The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

2152-13

Joint ICTP-IAEA Course on Natural Circulation Phenomena and Passive Safety Systems in Advanced Water Cooled Reactors

17 - 21 May 2010

Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment

F. D'Auria and more authors*
University of Pisa
DIMNP
Italy

Available online at www.sciencedirect.com
SCIENCE DIRECT®
Nuclear Engineering and Design 235 (2005) 2612–2631
Nuclear Engineering and Design
www.elsevier.com/locate/nucengdes

Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment

Michel Marquès [a,*], J.F. Pignatel [a], P. Saignes [a], F. D'Auria [b], L. Burgazzi [c], C. Müller [d], R. Bolado-Lavin [e], C. Kirchsteiger [e], V. La Lumia [f], I. Ivanov [g]

[a] *CEA/Cadarache, DER/SESI, Building 212, 13108 Saint-Paul-Lez-Durance Cedex, France*
[b] *CIRTEN, University of Pisa, Pisa, Italy*
[c] *ENEA, Bologna, Italy*
[d] *GRS, Garching, Germany*
[e] *EC-JRC/IE, Petten, The Netherlands*
[f] *TECHNICATOME, Aix en Provence, France*
[g] *Technical University of Sofia, Bulgaria*

Received 11 April 2005; received in revised form 19 June 2005; accepted 30 June 2005

Abstract

A methodology has been developed to evaluate the reliability of passive systems characterised by a moving fluid and whose operation is based on thermal–hydraulic (T-H) principles. The methodology includes:

- identification and quantification of the sources of uncertainties and determination of the important variables;
- propagation of the uncertainties through T-H models and assessment of T-H passive system unreliability;
- introduction of passive system unreliability in the accident sequence analysis.

Each step of the methodology is described and commented and a diagram of the methodology is presented. An example of passive system is presented with the aim to illustrate the possibilities of the methodology. This example is the Residual Passive heat Removal system on the Primary circuit (RP2), an innovating system supposed to be implemented on a 900 MWe Pressurized Water Reactor.

1. Introduction

The expanded consideration of severe accidents, the increased safety requirements and the aim of introducing effective – yet transparent – safety functions lead to growing consideration of passive safety systems for future nuclear reactors.

* Corresponding author. Tel.: +33 442257131; fax: +33 442252408.
E-mail address: michel.marques@cea.fr (M. Marquès).

0029-5493/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.nucengdes.2005.06.008

Nomenclature

ET	event tree
FMEA	Failure Mode and Effect Analysis
FORM/SORM	First and Second Order Reliability Methods
IE	initiating event
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RMPS	Reliability Methods for Passive Safety Functions
RP2	Residual Passive heat Removal system on the Primary circuit
T-H	thermal–hydraulics
TLPS	Total Loss of Power Supply

Innovative reactor concepts make use of passive safety features to a large extent in combination with active safety or operational systems. According to the IAEA (1991) definitions, a passive system does not need external input, especially energy to operate. That is why, passive systems are expected to combine among others, the advantages of simplicity, a decrease in the need for human interaction, a reduction or avoidance of external electrical power or signals.

Besides the open feedback on economic competitiveness, special aspects like lack of data on some phenomena, missing operating experience over the wide range of conditions and driving forces which are smaller – in most cases – than in active safety systems, must be taken into account.

This remark is especially applicable to the passive system B or C (i.e. implementing moving working fluid, following the IAEA (1991) classification) and in particular to the passive systems that utilize natural circulation. These passive safety systems in their designs rely on natural forces to perform their accident prevention and mitigation functions once actuated and started. These driving forces are not generated by external power sources (e.g. pumped systems), as is the case in operating and evolutionary reactor designs. Because the magnitude of the natural forces, which drive the operation of passive systems, is relatively small, counter-forces (e.g. friction) can be of comparable magnitude and cannot be ignored as is generally the case with pumped systems. Moreover, there are considerable uncertainties associated with factors on which the magnitude of these forces and counter-forces depends (e.g. values of heat transfer coefficients and pressure losses). In addition, the magnitude of such natural driving forces depends on specific plant conditions and configurations which could exist at the time a system is called upon to perform its safety function. All these uncertainties affect the thermal–hydraulic (T-H) performances of the passive system. This particular aspect, inherent to these passive systems, was discussed extensively in an international workshop (OECD, 2002). Previous work carried out by ENEA, University of Pisa and Polytechnic of Milan, led to the development of a procedure called REPAS, which help evaluate the reliability of natural circulation system under specific conditions (Jafari et al., 2003).

