manual interventions shall be specified in the operating handbook.

7.2.2 Monitoring

- (1) The parameters which are important for the identification of the condition of the systems (e.g. pressure, temperature, flow rate, level) shall be displayed or recorded in the control room.
- (2) The equipment required for this purpose shall be designed for the environmental conditions to be expected in the case of an incident.

Note:

The design criteria for Instrumentation and control equipment monitoring purposes are specified in greater detail in the safety standard KTA 3501.

7.3 External Events

7.3.1 Mode of Operation

(1) The degree of automation of the RHR stems shall be specified in relation to plant protection concept such that in the case of the external events to be met the reactor can be brought (from power operation) into the safe or subcritical condition and can be maintained in this condition.

(2) In case the control room is not operational and the emergency control center is neither manned nor can be manned quickly enough, RHR shall be possible automatically, i.e. without manual intervention, for a sufficiently long time, with the reactor remaining in a subcritical condition.

Note:

Present design practice is at least 10 hours; see RSK Guidelines for Pressurized Water Reactors, Sec. 22.2 (1).

It shall be possible to initiate the shutdown of the plant as soon as personnel is again available- the operation of components on location; and the use of auxiliary measures is allowable for this purpose.

(3) After an external event with consequences against which the control room and the switchgear building are protected, the modes of operation in accordance with Section 7.2.1 are allowable.

(4) Signals and commands from the emergency control center and from the part of the reactor protection system designed to withstand external events shall have priority over signals and commands from areas which are not protected against external events.

7.3.2 Monitoring

(1) The parameters of importance for the identification of the condition of the systems (e.g. pressure, temperature, flow rate, level) all be assigned to either the control room or the emergency control center in accordance with the concept for external events.

(2) The equipment required for this purpose shall be designed for the environmental conditions to be expected.

Note:

The design criteria for the Instrumentation and control equipment for monitoring purposes are specified in greater detail in the safety standard KTA 3501.

8 Power Supply.

8.1 Electrical Power Supply

The supply of electrical power to the RHR systems shall be designed in accordance with the requirements of the safety standard KTA 3701.1.

Note:

For this purpose, the following sections of the safety standard KTA 3701.1 are of importance:

- a) Sec. 3.2, Reliability,
- b) Sec. 3.4, Testability,
- c) Sec. 4.1, Basic Requirements for Off-Site Power Connections and Power Supply,
- d) Sec. 5.1, Basic Requirements for the Emergency Power System,
- e) Sec. 5.4, Protection against External Events,
- f) Sec. 5.5, Redundancy,
- g) Sec. 5.6, Functional Independence,
- h) Secs. 5.8.1 and 5.8.2, Determining the Emergency Power (Power Balance, Add-on Sequence),
- i) Sec. 5.9, Interruption and Delay Times,
- k) Sec. 5.10, Initiation and Termination of Emergency Power Operation,
- l) Sec. 7.3, Acceptance and Functional Tests on the Site, and
- m) Sec. 7.4, Inservice Inspections.

8.2 Non-Electrical Power-Supply

8.2.1 Direct-Coupled Drives

Diesel engines, which serve as direct drives of pumps, should be designed, manufactured and operated in accordance with the requirements for emergency power facilities with diesel generator sets according to the safety standards KTA 3702.1 and KTA 3702.2.

8.2.2 Pneumatic and Hydraulic Power Supplies

The same redundancy and reliability requirements shall apply as for other auxiliary and supply systems of the RHR systems (see also Sec. 5.2.2.1). However if a failure of the pneumatic or hydraulic power supply results in a safe condition a single-train design of the pneumatic or hydraulic power supply is adequate.

9 Ensuring Functional Capability and Operational Availability

9.1 Commissioning Tests

9.1.1 Purpose

The purpose of the commissioning tests is to demonstrate the functional capability and operational availability of the RHR systems and thus fulfill one of the prerequisites for the com-

mencement of the operation of the plant. In addition, the results of the commissioning tests shall be considered as the basis for the inservice inspections.

