A RELIABILITY APPROACH FOR INSPECTION STRATEGY APPLIED TO AN EMERGENCY CORE COOLING SYSTEM

H.-P. BALFANZ, F.W. HEUSER, W. ULLRICH

Institut für Reaktorsicherheit der Technischen Überwachungs-Vereine e.V., D-5000 Köln 1, Germany

SUMMARY

A reliability analysis is given for a model system of an emergency core cooling system of a pressurized water reactor. In order to show some basic relationships and influences on the system's failure probability the analysis deals only with some main components and subsystems of the emergency core cooling system. Referring to the design basis accident, i.e. the total rupture of a main coolant line, only the low pressure system is considered.

The overall system's failure probability is determined by the failure probability per demand, i.e. the unavailability of the system when called on for operation in the emergency case, and the cumulative probability of failure during the subsequent phase of residual heat removal. Detailed calculations have shown that the failure probability per demand is the leading term. Special attention is given to some parameter calculations dealing with the influence of inspection time intervals and repair procedures for different components and subsystems with respect to system's failure behaviour.

1. Introduction

The emergency core cooling system of a light water reactor plant will be regarded as an engineered safeguard against the loss of coolant accident. It has to ensure safety requirements for the case of small leckage as well as for the design basic accident which is described by the total rupture of a main cooling line. Since a loss of coolant accident always is combined with a large risk the emergency core cooling equipment must meet high safety standards. Therefore the design of the system must also meet some general safety criteria which have been worked out for nuclear power plants [1].

The paper deals with some aspects of a reliability analysis for an emergency core cooling system of a pressurized water reactor. Therein the main features of this analysis will be worked out with the aid of a simple model system including the main components and subsystems influencing the overall failure probability of the emergency core cooling equipment. Especially to be discussed is the system's failure behaviour in connection with the influence of some repair procedures, inspection strategies, and failures of subsystems.

