Reliability Analyses to Detect Weak Points in Secondary-Side Residual Heat Removal Systems of KWU PWR Plants

R. Schilling
Kraftwerk Union AG, Abteilung V112, Postfach 3220, D-8520 Erlangen, Germany

Summary

Requirements made by Federal German licensing authorities called for the analysis of the secondary-side residual heat removal systems of new PWR plants with regard to availability, possible weak points and the balanced nature of the overall system for different incident sequences.

Following a description of the generic concept and the process and safety-related systems for steam generator feed and main steam discharge, the reliability of the latter is analyzed for the small break LOCA and emergency power mode incidents, weak points in the process systems identified, remedial measures of a system-specific and test-strategic nature presented and their contribution to improving system availability quantified. A comparison with the results of the German Risk Study on Nuclear Power Plants (GRS) shows a distinct reduction in core meltdown frequency.

1 Purpose

The code to be applied in the Federal Republic of Germany for the design of nuclear power plants is without a doubt oriented towards deterministic criteria. In the general safety criteria of the Federal Ministry for the Interior, explicit allowance is however made for the fact that, in addition to overall assessment of the safety of a nuclear power plant, the reliability of safety-related systems may be determined using probabilistic methods. Some of the objectives of these realiability analyses are:

- recognition of viable possibilities for improvements within the system itself
- verification of adequate system reliability and
- establishment of a balanced safety concept with regard to the incidents to be mitigated and to safety functions.

Basing on these criteria and in response to the incident sequence analyses of the German Risk Study on Nuclear Power Plants (GRS), /1/, the independent experts for the follow-up plants (Grohnde, Philippsburg 2) to the reference plant of the GRS (Biblis B), whose licensability has already been proven on the basis of deterministic criteria, called for a quantitative analysis of the most importent safety-related systems in respect of their balanced nature in the event of various incident sequences. Depending on the varying incident-specific relevance of the systems, the required system reliability is oriented on the probability of occurence of the incidents.

In order to meet this requirement, the first step should be to perform a detailed probabilistic reliability analysis of the systems designed for secondary-side residual heat removal in order to establish dominant fault paths. The second step should be to identify the influence of different system modifications with the aid of a sensitivity analysis. For reasons of consistency, the process systems connected immediately upstream the safety systems should also be included in the analysis since these systems reduce the demand-mode frequency of safety-related systems in the present concept.

Although primary-side system functions are also required for incident mitigation, only the secondary-side system should be included in this investigation since these systems are of primary importance in the refarence plant of the GRS.

2 Description of the System Concept

The generic concept for secondary-side residual heat removal (steam generator feed, main-steam discharge) is illustrated using the example of the latest 1300 MW PWR plants (e.g. Isar 2), and the system structure and the function of available systems are described.

2.1 Steam Generator Feed

In the event of incidents, both process equipment and safety features are available to provide steam generator feed (Fig. 1).

In respect of process-related functions

- a feedwater system (3 pumps) and
- a startup and shutdown system (2 pumps)

are available
and for safety-related functions

- an emergency feed system (4 subsystems).

The process-related pump systems transfer hot water from the feedwater tank via steam-generator-specific valve stations into the steam generators. Make-up feed is pumped into the feedwater tank by three main condensate pumps, or alternatively, if the ultimate heat sink is not available, it is drawn from the demineralized water storage tank using the two demineralized water pumps. The startup and shutdown as well as the demineralized water pumps with the associated auxiliary equipments and valve stations are connected to the emergency power supply system and their capacity is such that one startup and shutdown pump together with one demineralized water pump are capable of transferring the necessary feed into the ateam generator(s) for the removal of residual heat.

The emergency feed system designed on the basis of safety-related criteria is characterized by its consistent four-train configuration with separate steam generator inlet nozzle. It is accommodated in the external impacts-proof (aircraft crash, explosion blast wave, earthquake, sabotage) emergency feed building and each of its trains is essentially mede up of a demineralized water pool, emergency feed pump with electric and diesel drive, generator, cooling equipment and connecting piping and valves. Each of the four redundant subsystems is capable of conveying the necessary demineralized water flow into the associated steam generator for the removal of residual heat. A manually operable connecting line between the four discharge trains makes it possible to feed each steam generator with any of the four subsystems. The stored media inventory (demineralized water, diesel oil) and the degree of automation allow independent operation of the system in the event of external impacts lasting more than ten hours.