9.1.2 Extent of the Tests

The following tests shall be carried out:

- a) Functional tests of the individual units: Testing the functional capability and setting of the individual units and interlocks as well as their auxiliary, supply and energy systems.
- b) Functional tests of the instrumentation and control equipment: The interlocks switch criteria, hazard alarms and functional sequences shall be tested (e.g. selection, startup, shutdown, various modes of operation) on the basis of the function descriptions or function diagrams.
- c) Functional tests of the systems: The function of the whole system shall be tested. The tests shall be carried out such that the results enable conclusions to be drawn for the intended uses.

(2) If individual units fulfill several functions, each of these functions shall be tested individually.

9.1.3 Performance and Documentation

During the individual testing steps in accordance with Section 9.1.2, the criteria and displays set during the commissioning of the RHR systems shall be checked and compared with the required values. The performance of each test step and its results shall be documented.

9.2 In-service Inspections

9.2.1 Periodic Functional Tests

9.2.1.1 Objective

By means of periodic functional tests, it shall be determined whether the tested components or the tested system are operationally available with respect to all the functions required of the system.

9.2.1.2 Requirements

(1) The systems shall basically be designed such that periodic functional tests can be carried out without restricting power operation. If this is not possible, it is allowable to test individual components at longer intervals outside power operation. It shall be demonstrated individually that this measure is not detrimental to safety.

(2) The test shall not unallowably restrict the availability of the systems needed for coping with incidents. Initiations from the reactor protection system shall be given priority over the test schedule.

(3) The periodic demonstration of operational availability should be carried out under conditions similar to those during incidents, in as far as this is possible without restricting operation.

The periodic functional tests, together with the type, manufacturing and commissioning tests carried out earlier, shall enable clear conclusions to be drawn regarding operational availability under incident conditions.

(4) The instrumentation, control and power supply for the systems, required to cope with incidents should be tested such that information on the operational availability of the systems, can be obtained.

(5) The signals from the reactor protection system may be simulated as parts of the reactor protection test schedule in accordance with the safety standard KTA 3501.

(6) All the parameters, which help to provide information on the operational availability of the components and systems, shall be measured and documented.

9.2.1.3 Test Intervals

Functional tests shall basically be carried out every three to six weeks. Test intervals deviating from this shall be substantiated.

Note:

Test intervals for pressure relief valves are specified in the safety standard KTA 3302.

9.2.2 Non-Destructive Examinations

The RHR systems shall be planned such that non-destructive examinations of the components are possible in accordance with the Pressure Vessel Ordinance (DruckbehV); the test intervals, the extent of the tests and the testing methods result from this.

9.3 Maintenance

(1) The RHR systems shall be operated and maintained in accordance with the operating and servicing regulations. Maintenance work shall be carried out in accordance with the work release procedure as specified in the operating handbook in accordance with the safety standard KTA 1201.

(2) All the maintenance work carried out shall be documented.

(3) Functional tests shall be carried out subsequent to maintenance work.

10 Reliability Analyses

10.1 Objectives

(1) Reliability analyses provide quantitative information regarding the functional safety of RHR during its respective intended uses. These reliability analyses may be used, together with deterministic criteria, when designing the RHR systems, under consideration of the auxiliary, supply and energy systems, to verify whether the safety concept is balanced.

(2) In addition, reliability analyses can be carried out to:

- a) derive design requirements in those cases where either no deterministic criteria are available or the available criteria are not sufficiently validated
- b) provide quantitative information for the assessment of boundary conditions for the design,
- c) determine the influence of testing intervals and maintenance durations on reliability.

10.2 Extent

To verify whether safety concept is balanced, reliability analyses are made for specific intended uses, e.g., the failure of the main feedwater supply system, the failure of the main heat sink, a small leak in the primary cooling system, a large break in the primary cooling system. For this purpose, the intended uses shall be selected such that the analyses cover the safety-related functions of the RHR systems, including the required auxiliary, supply and energy systems, and the intended uses which are not examined contribute less to the failure frequency of the RHR. Reference may be made to reliability analyses already carried out for comparable systems in other plants.

10.3 System Preparation and Specification of Boundary Conditions

(1) To determine the qualitative and quantitative failure behavior of the system, it is necessary to construct a suitable model of the system under consideration. For this purpose, established procedures such as the fault tree analysis, method and symbols, in accordance with DIN 25424, Part 1 shall be used.

(2) The specification of an undesirable event may be based on either conservative effectiveness conditions or effectiveness conditions based on validated, realistic analyses. In addition, the use of operating systems may be taken into account.

