A Probabilistic Method for Optimization of Fire Safety in Nuclear Power Plants

DIETMAR HOSSER and WOLFGANG SPREY
König und Heunisch, Consulting Engineers
Oskar-Sommer-Strasse 15-17, D-6000 Frankfurt/Main 70, FRG

ABSTRACT

As part of a comprehensive fire safety study for German Nuclear Power Plants*) a probabilistic method for the analysis and optimization of fire safety has been developed. It follows the general line of the American fire hazard analysis, with more or less important modifications in detail. At first, fire event trees in selected critical plant areas are established taking into account active and passive fire protection measures and safety systems endangered by the fire. Failure models for fire protection measures and safety systems are formulated depending on common parameters like time after ignition and fire effects. These dependences are properly taken into account in the analysis of the fire event trees with the help of first-order system reliability theory. In addition to frequencies of fire-induced safety system failures relative weights of event paths, fire protection measures within these paths and parameters of the failure models are calculated as functions of time. Based on these information optimization of fire safety is achieved by modifying primarily event paths, fire protection measures and parameters with the greatest relative weights. This procedure is illustrated using as an example a German 1300 MW PWR reference plant. It is shown that the recommended modifications also reduce the risk to plant personnel and fire damage.

INTRODUCTION

From 1982 to 1984 a comprehensive theoretical and experimental study on fire safety in nuclear power plants /1/ was conducted by several German research institutes. The work was sponsored by the Federal Minister of the Interior (BMI) and was coordinated by the Gesellschaft für Reaktorsicherheit (GRS).

One of the main aims of the study was the development of a method for analysing quantitatively fire hazards in critical plant areas in order to

- compare the fire risk with the risk due to other internal or external events
- detect weak points in fire safety concepts
- reduce fire risk by more efficient combinations of fire safety measures
- make fire safety measures more efficient by influencing the most important parameters.

*) Optimization of fire safety measures and quality control in nuclear power plants. Study SR 144/1, sponsored by the German Federal Minister of the Interior, 1982 - 1984

At the beginning, American methods for fire hazard analysis /2/ and fire risk analysis (e. g. /3, 4 /) were studied. These methods seemed to be less appropriate for German nuclear power plants because

- the German fire safety concept is mainly based on physical separation of systems and less on fire suppression measures
- the fire effects on fire protection measures and safety systems are not explicitly taken into account
- the dependences between single failures due to the time-dependent fire effects are not clearly treated in the event tree analyses.

Therefore, a somewhat modified methodology based on first-order reliability theory was developed consisting of:

- the assessment of time-dependent fire event trees
- the definition of simplified failure models for fire protection measures and safety systems to be used in reliability analyses
- the analysis of the fire event trees with the help of first-order system reliability methods
- the optimization of fire protection measures based on the results of the event tree analyses.

The latter two steps will be illustrated using as an example a German 1300 MW PWR reference plant.

TIME-DEPENDENT FIRE EVENT TREES

The risk-orientated investigations in /1/ started with the selection of areas in a typical German PWR plant, in which potential fire hazards could endanger safety systems or plant personnel. For these areas event sequences induced by the occurrence of an initial fire were established. Similar to /2/ different protective measures are provided to detect and suppress a fire or to limit the effects of a fire on safety sytems and personnel to the compartment affected (Fig. 1). From experience the most probable times of actuation (after ignition) with lower and upper bounds can be estimated for all active fire protection measures.