Figure 2 features a general outline of the stepped concept to ensure steam generator feed (feedwater, startup and shutdown, emergency feed system) and illustrates the allocation of power supply and mechanical equipment for process and safety-related systems. The electric emergency feed drive conceived for the latest plants is the result of a requirement imposed by independent experts which specifies that long-term assured steam generator feed should be provided in the event of incidents involving the failure of the process feedwater supply system but with a power supply from the interconncected grid available. This means that long-term operation of the diesel drives may be dispensed with.

2.2 Main Steam Discharge

For reasons of conservativenesa, this paper will not deal with the possibility of main steam discharge to the ultimate heat sink via the main steam bypass station.

If the ultimate heat sink is not available, residual heat is removed via the steam-generator-specific safety-related main steam exhaust stations which each essentially comprise one main steam isolating valve, one isolatable exhaust control valve and one isolatable safety valve. The safety-related design features of each of the four redundant stations are such that all the residual heat generated after shutdown and the stored heat present can be removed completely. The four exhaust stations are accomodated in a valve compartment located adjacent to the reactor building; they are physically separated and protected against all forms of external impact. The main steam header, which is arranged in the turbine building and which interconnects the four main steam lines, is part of the process system but mey, however, also be put into use in the event of transients and LOCAs.

3 System Analysis

The 'small break LOCA' and 'emergency power mode' incident sequences which play a predominant role in the GRS of core meltdown frequency within the scope of event sequence analyses were investigated with regard to the non-availability of systems for secondary-side residual heat removal in the form of a fault-tree analysis. The available and included systems (clearly illustrated in tha form of main components) and the associated effectiveness requirements (minimum requirements made of system function) are shown in Figures 3 and 4 in relation to incidents.

Possibilities for steam generator feed and main steam discharge including use of the main steam header are shown in Fig. 5 using the example of the small break LOCA. Even if only one steam generator is fed with the aid of one emergency feed pump and one startup and shutdown pump (double steam generator feed), the rapid temperature reduction (100 K/h) planned in the event of this incident can be achieved via any one of the main steam exhaust stations. In order to preserve clarity, this possibility was not taken into consideration in Fig. 4, but included in the analysis.

Detailed incident-specific fault trees reflecting the actual status were prepared which take into account both the mechanical systems and their actuation and power supply.

The non-availability of the systems was determined using the IASAPL computer program /2/. This included application of the failure rates generally accepted in the Federal Republic of Germany and took account of system and component-specific testing strategies. In the initial calculation only the non-availability of safety systems was determined whereas the second calculation included the above-mentioned process systems.

There were no dominant fault paths to be found in either the emergency feed system or in the main steam exhaust stations which meant that possible system-specific modifications would result in an increase in reliability in only a limited number of cases; the systems under consideration have already been optimized in the early stage of their development with in respect of structure, arrangement, minimum requirement and testing strategy.

Possibilities for improvements were established in the process systems. A flow limiter valve arranged in the header line downstream of the two startup and shutdown pumps and a feedwater tank feed control valve likewise arranged in the header line downstream of the demineralized water pumps were the primary cause of the non-availability of these systems. As indicated in Fig. 6, improvements were achieved by employing redundant design features. The effect was an increase in the availability of these systems (using the example of the emergency power mode) from 70 to 80 %. Since a further increase in availability by installing a third train appeared possible, but would be linked with a considerable amount of work, it was decided instead to upgrade the standby systems (normally only used for startup and shutdown, and for process-related demineralized water back-up feed) which have a minimum demand mode frequency of once per annum, by introducing a regular in-service inspection. It was evident that an optimized interval between in-service inspection of 3 months in the startup and shutdown, and demineralized water system would result in a marked increase in availability from 70 to 92 %. These two measures-system-specific and test-strategic-result in an increase in the availability of the considered process systems for steam generator feed from 70 to 97 % which means that in only 3 % (previously 30 %) of all emergency power modes a safety system (emergency feed system) demand mode is to be anticipated.