(3) Manual measures may be taken into account with no temporal restrictions.

(4) In general, the failure rates and maintenance times required for the calculation shall be obtained from the available literature, e. g. from reports on analyses which have already been made.

Note. Preference shall be given to operating experience acquired in German nuclear power plants. Common mode failures shall be taken into account in reliability analyses if this is required to meet the objective, if the data are of an adequate statistical basis, and if it can be assumed that the data are applicable to the intended use being examined and are also transferable from the point of view of systems engineering.

10.4 Calculation of Reliability Characteristics

(1) As characteristics for the reliability of the RHR systems the probabilities $W(t_A, T_D)$ of the RHR functions not being fulfilled shall be calculated. For this purpose, the procedure in equation (10-1) shall be used:

$$W(t_A, T_D) = U(t_A) + (1 - U(t_A)) F(T_D/\text{added-on at } t_A) \quad (10-1)$$

A failure of the RHR exists if the RHR systems fail to start up at the required time t_A , or if, after having started up, the RHR fails during the endurance phase T_D (i.e. the period of time for which RHR is required).

(3) $U(t_A)$ is the non-availability (unavailability) at time t_A , i. e. the probability that the RHR systems will not be added on successfully at the required time.

(4) $F(T_D/\text{added-on at } t_A)$ is the cumulative failure probability of the RHR in the time interval $(t_A, t_A + T_D)$ provided that adding-on took place at time t_A . An important point here is that at time t_A , several components or trains in the RHR systems may also have failed. The type and number of these failures are limited in that adding-on of the RHR is assumed to have been successful.

(5) If it can be shown that the non-availability and the cumulative failure probability are different by at least one order of magnitude, the calculation of the smaller reliability characteristics is not required.

(6) The calculation of the reliability characteristics for the RHR systems shall be based on the associated failure rates, the test intervals and the maintenance times for the different types of failures in each of the components. In general, constant failure rates or constant failure probabilities per requirement shall be assumed in this context. This requires that the higher-failure rates to be expected at the beginning and towards the end of the lifetime of a component are avoided by suitable system trials and later by the replacement of worn parts in time.

10.5 Evaluation of the Results

(1) The evaluation of the results of reliability analyses should be based on:

- a) plants with a comparable safety concept, and
- b) generic investigations, e.g. risk analyses.

(2) When evaluating the results of reliability analyses it shall be considered that

- a) the input data are affected by statistical uncertainties,
- b) the results will scatter depending on the computer code used,
- c) all the analyses refer to models with a simplified representation of the failure behavior of the systems,
- d) common mode failures can make a predominant contribution to the result, particularly in the case of very small values for the non-availability or failure probability, and
- e) depending on the preparation of the system, conservative boundary conditions may have been used.

Appendix A

List of the Systems within the Scope of this Safety Standard

Pressurized Water Reactor

- a) Residual heat removal system, consisting of
 - high-pressure coolant injection system for the injection of emergency coolant, with the aid of safety injection pumps, into the primary coolant system during the phase of RHR via steam generators, in the case of loss-of-coolant incidents,
 - accumulators for the rapid reflooding of the reactor core in the case of loss-of-coolant incidents,
 - low-pressure injection system or RHR circuit for the injection of emergency coolant into the primary coolant system, in the case of loss-of-coolant incidents, and for the recirculation of the coolant via the residual heat exchanger, with the aid of the RHR pumps, in the case of incidents and when required for operational purposes;
- b) Emergency feedwater system for cooling the primary coolant system via steam generators by means of evaporation of water and to remove the steam thus produced to emergency condensers or into the environment;
- c) Main steam safety and discharge control valve for the discharge of main steam into the environment;
- d) Nuclear component cooling system for the removal of heat from heat exchangers for RHR and from other components required for the functioning of the RHR systems, via component cooling heat exchangers, and as a barrier in the cooling chain against the escape of radioactive substances into the environment;
- e) Nuclear service cooling water systems for cooling the component cooling heat exchangers and other components required for the functioning of the RHR systems, with the discharge of heat into bodies of water or the air;
- f) Systems which ensure RHR in the case of external events;
- g) Auxiliary and supply systems whose function is necessary for the system under consideration, in as far as design criteria and requirements for these systems have been specified (e.g. instrumentation, ventilation, structures).