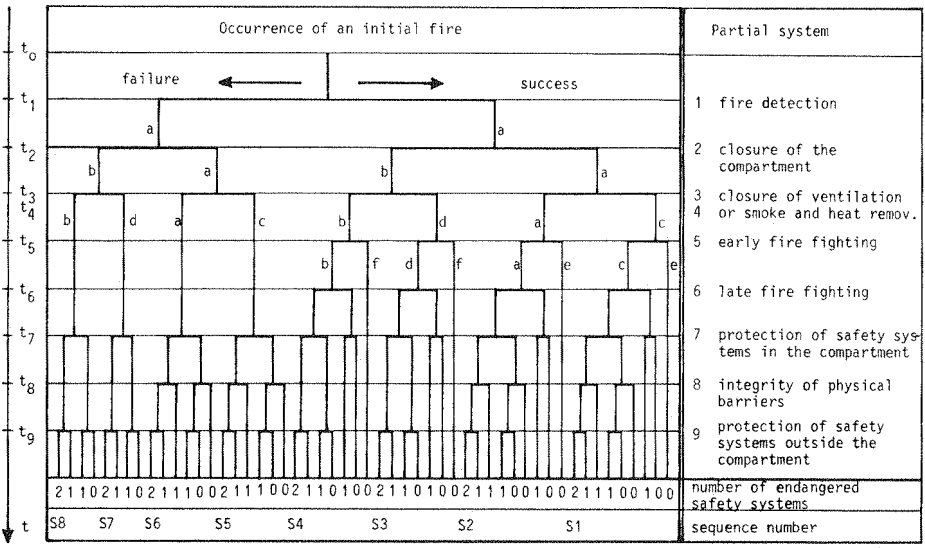

Fig. 1 Time-dependent fire event tree

Depending on success or failure of the active fire protection measures different time-histories of fire effects are expected. In Fig. 2 a set of temperature-time-histories is shown with the following boundary conditions:

curve a - normal conditions, compartment closed, fixed forced ventilation rate, no fire suppression
curve b - at least one door open (higher ventilation rate), no fire suppression
curve c - like a, but ventilation stopped at time t_3
curve d - like b, but ventilation stopped at time t_3
curve e - like a, but fire suppression started at time t_5
curve f - like b, but fire suppression started at time t_5.

If fire suppression measures are properly designed and actuated in due time the temperature decrease is so fast that curves e and f can be neglected in the analysis of consequences.

One of the above mentioned temperature-time-histories is assigned to each branch of the event tree in Fig. 1. Depending on the respective temperature at the time of demand failures of fire protection measures or safety systems due to fire can occur. Therefore, the consequences of a fire in a plant area depend on time, too. In the analysis of the event tree the frequencies of critical consequences, e. g. failure of one redundancy of safety systems in the fire compartment and failure of a physical barrier between two compartments and failure of a second redundancy in the adjacent compartment, are checked at varying time steps t*.

FAILURE MODELS FOR FIRE PROTECTION MEASURES AND SAFETY SYSTEMS

In order to account for dependences due to the time-dependent fire effects the single failures are described with the help of simplified mechanical models. The models are constructed as follows:

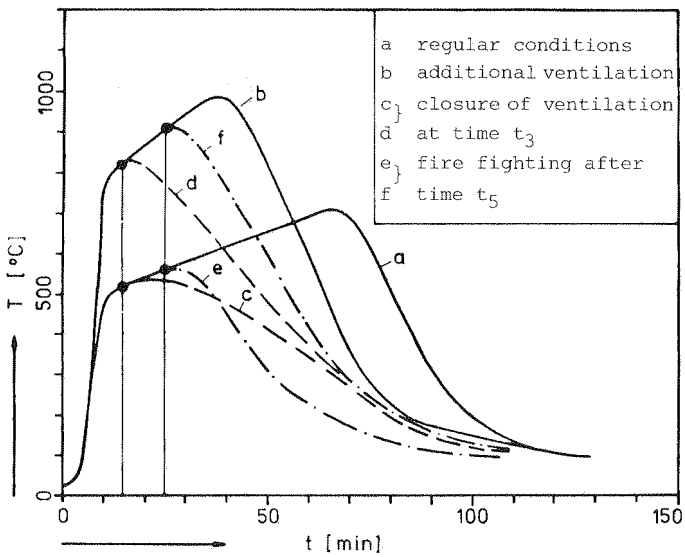

Fig. 2 Typical temperature-time-histories in NPP compartments

The active fire protection measures are divided in 6 "partial systems" as indicated in Fig. 1:

- fire detection and alarm
- closure of openings in the compartment boundary
- closure or shut down of compartment ventilation
- removal of smoke and heat
- early fire fighting inside the compartment
- late fire fighting from outside the compartment.

These partial systems are composed of "components" which act in parallel or series arrangements. The failure frequencies of the partial systems can be derived from failure rates of the components using fault tree models (e.g. Fig. 3).