4 Findings

By comparison with the reference plant of the GRS, about 10 years of further development in the field of plant engineering have been incorporated in PWR plants based on present-day concepts. This development confirmed the generic concept on safety, albeit a number of points were changed. These changes are the result of probabilistic and deterministic system analyses and discussions, system and component-specific developments, as well as operating experience and site-specific conditions. The non-mitigated plant condition "core meltdown" as defined in the GRS is applied as a yardstick for a comparative evaluation where the condition is the sum of the incident frequency and the non-availability of the systems required for incident mitigation.

To be able to make a comparison with the findings of the GRS, this investigation (and the GRS) was based for reasons of conservativeness on a diesel common-mode failure of 10^{-3}/demand mode which, in the opinion of KWU and that of German power plant owner/operators is considered unrealistic and extremely conservative; this is confirmed by the operating experience gained with diesel engines of this kind. For the two incident sequences investigated in which the secondary side plays a major role, the systems engineering incorporated and the above-mentioned modifications result in a marked increase in availability which is also evident in the reduction in core meltdown frequency. Even if a diesel common-mode failure is postulated, the non-availability of the secondary side is at least as low as that of the primary side which means that the latter no longer plays the major role established in the GRS.
Thus we obtain a balanced concept for the various safety functions which are required for incident mitigation.

Figure 7 features a comparison with the findings of the GRS. The frequency of occurrence of the small-break LOCA was taken from the GRS; in the case of the emergency power mode, a better value was used for the new plants since provision was made for improved grid integration.

Following on from the already low level of core meltdown frequency in the GRS, a further decrease is evident in the case of new plants. In both sequences graphic representation is terminated at a core meltdown frequency of 10^{-6}/a.

5 Conclusion

The process and safety systems for secondary-side residual heat removal in new PWR plants were investigated with the aid of probabilistic reliability analyses with regard to the non-availability of these systems for two major incident sequences. In keeping with the set objective,

- an improvement of the overall system was achieved by means of the detection of possible weak points in the startup and shutdown as well as the demineralized water system and with the aid of remedial measures involving modifications to system engineering and a reduction of the interval between inservice inspections,
- proof of adequate system reliability was furnished and
- it was established that the measures have resulted in a balanced safety concept. The quantitative comparison with the findings of the GRS indicates - where an extremely conservative diesel common-mode failure is applied in each case - an overall improvement in the incident sequences having a primary effect on core meltdown frequency.

6 References

/1/ Deutsche Risikostudie Kernkraftwerke
Hauptband, Verlag TÜV Rheinland, 1979

/2/ F. W. Heuser and W. Rosenhauer
"SAP-1 Ein neues Programm zur Berechnung von Zuverlässigkeitsgrößen komplexer Systeme"
Atomwirtschaft, 17, 2 (1972)

