FR8201019

ANS - ENS - International ANS/ENS topical meeting on
probabilistic risk assessment.
Port-Chester, N.Y., USA, September 20 - 24, 1981.
CEA - CONF 5995

PROGRESS IN METHODOLOGY FOR PROBABILISTIC ASSESSMENT OF ACCIDENTS : TIMING OF ACCIDENT SEQUENCES

J.M. LANORE[1], C. VILLEROUX[1], F. BOUSCATIE[1]
N. MAIGRET[2]

([1]) CEA - IPSN, B.P. n°6, 92260 Fontenay-aux-Roses (France)

([2]) CEA - DEDR, CEN Saclay, 91191 Gif-sur-Yvette (France)

ABSTRACT

There is an important problem for probabilistic studies of accident sequences using the current event tree techniques. Indeed this method does not take into account the dependence in time of the real accident scenarios, involving the random behaviour of the systems (lack or delay in intervention, partial failures, repair, operator actions ...) and the correlated evolution of the physical parameters.

A powerful method to perform the probabilistic treatment of these complex sequences (dynamic evolution of systems and associated physics) is Monte-Carlo simulation, very rare events being treated with the help of suitable weighting and biasing techniques.

As a practical example the accident sequences related to the loss of the residual heat removal system in a fast breeder reactor has been treated with that method.

INTRODUCTION

This paper describes a methodology developed to treat the accident sequences in a more realistic way than the current event tree method. Indeed the event tree is a static technique which cannot take into account the time dependent behaviour of the systems during the accident evolution (repairs, operator actions, delays, partial failures...).

The method described here is a treatment of the installation as a whole, based on its operational states, the transitions between states, and the corre-

lated evolution of physical parameters. Quantification requires a Monte-Carlo method and the Response Surface technique.

As an example, the accident sequences related to the loss of the residual heat removal system in a fast breeder reactor are analysed according to that method.

METHODOLOGY

Event Tree Method

To perform a risk assessment, that is in particular to assess the probability of an undesired event, the current method developed in the RSS study, is the use of the event tree technique. This technique is briefly summarized :

- Identification of initiating events.
- From each one, construction of a tree according to the operability of the safeguard systems.
- Analysis of the consequences along each branch.
- Probability evaluation for the branches leading to unacceptable consequences (Figure 1).

This scheme is convenient when the safeguard systems may have only two states (running or not) and when the different sequences (branches of the tree) are independent.

However in several cases this state treatment is inadequate to represent the real phenomena. For instance it is impossible to take into account the time-dependent behaviour of the systems during the accident evolution involving repairs, delays, operator intervention, or partial failures. The resulting sequences are no more a tree branch, but a complex path with several backward connections. Similar difficulties arise when the safeguard systems are not in stand-by but in continuous functioning, or when interrelations exist between these systems.

To deal with these situations important difficulties arise, indeed there is then a lot of possible sequences with correlations between the different paths. The consequences depend on the particular path and on the time needed to follow it.

It is no more possible to treat a limited number of scenarios defined *a priori*. A whole treatment becomes necessary where the time is a fundamental parameter.

States Representation

We intend to represent the functionnement of the safeguard systems not by an event tree but by a list of operational states for the whole installation. Each state is a combination of the individual systems state (stand-by, running, total or partial failure ...).

Transitions exist between the states, with probability laws (failure or repair laws versus time, probability of operator action ...). These laws may depend on other parameters like physics, absolute time, etc... (Figure 1).

For each state there are corresponding laws for physical parameters evolution.

The unacceptable consequences are characterized by a critical value for one or several physical parameters.

In such a scheme an accident sequence is a more or less complex path, going through different states and along which a critical threshold is reached. The path starts by the state (or the states, with the corresponding probabilities) in which the system is found when the initiating event appears.