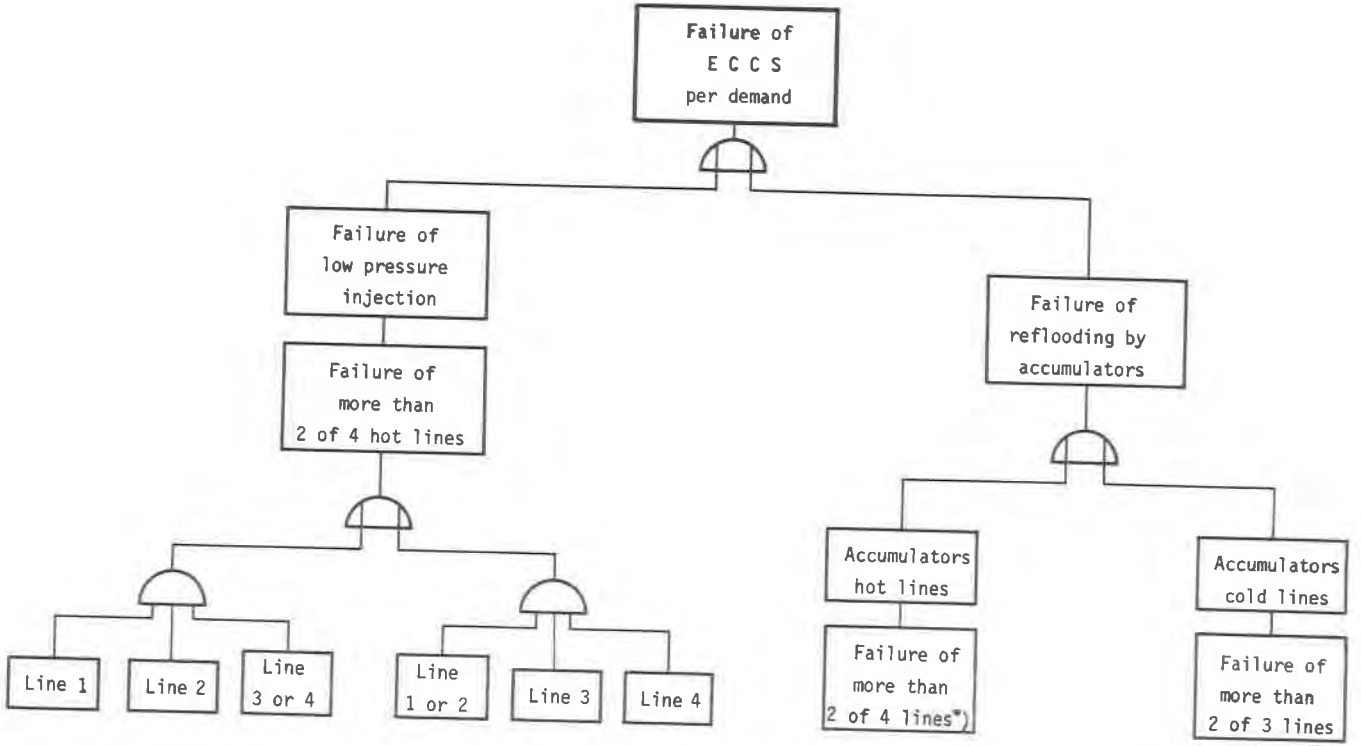
2. System Description

Fig. 1 gives a block diagram of the model system considered here. Only the low pressure system will be discussed. It consists of two subsystems, the accumulators' system and the recirculation system for low pressure injection and residual heat removal.

The equipment consists of four emergency cooling lines each splitting into two branches leading to the hot and the cold leg of the corresponding main cooling lines. The check valves at the end of each emergency train separate the emergency cooling lines from the main coolant system. Further, each cooling line is made up by an accumulator, a residual heat exchanger, one low pressure pump and some valves for switching the cooling line from the borated water storage tanks to the supply from the containment sump. In case of loss of normal power each pump will be supplied by one Diesel generator assigned to each cooling line.

Considering the design basic accident as the reference case, i.e. the total rupture of a main cooling line, the operating procedure after accident can be divided into different phases following one after another sequentially.

In order to prevent the melting of fuel rods the reactor must be reflooded immediately after accident. For this purpose at least two of four accumulators must be available for reflooding the core. The low pressure pumps are started automatically by the low pressure injection signal; two of four pumps are necessary for feeding borated water from the storage tanks to the reactor vessel. After nearly 20 min the water storage



*) One line is taken in account only with W = 0,2

FIGURE 2:

Fault tree of the emergency core cooling system for calculating the failure probability per demand.

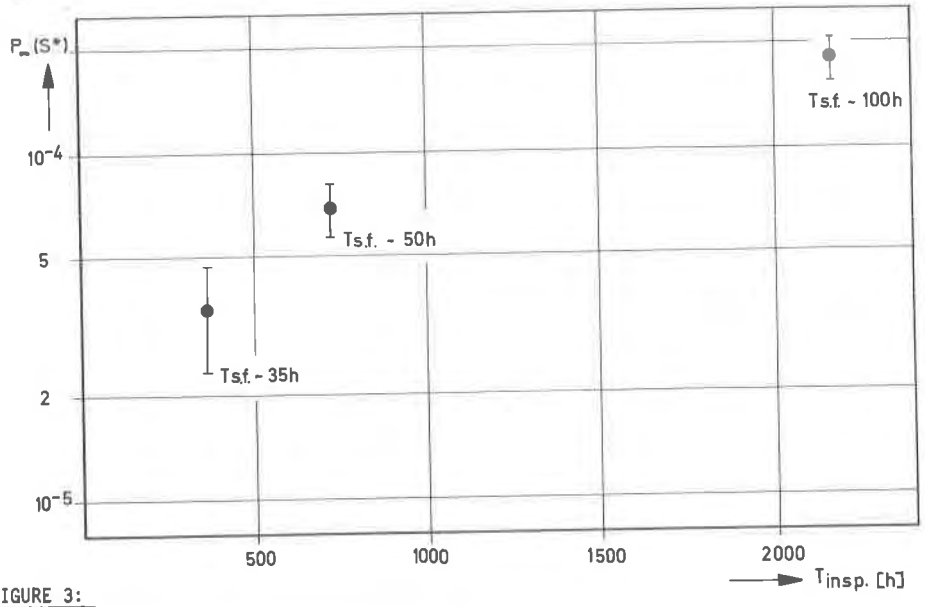


FIGURE 3:

Unavailability $P_{\infty}(S^{*})$ and averaged system's failure time $T_{s.f.}$ depending on different inspection time intervals $T_{insp.}$