Failure rates of the "components" are only partly known from statistical data. Especially, the portion of failures due to fire or late actuation is not sufficiently well covered by data. Therefore, simplified limit-state models are formulated and treated with the help of first-order reliability theory. For the partial system "early fire fighting" shown in Fig. 3, the limit-state functions are as follows:

$p_{51} = P\{Z_{51} \leqq -\beta_{51}\}$

β_{51} = standardized Gaussian variable calibrated with statistical data for p_{51}

$p_{52} = P\{Z_{52} \leqq -\beta_{52}\}$

β_{52} = analogical to β_{51}

$p_{53} = P\{Z_{53} \leqq T_{RM} - T(t_5)\}$

T_{RM} = ultimate temperature (°C) for manual fire suppression

$T(t_5)$ = gas temperature (°C) at time t_5

$t_5 = t_1 + \Delta t_5$

= time of fire detection + delay from detection to arrival of fire emissary

$p_{54} = P\{Z_{54} \leqq -\beta_{54}\}$

β_{54} = analogical to β_{51}

$p_{55} = P\{Z_{55} \leqq T_{RL} - T(t_5)\}$

T_{RL} = ultimate temperature (°C) for fire suppression system

$p_{56} = P\{Z_{56} \leqq -\beta_{56}\}$

β_{56} = analogical to β_{51}

$p_{57} = P\{Z_{57} \leqq t^* - t_5 - \Delta t_5^*\}$

t^* = varying time for checking the consequences

Δt_5^*= duration of fire fighting until success.

The failure frequencies of passive fire protection measures (physical barriers) and safety systems depend strongly on fire effects, especially on gas temperature, which are functions of the time after occurrence of the initial

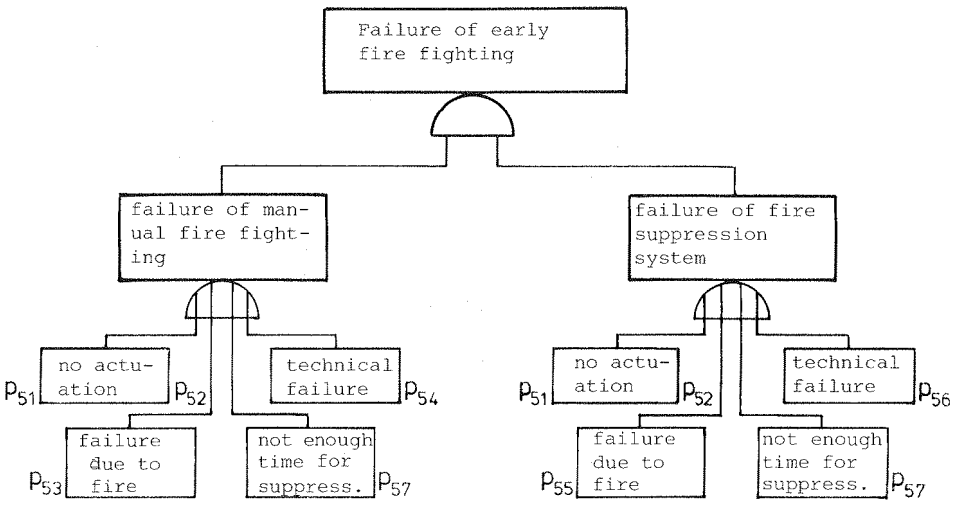

Fig. 3 Fault tree for failure of early fire fighting within the compartment

fire. For safety systems (mechanical and electrical components) ultimate gas temperatures have to be specified during design, based on fire test or experience. Passive fire protection measures are usually tested in standard fire tests, e. g. in Germany according to DIN 4102 /6/. The fire resistance of these measures does not only depend on the gas temperature but also on the time of action of the temperature; therefore, the time-integral of the standard fire curve up to the fire resistance time is taken as ultimate limit of fire resistance. In /1/ it was shown that this ultimate limit is valid not only for standard fires but also for natural fires in the compartments under consideration (cf. /7/).

All limit-state definitions used for the "components" of active fire protection measures as well as for passive fire protection measures and safety systems are summarized in Tab. 1. The parameters influencing the limit-states are random variables which are described by distribution parameters (cf. Tab. 2). The limit-states are dependent, due to common parameters.