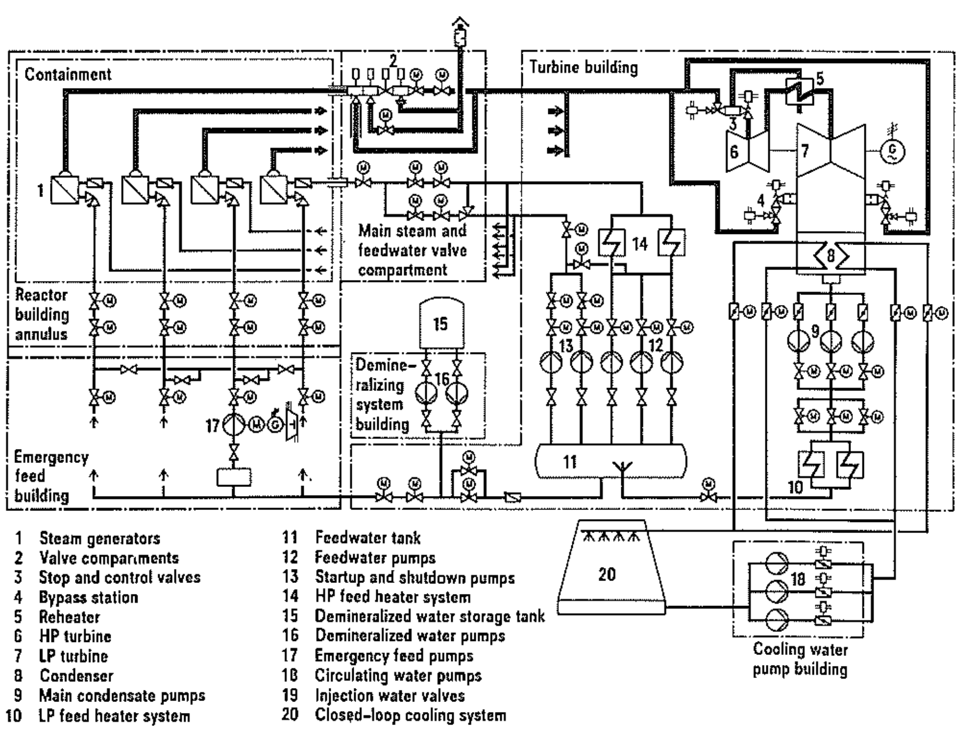

Fig. 1

1300 MW PWR (4×20 m²)
Systems for Secondary-side Heat Removal (Survey)

E 83 096 C

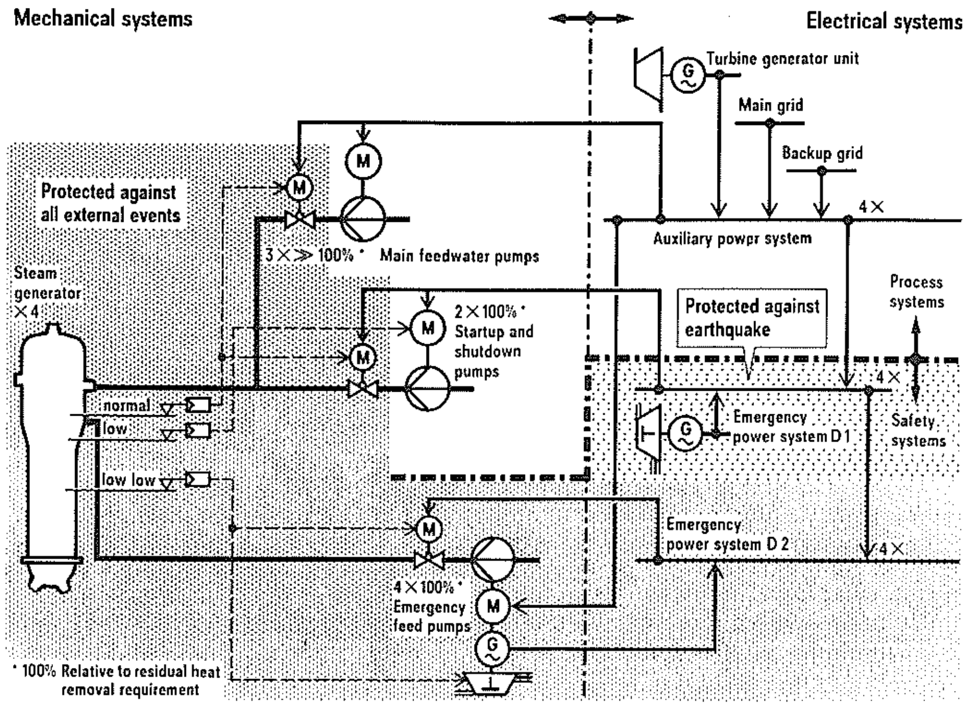

Fig. 2 1300 MW PWR
Possible Modes of Steam Generator Feed (Survey)