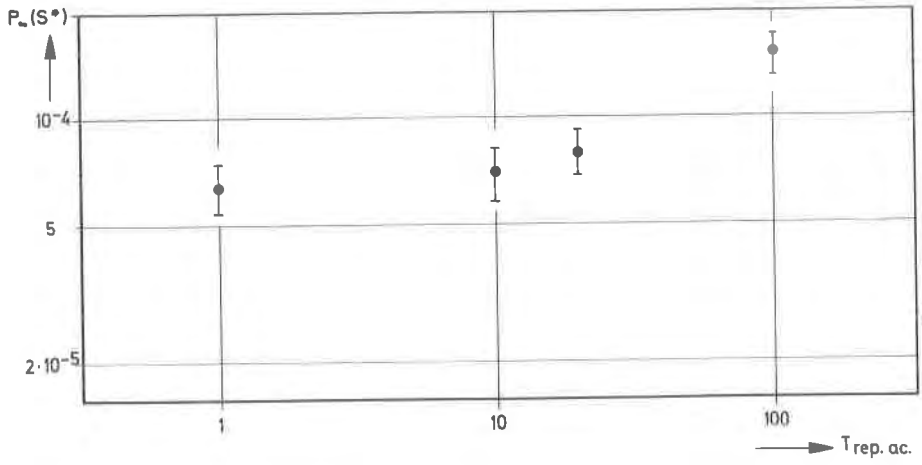


FIGURE 4:

Unavailability $P_{\infty}(S^{*})$ depending on the allowed repair time $T_{rep.ac.}$ for an accumulator.

Table 1

Failure, Inspection and Repair Data

Type of Failure	MTTF [h]	MTTI [h]	MTTR [h]
Check valve fails to open	$2 \cdot 10^6$	720 8760 1)	20
Valve (motor driven)			
- fails to open (to close)	$1 \cdot 10^5$	720	20
Low pressure pump			
- during standby	$6{,}7 \cdot 10^4$	720	40
- during operation	$6{,}7 \cdot 10^4$	-	60
Residual Heat Exchanger	$1{,}7 \cdot 10^4$	-	40
Accumulator	$2 \cdot 10^4$	-	10
Loss of Normal Power			
- coincident w. loss of cool. acc.	0,2 (per demand)		-
- during operation	$5 \cdot 10^4$	-	30
Power Switch			
- fails to open (to close)	$5 \cdot 10^6$	360	5
Diesel generator			
- during standby	$8 \cdot 10^3$	360	75
- during operation	$8 \cdot 10^3$	-	
- starting switching device	$2{,}5 \cdot 10^4$	360	10

MTTF - Mean Time To Failure
MTTI - Mean Time To Inspection
MTTR - Mean Time To Repair

1) Check valves separating the emergency cooling lines from the main coolant system