Boiling Water Reactor

- a) Residual heat removal system, consisting of
 - high-pressure injection system for injection into the primary coolant system with the aid of the high-pressure pumps to replace losses due to leaks and the steam discharged via the relief valves into the pressure suppression chamber,
 - low-pressure injection System or RHR circuit, for the injection of emergency coolant into the primary coolant system in the case of loss-of-coolant incidents, for the recirculation of the coolant via the residual heat exchangers and for the cooling of the suppression chamber, with the aid of the RHR pumps, in the case of incidents and when required for operational purposes;
- b) Safety and relief valves for the reduction and limitation of pressure in the case of incidents in the primary coolant system by discharging the steam produced by residual heat into the condensation chamber;
- c) Nuclear component cooling system for the removal of heat from heat exchangers for RHR and from other components required for the functioning of the RHR systems, via component cooling heat exchangers and as a barrier in the cooling chain against the escape of radioactive substances into the environment;
- d) Nuclear service cooling water system for cooling the component cooling heat exchangers and other components required for the functioning of the systems, with the discharge of heat into bodies of water or the air;
- e) Systems which ensure RHR in the case of external events;
- f) Auxiliary and supply systems whose function is necessary for the system under consideration, in as far as design criteria and requirements for these systems have been specified (e.g. power supply, control, instrumentation, ventilation, structures).

The basic diagrams in **Figure A-1**, **Figure A-2** and **Figure A-3** show examples of the residual heat removal systems presently used in the Federal Republic of Germany. In each case, just one of the redundant trains is shown.

- | | |
|--|---|
| <ul style="list-style-type: none"> a Main steam pipe b Emergency feedwater system c Heat sink d Nuclear component cooling system e Nuclear service cooling water system f Residual heat removal system | <ul style="list-style-type: none"> 6 Component cooling water pump 7 Component cooling heat exchanger 8 Service cooling water pump 9 Emergency feedwater pump 10 Demineralized water tank/pool 11 Main steam discharge station 12 Containment vessel sump |
| <ul style="list-style-type: none"> 1 Accumulator 2 Safety injection pump 3 Residual heat removal pump 4 Residual heat exchanger 5 Flooding tank/pool | <ul style="list-style-type: none"> A Containment vessel B Reactor pressure vessel C Steam generator D Primary coolant pump |