SYSTEM RELIABILITY ANALYSIS

The fire event tree in Fig. 1 can be treated like a technical system consisting of the different event sequences with the same consequence in series arrangement. Within each event sequence the partial systems according to the preceding section are arranged in parallel. Finally, the partial systems act as parallel or series system with several "components". The state of the overall system can be formulated with the help of Boolean algebra. Alternatively, the system state can be directly related to the states of the individual "components" or it can be determined indirectly using intermediate systems (i. e. event sequences) or partial systems as a kind of macro-components.

In the following, mainly the second "subsystem method" is used because of its advantages with respect to calculation effort and interpretation of the results. Because of the above mentioned dependences between some of the single components the classical methods for fault tree and event tree analysis are not

Tab. 1 Limit-states of the event tree in Fig. 1

limit state				partial system	
no.	name	failure for $Z_i \leq 0$	fire curve	no.	function
1	Z_{11}	no manual direct fire detection			
2	Z_{12}	no automatic fire detection			
3	Z_{13}	no manual indirect fire detection		1	fire detection
4	Z_{14}	no automatic indirect fire detection			
5	Z_{15}	no indirect fire detection through failure of components			
6	Z_{21}	Opening in physical separation not closed			
7	Z_{22}	no automatic closure		2	physical separation of the compartment
8	Z_{23}	technical failure			
9	Z_{24}	no manual closure			
10	Z_{31}	no closure of the air ventilation through personnel			
11	Z_{32}	no closure of the air ventilation through fire emissary			
12	Z_{33}	no closure of the air ventilation from the control room			
13	Z_{34a}	no automatic closure of the air ventilation	a	3	closure of the air ventilation
14	Z_{34b}		b		
15	Z_{35}	technical failure			
16	Z_{41}	no actuation of smoke and heat removal system by personnel			
17	Z_{42}	no actuation of smoke and heat removal system by fire emissary		4	smoke and heat removal
18	Z_{43}	no switch over of the air ventilation			
19	Z_{44}	technical failure			
20	Z_{51}	no early fire fighting through personnel			
21	Z_{52}	no early fire fighting through fire emissary			
22	Z_{53a}	failure of manual fire fighting due to fire	a		
23	Z_{53b}		b		
24	Z_{53c}		c		
25	Z_{53d}		d	5	early fire fighting in the compartment
26	Z_{54}	technical failure of the manual fire fighting			
27	Z_{55a}	failure of the fire suppression system due to fire	a		
28	Z_{55b}		b		
29	Z_{55c}		c		
30	Z_{55d}		d		
31	Z_{56}	technical failure of the fire suppression system			
32	Z_{57}	not enough time for fire suppression			
33	Z_{61}	not enough time for late fire fighting		6	late fire fighting from outside the compartment
34	Z_{64}	technical failure			
35	Z_{71a}	failure of safety systems in the compartment	a		
36	Z_{71b}	due to fire effects	b	7	protection of safety systems in the compartment
37	Z_{71c}		c		
38	Z_{71d}		d		
39	Z_{81a}	failure of physical barriers due to fire effects	a		
40	Z_{81b}		b	8	integrity of physical barriers
41	Z_{81c}		c		
42	Z_{81d}		d		
43	Z_{91a}	failure of safety systems in an adjacent compartment due to fire effects	a		
44	Z_{91b}		b	9	protection of safety systems in an adjacent compartment
45	Z_{91c}		c		
46	Z_{91d}		d		
47	Z_{92}	late fire spread to an adjacent compartment or redundancy			

applicable; i. e. the frequencies of the overall system states cannot be calculated by multiplying (for intersections) or summing up (for unions) the component or macro-component state frequencies. Therefore, first-order system reliability methods are used which are based on proposals in /7-10/. Only very few aspects of these methods can be discussed here.

As shown before, the states of all single components are described by state functions Z_i (cf. Tab. 1) where

$Z_i \leq 0$: failure of the component

$Z_i > 0$: success of the component.