To assess the impact of uncertainties on the predicted performance of the passive system, a large number of calculations with best estimate T-H codes are needed. If all the sequences where the passive system studied is involved are considered, the number of calculations can be prohibitive. For all these reasons, it appeared necessary to create a specific methodology to assess the reliability of passive system B or C. The methodology has been developed within the framework of a project called Reliability Methods for Passive Safety Functions (RMPS),[1] performed under the auspices of the European 5th Framework Programme. The methodology addresses the following problems:

- identification and quantification of the sources of uncertainties and determination of the important variables;
- propagation of the uncertainties through T-H models and assessment of T-H passive system unreliability;
- introduction of passive system unreliability in the accident sequence analysis.

In Section 2, each step of the methodology is described and commented and a diagram of the methodology is presented. The example of the Residual Passive heat Removal system on the Primary circuit (RP2), an innovative passive system, is presented in Section 3 to illustrate the possibilities of such a methodology.

[1] All the reports of the RMPS project are available on www.rmps.info.

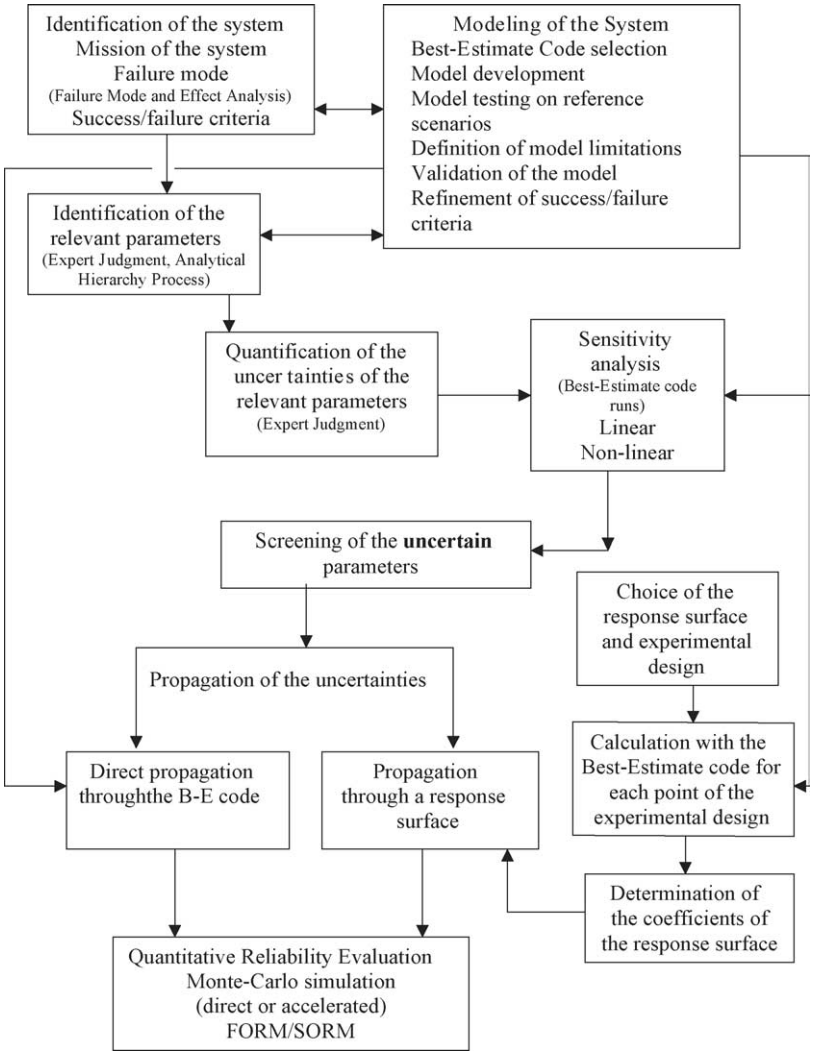

Fig. 1. RMPS methodology roadmap.