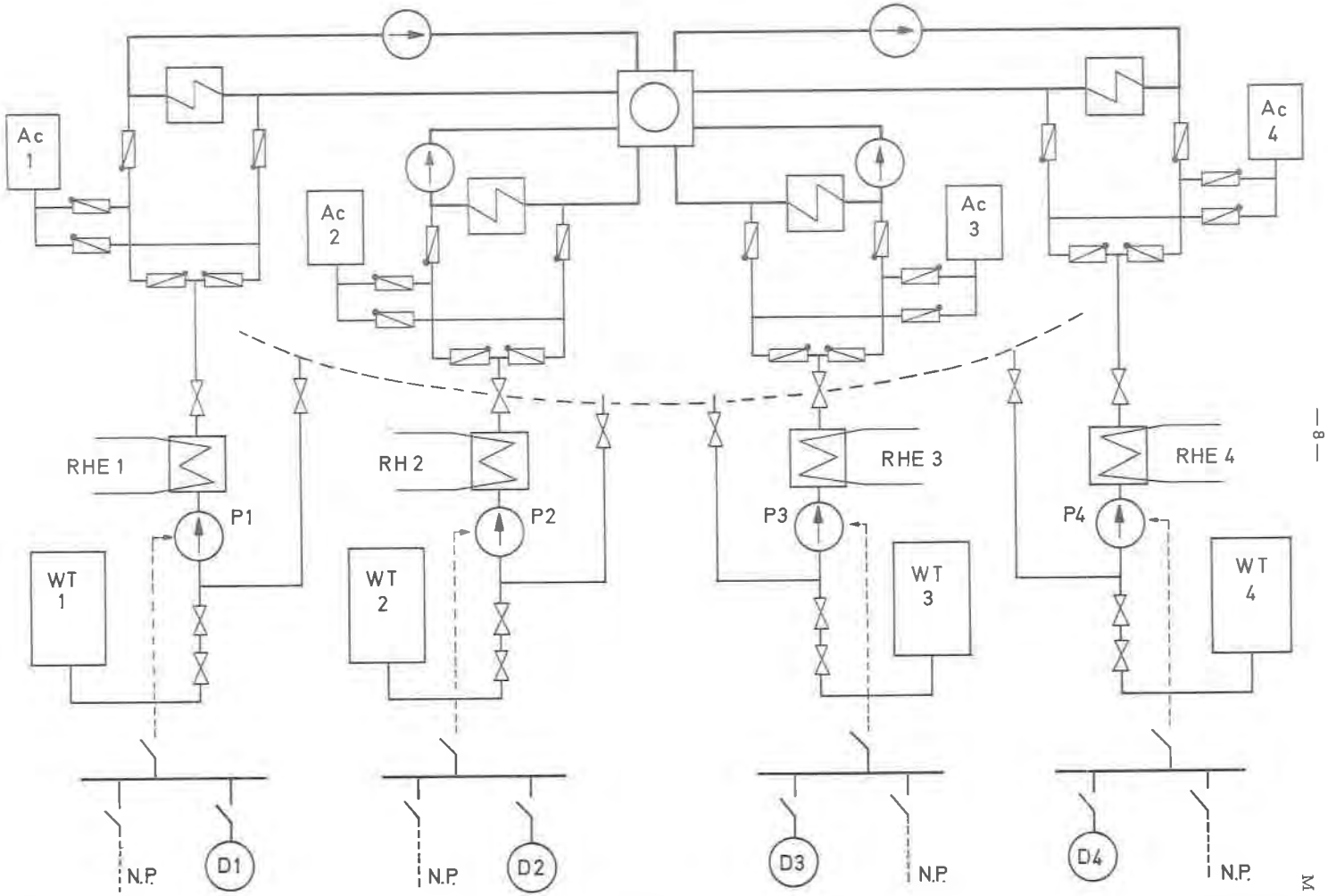


FIGURE 1: Block diagram of the emergency core cooling system.

- the emergency Diesel generators are tested (start-up) every two weeks.

5. Discussion of Results

In the following some influences on the system's failure behaviour will be discussed from the results obtained so far. It should be emphasized that the numerical values of these results, however, can only be considered in connection with the simplified model system that has been analyzed here.

The overall system's failure probability mainly is given by the failure probability per demand, i.e. looking at Equ. (2) $P(S^x)$, the unavailability of the system is the leading term. Taking the reference data set given in Table 1 the stationary value of the unavailability comes out to be $P_\infty(S^x) \sim 7 \cdot 10^{-5}$. Besides $P_\infty(S^x)$ also the averaged system's failure time in case of undetected system's failure in the standby state has been determined by simulation runs as $T_{s.f.} \sim 50$ hours. As has also been proved directly this rather low value of $T_{s.f.}$ indicates that the stationary value of the system's unavailability already is reached some hundred hours after inspection of all components. Concerning the second term of Equ. (2) one has shown that the cumulative failure probability of the system during the heat removal phase (which was accepted to be about 2000 hours) is less than 10^{-6}.

Therefore some calculations have been made to ascertain the influence of inspection on the system's unavailability. The results of this are shown in Fig. 3, giving $P_\infty(S^x)$, the unavailability of the system and $T_{s.f.}$, the averaged system's failure time (during standby) depending on different time intervals for inspection of the low pressure pumps and corresponding valves. The values shown at $T_{insp.} = 720$ hours (1 month) correspond to the reference data set. Although the calculations have been made only for three values of T_{insp} the diagram is a good representation of the change in system's availability and system's failure time depending on a change of inspection time intervals.

Special interest was given to the influence of the repair times allowed for the accumulators. Fig. 4 shows the results of some parameter calculations; there the unavailability of the system $P_\infty(S^x)$ is plotted versus $T_{rep.ac.}$ the allowed repair time for one accumulator. For very short times, say $T_{rep.ac.}$ smaller than 10 hours the accumulators only give a small contribution to system's unavailability, accepting larger values of repair times the influence of the accumulators becomes evident. If one argues however, that the influence of loss of electrical power supply is some what overestimated by the data used here, it becomes obvious that the system's availability is strongly limited by the accumulators, since in this case by lowering the failure probability for loss of power the contribution of all other subsystems decreases sensitively. The effect of this has been shown explicetely by some calculations assuming the probability for loss of coolant accident as parameter. Taking $w = 0.01$ instead of $w = 0.2$ (e.g. considering redundant normal power supply) the system's unavailability then decreases to $P_\infty(S^x) \sim 1.5 \cdot 10^{-5}$.

6. Conclusion

Although the results and their dependencies discussed above are fairly well understood the analysis of the model system presented here only can give some basic relationships and suggestions for detailed investigations of complex systems. In this sense it is the aim of the paper to show how to get a systematic approach for analyzing system's safety requirements with the aid of mathematical reliability methods.