From these initiating events and according to all the transition laws, a overall probability of reaching a critical threshold will be assessed. It will be then possible to determine *a posteriori* the paths which gave the more important contribution to this probability that is the more dangerous accident sequences.

QUANTIFICATION

Method

The method to use will depend on the specific problem since it depends on the transition and physic laws. In some cases the system can be a markovian or semi-markovian one, where analytical solution can be obtained.

In the most general case, a very powerfull tool is Monte-Carlo simulation. Indeed the great flexibility of this method enables it to take into account very complex laws and conditions encountered in some realistic problems.

The principle of calculations is to build by random sampling a very large number of event sequences (of paths from state to state) according to the transition laws. During each sequence it is possible to calculate the physical parameters evolution and to check if a criterion is reached.

The searched for probability can be assessed by counting the number of sequences leading to the unacceptable criterion.

Limitation of Computing Time

In principle a Monte-Carlo method is able to deal with practically any situation. However the computing time may be a prohibitive limitation.

In the present problem the computing time may be very large for two reasons :
- each sequence (or history) is time consuming because it needs a physical calculation for which complex models are often necessary ;

- the searched for probabilities are very low, so a very large number of histories must be simulated to obtain a sufficient number of contributions to the result (a reasonable variance).

Two interesting techniques can be used to reduce the computing time :
- The Response Surface Method : the time consuming physical code is replaced by an analytical formula fitted to a limited number of exact calculations.
- The biasing and weighting technique for Monte-Carlo simulations : for the random samplings the real transition probabilities are replaced by biased ones, in order to favour the interesting histories (those which contribute to the result), the bias being corrected by a weight. If at time t the system is in state i, the weight w(t) must verify

$$w(t) = \frac{P_i(t)}{P_i^*(t)}$$

when $P_i(t)$ is the probability to be in state i at time t with the real transition laws, and $P_i^*(t)$ the probability with the biased laws.

With a suitable choice for the biased transitions, this technique may be very powerfull, and can deal with even very low probabilities.

By using these two techniques the simulation becomes perfectly manageable, and the practical examples treated showed that quite complex problems can be satisfactorily solved with very low computation times.

EXAMPLE. ASSESSMENT OF THE LOSS OF RESIDUAL HEAT REMOVAL FUNCTION

As an illustration of this methodology, a study is presented on the accident sequences related to the loss of the residual heat removal function of the fast breeder reactor Phenix.

Indeed, due to the important thermal inertia of the sodium cooled reactors, a treatment where the repair possibilities are not taken into account would be quite unrealistic. Moreover the systems involved in this function are also in service during normal reactor operation, and their failures are themselves initiating events for accident sequences. This case is then a typical application for the method presented here.

Systems Description

The example is presented as an illustration of a method, and not as a detailed study of a system. So a simplified description is just given, more complete informations are available in refs. [1,2].

Two distinct systems remove the residual heat from the reactor :
- The secondary cooling system : three sodium loops transfer decay heat to the steam generators, which are cooled by natural air convection. It is assumed that

the secundary loops are effective only during forced (pumped) circulation of the sodium.
Electrical power for main and auxiliary motors of the secondary pumps is supplied by two off-site lines and two emergency diesel generators. An additional air-cooled diesel generator can supply power to the auxiliary motors.
- The emergency cooling system : two cooling-circuits where treated water is circulated remove heat from the safety vessel and transfer it to raw water by heat exchanger. Upon loss of normal water supply, the circuits can be placed in some of their alternative coolant configurations (raw, industrial or fire-fighting water). The re-configuration does not require use of electric power (actuating of valves only).

States and Transitions

The twelve possible states are characterized by the number of secundary loops (3, 2, 1, 0) and of emergency circuits (2, 1, 0) operating.

Detailed analysis of the systems provided the equivalent transition laws between states and the associated numerical values.