Tab. 2 Random basic variables for the limit-states of Tab. 1

Random variables		
no.	name	significations
1	p_{11}	failure probability of personnel in the compartment
2	p_{12}	failure probability of automatic alarm in the compartment
3	p_{13}	failure probability of personnel in adjacent compartments
4	p_{14}	failure probability of automatic alarm in adjacent compartments
5	p_{15}	probability of not recognizing component failures
6	p_{21}	probability of physical separations being not closed
7	p_{22}	failure probability of automatic closure
8	p_{23}	probability of a technical failure
9	p_{32}	probability of air ventilation being not closed by the fire emissary
10	p_{33}	failure probability of actuation from the control room
11	p_{35}	probability of smoke and heat removal system not being actuated by personnel
12	p_{42}	probability of smoke and heat removal system not being actuated by f. emissary
13	p_{43}	probability of air ventilation not being switched over
14	p_{44}	probability of technical failure
15	p_{54}	failure probability of manual fire fighting equipment
16	p_{56}	failure probability of fire suppression system
17	p_{62}	failure probability of equipment for indirect fire suppression
18	T_S	actuation temperature of solder
19	ΔT_A	temperature difference between compartment and exhaust air duct
20	ΔT_Z	temperature difference between compartment and supply air duct
21	ΔT_{KN}	temperature difference between compartment and safety system in adjacent area
22	T_{KM}	ultimate temperature of the manual fire fighting
23	T_{RL}	ultimate temperature of the fire suppression system
24	T_{RK}	ultimate temperature of safety systems in the compartment
25	T_{RKN}	ultimate temperature of safety systems in the adjacent compartment
26	$\int T\,dt$	temperature capacity of the physical barriers
27	T_{10}	parameters to describe the temperature-time-history a
28	a_1	
29	a_{A1}	
30	α_{A1}	
31	t_{A1}	
32	T_{20}	parameters to describe the temperature-time-history b
33	a_2	
34	a_{A2}	
35	α_{A2}	
36	t_{A2}	
37	a_{A3}	- " - c
38	α_{A3}	
39	a_{A4}	- " - d
40	α_{A4}	
41	t_i	time of fire alarm
42	Δt_3	delay from alarm to closure of air ventilation (arrival of fire emissary)
43	Δt_4	delay from alarm to actuation of the smoke and heat removal system
44	Δt_5	delay from alarm to actuation of fire fighting
45	Δt_5^*	duration of fire fighting until successful suppression
46	Δt_6	delay from direct to indirect fire fighting
47	Δt_6^*	duration of indirect fire fighting
48	t_W	delay from initial fire to fire spread into an adjacent area
49	t^*	varying time for checking the consequences of the fire

If Z_i is a function of a parameter vector $\underline{X}$ according to Fig. 4 and each parameter is known with its probability distribution, then e. g. the probability of component failure

$$p_{fi} = P\ (Z_i\ (\underline{X}) \leq 0) \qquad (1)$$

can be calculated by a first-order reliability method. The basic principle of the applied method is to transform the limit-state Z_i into a linear function of uncorrelated standardized Gaussian variables. Then the probability distribution Φ_{Zi} is standardized Gaussian, too and can easily be determined; the probability of failure is $\Phi_{Zi}\ (Z_i = -\beta_i)$ where β_i is the so-called safety index. The contributions of the random variations of the parameters $\underline{X}_i$ to the safety index β_i are given by so-called weighting factors α_{Xi} which are calculated during linearization of the limit-state following an idea in /8/.

The weighting factors $\alpha_{\underline{X}_i}$ are an appropriate means for identifying the re-

lative importance of the parameters $\underline{X}_i$ for a limit-state under consideration. They help also to evaluate the degree of correlation between two limit-states Z_i and Z_j with commom parameters $\underline{X}$ because the correlation coefficient ρ_{ij} is simply

$$\rho_{ij} = \sum_{k=1}^{n} \alpha_{ik} \cdot \alpha_{jk} \qquad (2)$$

Now, the conditions for system analysis are as follows:

- All components of the system are described by state functions Z_i.
- The safety indices β_i and the weighting factors $\alpha_{\underline{X}_i}$ have been calculated separately for each limit-state
- The correlation coefficients ρ_{ij} for each couple of two limit-states Z_i and Z_j are determined with Eq. (3)
- The states of the partial systems with components in parallel and series arrangement have to be analyzed as intersections and unions of correlated component states, e. g. for failure F_5 of partial system no. 5 "early fire fighting" according to Fig. 3:

$$F_5 = \{(Z_{51} \leqq 0) \cup (Z_{52} \leqq 0) \cup (Z_{53} \leqq 0) \cup (Z_{54} \leqq 0) \cup (Z_{57} \leqq 0)\}$$

$$\cap \{(Z_{51} \leqq 0) \cup (Z_{52} \leqq 0) \cup (Z_{55} \leqq 0) \cup (Z_{56} \leqq 0) \cup (Z_{57} \leqq 0)\}$$