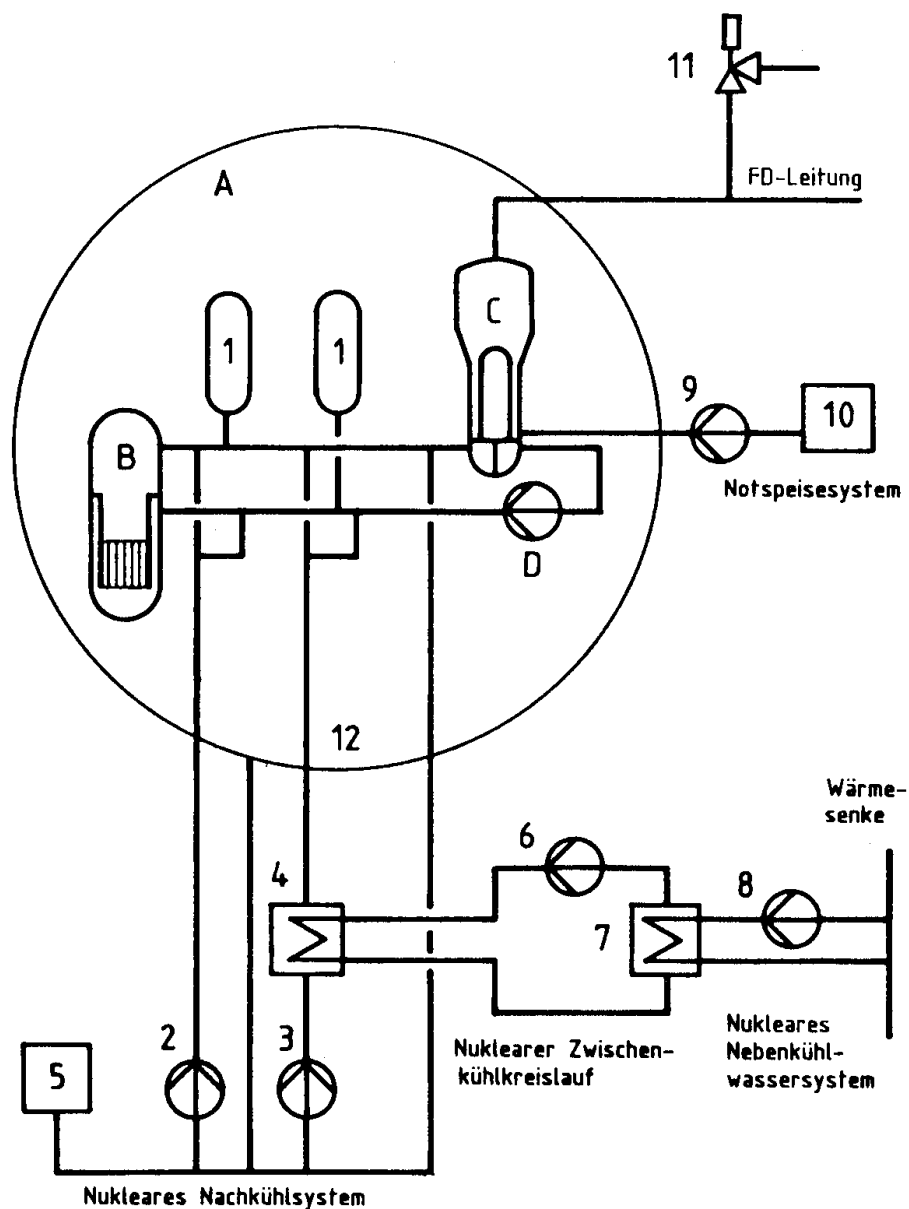
Figure A-1: Simplified Diagram of the Residual Heat Removal Systems, - Example 1 (PWR)

- | | |
|--|--|
| <ul style="list-style-type: none"> a Main steam pipe b Emergency cooling system c Emergency feedwater system d Heat sink e Nuclear component cooling system f Nuclear service cooling water system g Residual heat removal system | <ul style="list-style-type: none"> 7 Component cooling heat exchanger 8 Service cooling water pump 9 Emergency feedwater pump 10 Receiving tank 11 Main steam discharge station 12 Containment vessel sump 13 Emergency condenser 14 Condensate pool 15 Condensate pump |
| <ul style="list-style-type: none"> 1 Accumulator (core flooding tank) 2 Safety injection pump 3 Residual heat removal pump 4 Residual heat exchanger 5 Borated water storage pool 6 Component cooling water pump | <ul style="list-style-type: none"> A Containment vessel B Reactor pressure vessel C Steam generator D Primary coolant pump |

Figure A-2: Simplified Diagram of the Residual Heat Removal Systems, Example 2 (PWR)

- | | |
|--|---|
| <ul style="list-style-type: none"> a Main steam pipe b Residual heat removal system c Nuclear component cooling system d Nuclear service cooling water system e Heat sink | <ul style="list-style-type: none"> 3 Residual heat removal pump (preliminary stage, low-pressure stage) 4 Residual heat exchanger 5 Component cooling water pump 6 Component cooling heat exchanger 7 Service cooling water pump |
| <ul style="list-style-type: none"> 1 Safety and relief valve 2 High-pressure pump | <ul style="list-style-type: none"> A Containment vessel B Reactor pressure vessel C Pressure suppression chamber |

Figure A-3: Simplified Diagram of the Residual Heat Removal Systems, Example 3 (BWR)