- Single transitions :

. mechanical failure or leak on a secundary loop (which necessitates emptying the loop)

$\lambda = 3.3\ 10^{-4}/h$ $\quad 1/\mu = 24$ h

. mechanical failure of an emergency circuit

$\lambda = 3\ 10^{-8}/h$ no repair

- Common mode transitions :

. loss of the three secundary loops (sodium fire)

$\lambda = 10^{-6}/h$ no repair

. loss of normal water supply of emergency circuits by common mode failure

$\lambda = 10^{-9}/h$ no repair
and failure of re-configuration for an alternative supply

$\lambda = 2\ 10^{-7}/h$ no repair

. loss of electrical power supply (off-site lines and emergency diesel generators)

$\lambda = 3\ 10^{-9}/h$ $\quad 1/\mu = 20$ h
which leads to the loss of the three secundary loops upon failure of the air-cooled diesel

$\gamma = 0.1$ $\quad 1/\mu = 80$ h
and to the loss of emergency cooling system upon failure of re-configuration
$\lambda = 2\ 10^{-7}/h$ no repair

Initiating Events and Sequences

An initiating event is an event causing a shutdown of the reactor.

In our problem two types of events must be considered :
- shutdowns for a cause external to the heat removal system (scheduled shutdowns, problems on the steam circuit, etc...) ;
- shutdowns due to partial failures of the systems.

The initial state of a sequence is the state of the system when a shutdown occurs, that is :
- for the external initiating events, the normal operating states of the reactor (according to the operation procedures) ;
- for the internal initiating events, the states for which a shutdown is required.

Schematically the probability of an accident sequence resulting in failure of the function can be divided into three terms :

$$P = P_1 \times P_2 \times P_3$$

P_1 = probability for the system to be in one of the operating states, or to fall in a state requiring a shutdown (during the whole life-time of the reactor).

P_2 = probability of observing a shutdown in the considered state - For internal events $P_2 = 1$.

P_3 = starting from each state, conditional probability of function failure, that is probability to reach a physical threshold during the time of residual heat decay.

Physical Criterion

The safety criterion used in this analysis to indicate the failure of the function is the temperature of the primary sodium. This temperature must not exceed $T_c = 750°C$ to limit the risk of creep in the main vessel. So the only physical parameter to assess is the primary sodium temperature versus time t :

In the state i : $T_i(T_o, t_o, t)$

with the criteria $T_i \leq T_c$

T_o = temperature at the time t_o when the system reaches state i.

t_o and t are counted from the time of the reactor shutdown.

Some preliminary calculations showed that some simplifications are possible:
- The parameter T_c can be replaced by the parameter τ_c (available time before reaching the limiting temperature value). For the state i : $\tau_i^c(T_o, t_o)$ and the criterion becomes $\tau_i \leq \tau_i^c(T_o, t_o)$.

- The temperature criterion can be reached only in the 12th state (state with total failure of the five elementary systems) and τ_{12} does not depend much on the value of T_o. So, fixing T_o in a conservative way, the only parameter used is the time τ_{12} elapsed in the state 12 with the criterion :

$$\tau_{12} \leq \tau_{12}^{c}(t_o)$$

An analytical formula for $\tau_{12}^{c}(t_o)$ can be obtained from a fit to exact calculations (a simplified response surface for this problem with a single parameter)

Calculation

30 years of the reactor life were simulated, in each history, by a Monte-Carlo method, starting from a state in which all systems are operating and treating the different failures, repairs, and reactor shutdowns, according to the transition laws described above. The failure probability of the function being very low, an efficient biasing system had to be used : Biased values for the λ_i and γ_i were used to build the histories, and exact expressions of the weight w(t) were assessed according to the real and biased transition laws. Results could then be obtained with a small variance in a very limited computing time.

This type of calculation gives together the overall failure probability of the function, and by analysing the different histories the relative contributions of the possible paths to the result.

Results

The yearly failure probability for the residual heat removal system is found to be

2.10^{-8}/year .

Besides, the study provides informations about the relative weights of the risk components which are perhaps even more interesting.