- The state of the overall system has to be evaluated as intersection of the states of different event sequences defined as unions of the states of the correlated partial systems, e. g. for the consequence "loss of two redundancies of safety systems" according to Fig. 1:

$$F = \{S1 \cup S2 \cup S3 \cup \ldots \cup S8\}$$

with

$$S1 = \{\bar{F}_1 \cap \bar{F}_2 \cap \bar{F}_3 \cap F_5 \cap F_6 \cap F_7 \cap F_8 \cap F_9\}$$

To analyze the state probabilities approximate solutions of the multinormal probability integral on the basis of / 9/ for intersections and /10/ for unions are applied. By using equivalent linearizations according to / 7/ for partial systems, intermediate systems and the overall system , equivalent safety indices and equivalent weighting factors can be evaluated for all these systems. These values are very helpful for interpreting the results of such complex system analyses.

OPTIMIZATION OF FIRE PROTECTION MEASURES

The optimization of fire protection measures and quality controls in nuclear power plants can have different aims, e. g.:

- minimization of the total of construction cost, control and maintenance cost and damage cost for a given fire safety level
- minimization of the frequency of fire-induced consequences for given total cost
- reduction of the frequency of fire-induced consequences with the help of more effective fire protection measures.

Since the information on the different cost contributions was very poor the more pragmatic third aim was chosen for the optimization in /1/. A good basis for the assessment of fire protection measures are the results of the system reliability analyses. They show clearly

- which plant area is critical with respect to the consequences of a fire for reactor safety, plant personnel or plant operation

- which protective measures really reduce the frequency of the consequences or limit the damage cost
- which parameter has the greatest influence on the efficiency of the most important protective measures.

The fire safety level in uncritical plant areas should be chosen according to conventional requirements. In critical areas a higher fire safety level seems to be reasonable in order to minimize the consequences of a fire. Fire protection measures which are expensive but unreliable should be avoided. Also protective measures without any influence on frequency or extend of consequences are unreasonable. The best way to increase the efficiency of fire protection measures is by variation of parameters with the greatest relative weight.

APPLICATION TO A REFERENCE PLANT

The methods described in the preceding sections were applied in /1/ to a German 1300 MW PWR reference plant in order i) to demonstrate the efficiency of the methodology, ii) to check the completeness of the available input data and to study the influence of uncertain data, iii) to assess the fire safety concept and identify relative weak points and iv) to derive recommendations for the optimization of fire protection measures and related quality controls.

For all selected plant areas the frequencies p_f of critical fire-induced consequences were calculated as functions of time after occurrence of the initial fire. In most cases exists a maximum of p_f indicating the most critical situation during a fire. The decrease of p_f after the maximum results either from the cooling phase of the fire or from the effect of fire suppression; the closure of the air ventilation has no influence because of the unreliable actuation. Beside the frequency p_f also the time-dependent squared weighting factors α_i^2 (equivalent values related to the overall system) were determined. For illustration, the frequency p_f and weighting factors α_i^2 from the analysis of the area of the main cooling pumps in the reactor building containment are depicted in Fig. 4. The main impact of the fire on safety systems comes from fire-induced failures of electrical equipment. Only the "regular" temperature-time-history a is of interest. The most critical situation is reached in an early stage of the fire when fire fighting by the fire suppression system is not yet manually actuated.