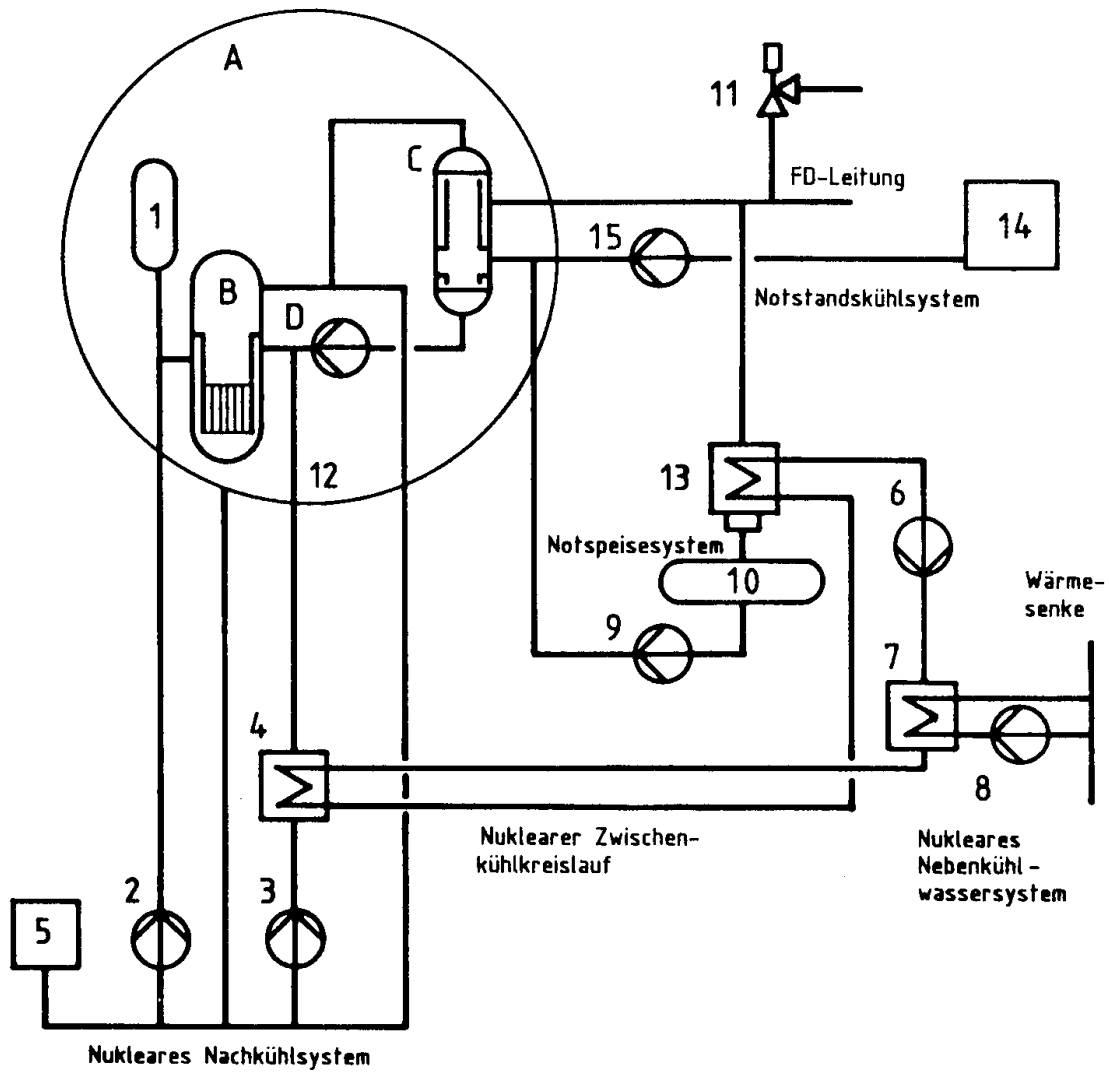


- 1 Druckspeicher
- 2 Sicherheitseinspeisepumpe
- 3 Nachkühlpumpe
- 4 Nachwärmekühler
- 5 Flutbehälter / Flutbecken
- 6 Zwischenkühlpumpe
- 7 Zwischenkühler
- 8 Nebenkühlwasserpumpe
- 9 Notspeisewasserpumpe
- 10 Deionatbehälter / Deionatbecken
- 11 Frischdampf - Abblasestation
- 12 Sicherheitsbehältersumpf

- A Sicherheitsbehälter
- B Reaktordruckbehälter
- C Dampferzeuger
- D Hauptkühlmittelpumpe