Initiating events external to the system : P_{ex} being the annual probability of a shutdown for a cause external to the system, the failure probability of the function is $10^{-12} \times P_{ex}$/year.
The statistics on reactor operation give a value of $P_{ex} = 20$/year. So the contribution of the initiating events external to the system is very low : 2.10^{-11}/year.
The risk is essentially related to failures of the system itself during operation.

- Internal initiating events :

In order of importance, the sequences contributing most are :

S.E. (45 h) + D + V	$.7\ 10^{-8}$
US1 + US2 + BS	$.4\ 10^{-8}$
US1 + BS + US2	$.3\ 10^{-8}$
BS + S.E. (2 h) + V	$1.6\ 10^{-9}$
BS + US + V	$1.3\ 10^{-9}$

with S.E.(t) loss of electrical power supply during a time longer than t.
BS loss of the 3 secundary loops by common mode failure.
US1,US2 mechanical failure of the emergency cooling circuits.
US common mode failure of the emergency cooling circuits.

V failure of re-configuration of these circuits.
D failure upon demand of the air-cooled diesel generator.

The paths involving mechanical failures of the secondary loop have a negligible contribution (possibility of repair).

This study points out clearly the weak points of the installation,
- for the systems (electrical power, common mode failure of the secundary loop),
- for the operating procedures (the allowed operation with two loops out of three has a negligible contribution to the total risk, while operation with a failed emergency circuit leads to paths with a more important risk).

CONCLUSION

In order to treat the accident sequences in a more realistic manner, a methodology is proposed involving a overall treatment of the installation based on its functional states, the transitions between states, and the correlated evolution of physical parameters.

The main advantages of the method are :
- a more realistic treatment of the sequences, by taking into account the evolution in time of the accident and the possible interventions on the systems during the sequence ;
- a more exhaustive analysis, because the method does not need a pre-determination of the event sequences.

As an example, the analysis of the residual heat removal function of a fast breeder reactor showed that the method is perfectly manageable for quite complex problems, with the help of suitable techniques as biased Monte-Carlo simulation and response surface method.

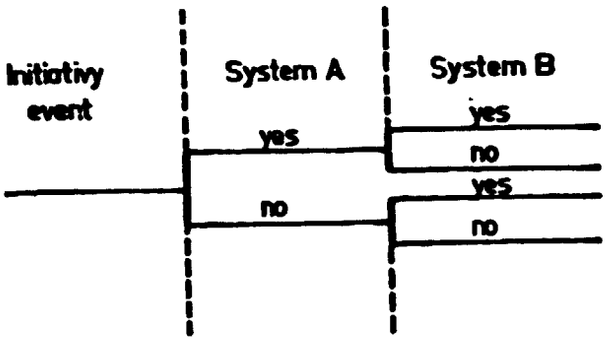
Encouraging results were obtained with this study, so the method can certainly be used, in other risk studies, for more and more complex systems.

REFERENCES

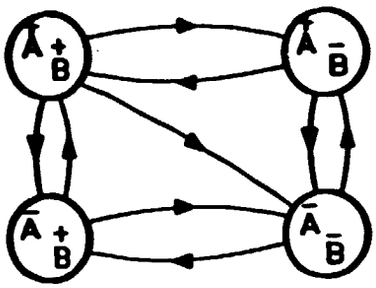
1. C. VILLEROUX-LOMBARD, A. PAVRET de la ROCHEFORDIERE, "Etude de la fiabilité du système d'évacuation de la puissance résiduelle du réacteur rapide Phénix", Rapp. DSN/SETSSR n°99, Juillet 1976.

2. G. JUBAULT, A. CARNINO, "Fast reactor safety - Reliability analysis of Phenix decay heat removal function", Rapp. DSN n°308, août 1979.
International Conference on fast reactor Safety - SEATTLE.

Figure 1



Event tree



State representation