83 093 C

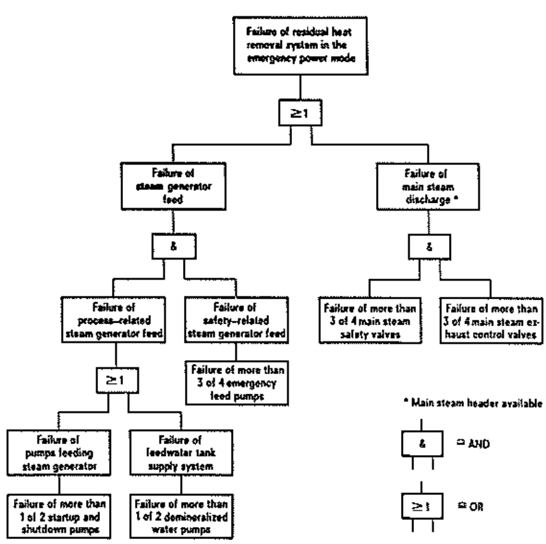

Fig. 3

1300 MW PWR
General Fault Tree for the Failuro of the Secondary-side Residual Heat Removal System in the Emergency Power Mode

E83 094 C

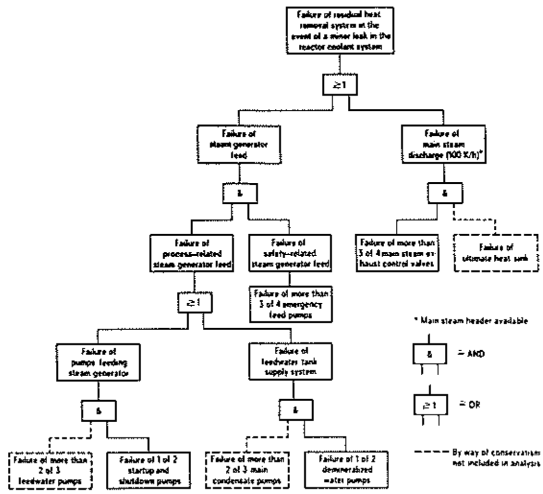

Fig. 4

1300 MW PWR/General Fault Tree for the Failure of the Secondary-side Residual Heat Removal System in the Event of a Minor Leak in the Reactor Coolant System

E83 095 C

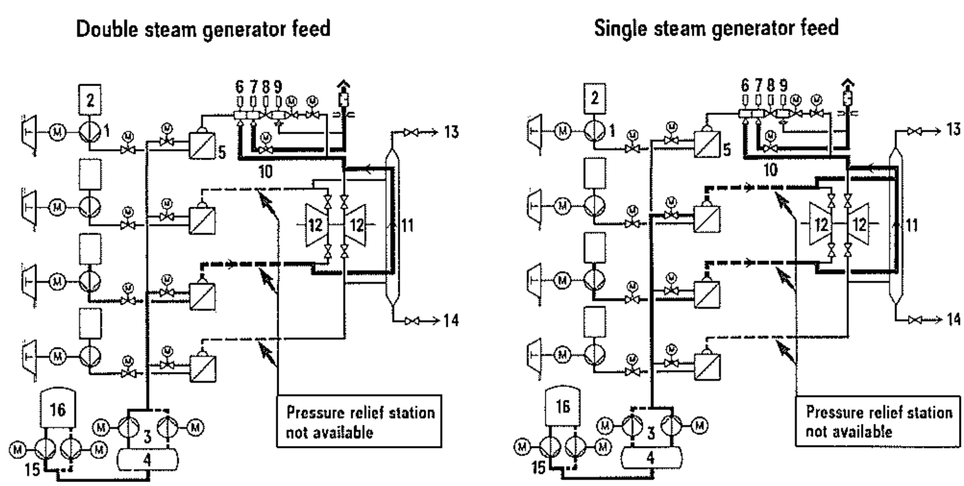

Fig. 5

1 Emergency feed pump
2 Demineralized water tank
3 Startup and shutdown pumps
4 Feedwater tank
5 Steam generator
6 Main steam isolation valve
7 Main steam exhaust isolating valve
8 Isolating valve upstream of main steam safety valve
9 Main steam safety valve
10 Main steam exhaust control valve
11 Main steam header
12 HP turbine
13 To feedwater tank pegging steam supply
14 To main steam bypass station
15 Demineralized water pumps
16 Demineralized water storage tank