Bild A-1

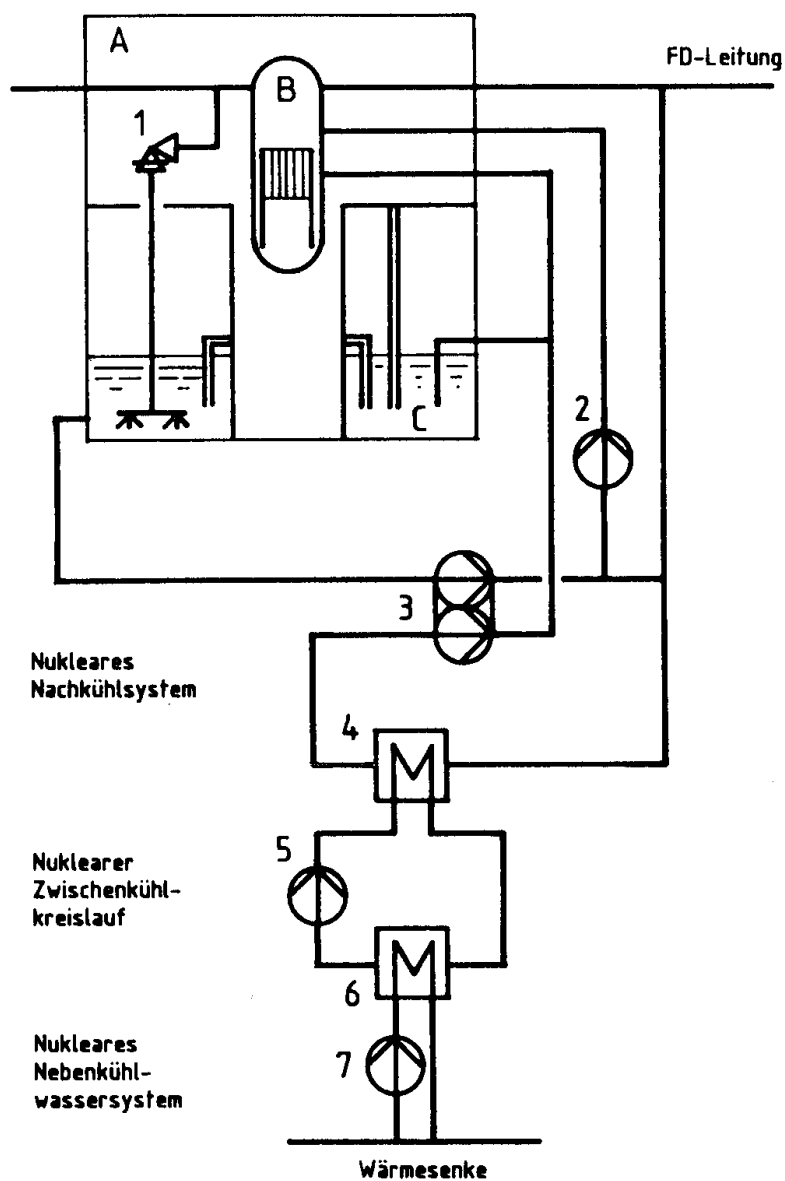
Vereinfachte Darstellung der Nachwärmeabfuhrsysteme, Beispiel 1 (DWR)



- | | |
|------------------------------------|------------------------|
| 1 Druckspeicher (Kernflutbehälter) | A Sicherheitsbehälter |
| 2 Sicherheitseinspeisepumpe | B Reaktordruckbehälter |
| 3 Nachkühlpumpe | C Dampferzeuger |
| 4 Nachwärmekühler | D Hauptkühlmittelpumpe |
| 5 Borwasserbecken | |
| 6 Zwischenkühlpumpe | |
| 7 Zwischenkühler | |
| 8 Nebenkühlwasserpumpe | |
| 9 Notspeisewasserpumpe | |
| 10 Vorlagebehälter | |
| 11 Frischdampf-Abblasestation | |
| 12 Sicherheitsbehältersumpf | |
| 13 Notkondensator | |
| 14 Kondensatbecken | |
| 15 Kondensatpumpe | |

Bild A-2

Vereinfachte Darstellung der Nachwärmeabfuhrsysteme, Beispiel 2 (DWR)