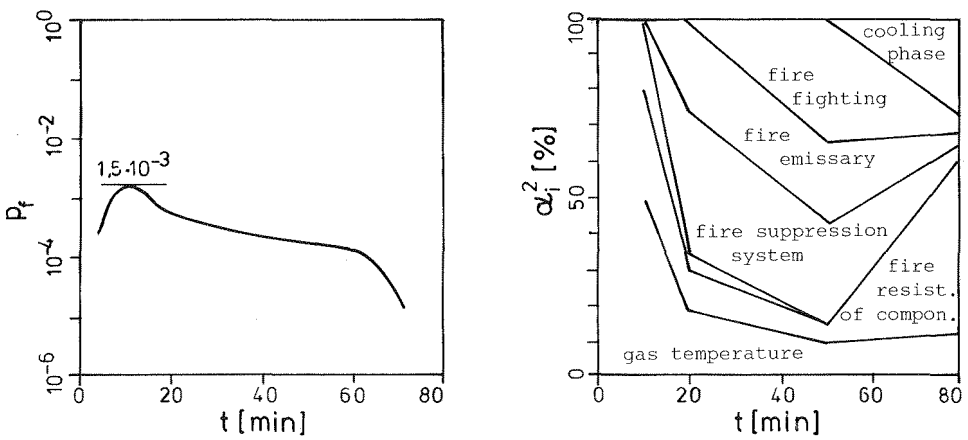

Fig. 4 Time-dependent frequency p_f and squared weighting factors α_i^2 of parameters for the event "fire-induced loss of the main cooling pumps"

Important parameters at this stage are the gas temperature and the ultimate temperature of the electrical equipment in this area. About 10 min. after the occurrence of the initial fire the early fire fighting by the suppression system becomes effective and p_f is reduced. Further reductions of p_f come from the effect of the late fire fighting and the beginning of the cooling phase of the fire. As the failure of the electrical equipment of all main cooling pumps is to be expected at an early time, the only way to reduce the failure frequency p_f is to actuate immediately the fire suppression system, either manually from the control room after checking the situation by TV monitors or automatically by fire detectors. Such a modification would also reduce the risk to plant personnel and limit the damage due to spreading corrosive smoke.

CONCLUSIONS

A probabilistic method for the quantitative evaluation of fire hazards in nuclear power installations has been developed. It is based on fire event sequences which depend on success or failure of different active or passive fire protection measures. Single failures of these measures and of safety systems endangered by a fire are dependent events due to the common influence of the fire effects. With the help of a first-order reliability method the dependences can be modelled and properly taken into account in the event tree analysis. Beside frequencies of undesired consequences of event sequences, relative weights of event sequences, fire protection measures and parameters influencing the measures are determined. Based on such information weak points in fire safety concepts can easily be identified and optimal combinations of fire protection measures for a required fire safety level can be recommended.

REFERENCES

/1/ ABK/GRS: Optimization of fire safety measures and quality control in nuclear power plants. Final report of the research project SR 144/1 sponsored by the Federal Minister of the Interior. December 1984 (in German).

/2/ Berry, D. L. and E. E. Minor: Nuclear Power Plant Fire Protection - Fire Hazard Analysis (Subsystems Study Task 4). NUREG/CR-0654, September 1979.

/3/ Fleming, K. N., W. J. Houghton, F. P. Scarletta: A Methodology for Risk Assessment of Major Fires and its Application to a HTGR Plant. General Atomic Company, July 1979.

/4/ Gallucci, R. and R. Hockenbury: Fire-induced Loss of Nuclear Power Plant Safety Functions. Nuclear Engineering and Design 64 (1981), 135 - 147.

/5/ DIN 4102: Brandverhalten von Baustoffen und Bauteilen; Teil 2: Bauteile, Begriffe, Anforderungen und Prüfungen. Ausgabe September 1977.

/6/ Schneider, U. und D. Hosser: Reliability based Design of Structural Members. First International Symposium on Fire Safety Science. Gaithersburg, MD (USA), October 9 - 11, 1985.

/7/ Hohenbichler, M. and R. Rackwitz: First-Order Concepts in System Reliability. Structural Safety 1 (1983).

/8/ Hasofer, A. M. and N. C. Lind: An Exact and Invariant First-Order Reliability Format. Journal Eng. Mech., ASCE, 100, EM1, 1974.

/9/ Breitung, K.: An Asymptotic Formula for the Failure Probability. EUROMECH 155, Kopenhagen, 15 - 17 Juni 1982.

/10/ Hohenbichler, M.: Approximate Evaluation of the Multinormal Distribution Function. Berichte zur Zuverlässigkeitstheorie der Bauwerke, Technische Universität München, Heft 58, 1981.