1300 MW PWR/Examples of Steam Generator Feed and Main Steam Discharge in the Event of a Minor Leak in the Reactor Coolant with Ultimate Heat Sink Failure (Survey)

E83 099 C

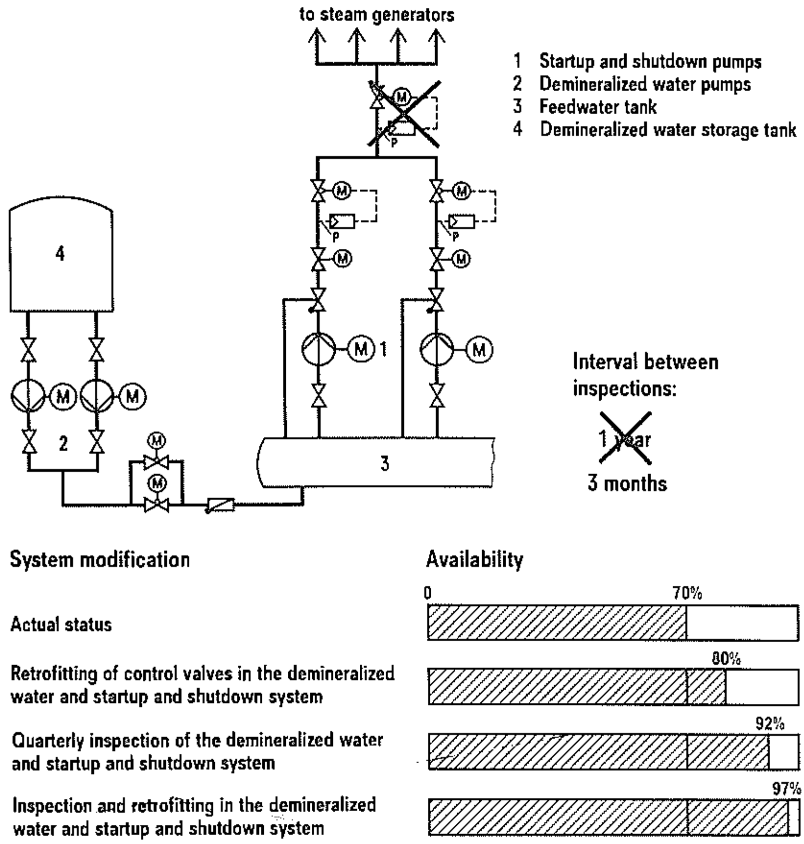

Fig. 6

1300 MW PWR/Increase in the Availability of the Process Steam Generator Feed System by Improvements to Systems and Reduction of the Intervals between Inspections

E 83 098 C

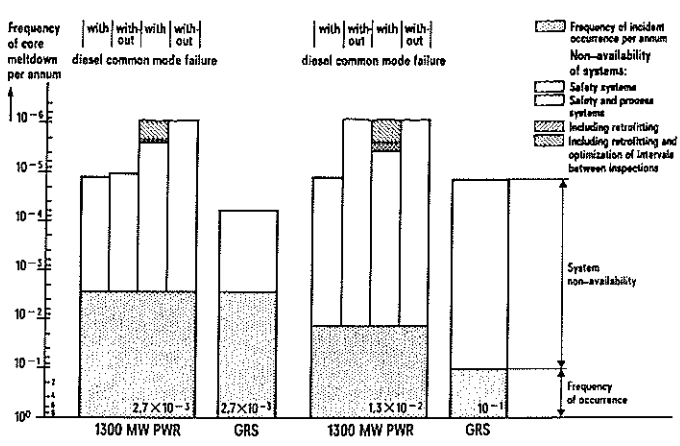

Fig. 7

1300 MW PWR/German Risk Study on Nuclear Power Plants (GRS)
Comparison of the Core Meltdown Frequency for the Minor Leak in the Reactor Coolant System and Emergency Power Mode Incidents

E 83 097 C