- | | | | |
|---|--|---|----------------------|
| 1 | Sicherheits- und Entlastungsventil | A | Sicherheitsbehälter |
| 2 | Hochdruckpumpe | B | Reaktordruckbehälter |
| 3 | Nachkühlpumpe (Vorstufe, Niederdruckstufe) | C | Kondensationskammer |
| 4 | Nachwärmekühler | | |
| 5 | Zwischenkühlpumpe | | |
| 6 | Zwischenkühler | | |
| 7 | Nebenkühlwasserpumpe | | |

Appendix B

Regulations Referred to in this Safety Standard

| | | |
|---|--|---|
| Radiological Protection Ordinance | | Ordinance on the Protection Against Damage and Injuries Caused by Ionizing Radiation (Radiological Protection Ordinance - StrlSchV) dated October 13, 1976(BGBl. I, p. 2905), last modified by the Ordinance dated May 22, 1981 (BGBl. I, p. 445) |
| Incident Guidelines | | Guidelines for the Assessment of the Design of Nuclear Power Plants with Pressurized Water Reactors against Incidents pursuant to Sec. 28 para. 3 StrlSchV - Incident Guidelines (made public by the Federal Minister of the Interior (October 18, 1983; Bundesanzeiger No. 245a of December 31, 1983) |
| Pressure Vessel Ordinance | | Ordinance Relating to Pressure Vessels, Compressed Gas Vessels and Filling Equipment (Pressure Vessel Ordinance - DruckbehV) dated February 27, 1980 (BGBl. I, p. 184). |
| Guideline for Radiological Protection Planning (7/78) | | Guideline for the Protection against Radiation of Personnel during die Execution of Maintenance Work in Nuclear Power Plants with Light Water Reactors: The Precautionary Protective Measures to be taken during the Planning of the Plant (Circular issued by BMI on July 10, 1978 - RS 11 3) (GMBI. 1978, p. 418), Reactor Safety Handbook No. 3.43 |
| Guideline for Radiological Protection Measures (6/81) | | Guideline for the Protection against Radiation of Personnel during the Execution of Maintenance Work in Nuclear Plants with Light Water Reactors; Part II: Radiological Protection Measures during Commissioning and Operation of the Plant, as amended on June 23, 1981 (Circular issued by BMI on August 4, 1981 - RS II 3 - 515 800/5); (GMBI. 1981, p. 363), Reactor Safety Handbook No. 3.43.1 |
| Maintenance Guideline (6/78) | | Guideline Relating to the Procedure for the Preparation and Implementation of Maintenance Work and Modifications at Nuclear Power Plants (made public by BMI on June 1, 1978 - RS I 6), (GMBI. 1978, p. 342), Reactor Safety Handbook No. 3.41 |
| Safety Criteria (10/77) | | Safety Criteria for Nuclear Power Plants (made public by BMI on October 21, 1977, Bundesanzeiger No. 206 of November 3, 1977) |
| Single Failure Concept (4/84) | | Interpretations o the Safety Criteria for Nuclear Power Plants, Single Failure Concept - General Principles for the Application of the Single Failure Concept (made public by BMI on April 12, 1984), (GMB1. 1984, p. 208) |
| KTA 1201 (3/81) | | Requirements for he Operating Manual |
| KTA 1301.2 (6/89) | | Radiological Protection Considerations for Plant Personnel in the Design and Operation of Nuclear Power Plants, Part 2: Operation |
| KTA 1504 (6/78) | | Measuring Liquid Radioactive Materials for Monitoring the Radioactive Discharge |
| KTA 3501 (6/85) | | Reactor Protection System and Monitoring of Equipment of the Safety System |
| KTA 3701.1 (6/78) | | Basic Requirements for the Electrical Power Supply of the Safety System in Nuclear Power Plants; Part 1: Single-Unit Plants |
| KTA 3702.1 (6/80) | | Emergency Power Facilities with Diesel Generator Sets in Nuclear Power Plants, Part 1: Design |
| KTA 3702.2 (11/82) | | Emergency Power Facilities with Diesel Generator Sets in Nuclear Power Plants, Part 2: Tests and Inspections |
| DIN 24260 (6/71) | | Centrifugal Pumps and Centrifugal Pump Units; Definitions, Symbols, Units |
| DIN 25424 Part 1 (9/81) | | Fault Tree Analysis: Methods and Graphical Symbols |
| DIN 25463 Part 1 (5/90) | | Calculation of the Decay Heat Power in Nuclear Fuels of Light Water Reactors |