REFERENCES:

[1] Sicherheitskriterien für Kernkraftwerke, IRS-R-2, 1969

[2] HEUSER, F.W., ROSENHAUER, W.:
"SAP-1, Ein neues Programm zur Berechnung von Zuverlässigkeitsgrößen komplexer Systeme", atw, Jg. 17, Nr. 2 (1972)

[3] GREEN, A.E., BOURNE, A.J.:
"Safety Assessment with Reference to Automatic Protective Systems for Nuclear Reactors, Part 3, AHSB (S) R 117 (1966)

[4] GARRICK, B.J., GEKLER, W.C. et al:
"Reliability Analysis of Nuclear Power Plant Protective Systems", HN 190 (1967)

tanks will be exhausted, the operating cooling lines then are switched for supply from the containment sump by closing the valves from the water storage tanks and opening the valves for sump circulation. The required heat removal now is taken over by the residual heat exchangers to the component cooling system and the service water system. The first phase of residual heat removal lasts from 5 to 10 hours. At the end of this phase the residual heat has already decreased to nearly one per cent of the total thermal emergy. For subsequent long-time heat removal thereafter only one of four pumps are needed.

3. Reliability Concept

The overall reliability of the system is determined by two terms contributing to the system's failure probability. To begin with on one hand one has to calculate the system's failure probability considering the system in the standby state, i.e. one determines the failure probability per demand or respectively the unavailability of the system for the case that the system is called upon for operation immediately. On the other hand considering the system after start-up one calculates the cumulative probability of system's failure depending on the operating period required for residual heat removal.

The relationship between both terms can casily be seen analytically. Introducing conditional probabilities the system's failure probability P (S) can be expressed as

$$P(S) = P(S/S^{*}) \cdot P(S^{*}) + P(S/\overline{S^{*}}) \cdot P(\overline{S^{*}}), \qquad (1)$$

where S^{*} stands for "system unavailable" and $\overline{S^{*}}$ for "system available". Since $P(S/S^{*}) = 1$ and $P(\overline{S^{*}}) = 1 - P(S^{*}) \approx 1$, one obtains simply

$$P(S) = P(S^{*}) + P(S/\overline{S^{*}}), \qquad (2)$$

Here the first term gives the unavailability of the system and the second one the system's failure probability during the operating period assuming that the system has been started successfully.

According to the description of the cooling procedure given in section 2 the system's failure probability during the short time period of core flooding is given by the first term of Equ. (2), i.e. the unavailability of the system. This term, of course, also takes into account the switching of the cooling lines for sump circulation. The failure probability of the following short-time operating phase for residual heat removal with two of four pumps can be neglected against the first term, since the operating period of this phase is very small compared with the inspection time intervals of the system during standby. Therefore the second term of Equ. (2) essentially is given by the failure probability related to the long-time phase of residual heat removal performed by only one of four pumps.

4. Fault Tree Analysis

Having outlined the reliability concept now the fault trees belonging to the different phases of emergency core cooling can be evaluated. As an example Fig. 2 is a draft showing the main features of the fault tree for calculating the availability of the system in the emergency case. Hereby one assumes that the loss of coolant accident has occurred in the cold leg of one main coolant line. According to this, water supply for core flooding from one accumulator via the cold leg remains unconsidered, more over, referring to the supply via the hot leg of this line a failure probability for insufficient flooding from this accumulator has been introduced additionally. Dealing with the low pressure injection system it is assumed that a least two of four flooding lines must be available via the hot legs.

Referring to the fault tree of the long-time phase for residual heat removal only the outage of an (1 of 4) - system is considered. According to Equ. (2) however, one has to take care of the condition that the emergency core cooling system already has been available for flooding. This means, although the system as a whole has been successfull, one cannot assume that all components of the system have been available when called upon (e.g. although the system has been ready for start-up, there is a chance that the check valves of one line had failed to open, so that this cooling line is blocked for the operating period). Therefore besides the failure modes referring to components in the operating state (e.g. pump fails operating) the fault tree also includes additional inputs as failure modes per demand (e.g. pump failed to start).

The numerical calculations are performed with the computer programs FESIVAR and SAP [2], using analytical and Monte Carlo simulation methods. The computations take into account failure, inspection and repair of components and failures on demand for switching to different components and subsystems.

Table 1 gives a list of the failure, inspection, and repair data of the main components contained in the model system. The failure rates mainly are taken from literature [3], [4], the reference set of inspection and repair times fairly well corresponds to engineering maintenance. Referring to the inspection data generally there are different time intervals that have been specified with respect to different maintenance and testing procedures or safety requirements for the system:

- the low pressure pumps and all main valves are inspected monthly,
- the check valves separating the emergency cooling lines from the main coolant system, however, are checked only once a year, since inspection of these valves only is made if the reactor is shut down (for testing, the pressure of the reactor system is relieved below the level for starting the high pressure emergency feed pumps),
- the accumulators containing water under pressure can be assumed to be controlled continously,