2. Methodology overview

The methodology proposed consists of several steps, which are shown in Fig. 1 and are detailed in the following sections.

2.1. Definition of the accident scenario

The first step of the methodology is the definition of the accident scenario in which the passive system will operate. Knowledge of this scenario helps identify the specific failure criteria and relevant parameters and the specific quantification of uncertainties. The results obtained in the reliability and sensitivity analyses of the passive system are thus specific to this scenario. A global evaluation of the passive system is obtained by the integration of its unreliability in a Probabilistic Safety Assessment, in which all the sequences involving the passive system are considered (see Section 2.9). This approach is preferred to conservative analyses consisting in evaluating the system reliability for the worst scenario considered or in integrating the larger variability of the uncertain parameters covering all the scenarios involving the system.

2.2. Characterisation of the system

The purpose of this analysis is to obtain information on the behaviour of the passive system, in an accident scenario occurring during the life of the nuclear reactor and to identify the failure zones and conditions, if such exist. Therefore, the missions of the system, its failure modes and the failure criteria must be defined.

2.2.1. Mission of the system

The missions of the system are the goals for which the passive system has been designed and located within the overall system. For instance, the mission of the passive system can be decay heat removal, vessel cooling, the pressure decrease of the primary circuit, ... In some cases, the passive system can be designed to fulfil several missions at the same time or different missions depending on the considered scenario.

2.2.2. Failure mode

Due to the complexity of thermal–hydraulic phenomena and to the interaction between the passive system and the overall system, it is not always obvious to associate a failure mode to the mission of the system. A qualitative analysis is often necessary so as to identify potential failure modes and their consequences, associated with the passive system operation. A hazard identification qualitative method such as the Failure Mode and Effect Analysis (FMEA) can be used to identify the parameters judged critical for the performance of the passive system and to help associate failure modes and corresponding indicators of the failure cause. This method can necessitate the introduction, in addition to mechanical components of the system (piping, drain valve, etc.), of a "virtual" component. This component is identified as natural circulation and is evaluated in terms of potential "phenomenological" factors (these include non-condensable gas build up, thermal stratification, surface oxidation, cracking, etc.), whose consequences can affect the passive system performance.

2.2.3. Success/failure criteria

Knowledge on the system missions and failure modes allows the evaluation of the failure criteria. The failure criteria can be established as single-targets (e.g. the system must deliver a specific quantity of liquid within a fixed time) or as a function of time targets or integral values over a mission time (e.g. the system must reject at least a mean value of thermal power during the entire system intervention). In these cases, the failure criterion is obtained by the comparison between the real performance of the system and the expected value of this performance. In some cases, it is better to define a global failure criterion for the whole system instead of a specific criterion for the passive system. For instance, the failure criterion can be based on the maximal clad temperature during a specified period. In this case, it will be necessary to have modeled the complete system and not only the passive system.

2.3. Modeling of the system

Due to the lack of suitable experimental databases for passive systems in operation, the evaluation must rely on numerical modeling. The system analysis must be carried out with a qualified thermal–hydraulic system code and performing best estimate calculations. Indeed, there is an increasing interest in computational reactor safety analysis to replace the conservative evaluation model calculations by best estimate calculations supplemented by a quantitative uncertainty analysis (Gläser, 2002). Particularly in the present methodology where the objective is the evaluation of the reliability of the passive system, it is important to calculate the passive system performance in a realistic and not conservative way. At this stage, calculations have to be carried out on the reference case with nominal values of the parameters characteristic of the system. The results have to be compared with experimental data if any exist. During the characterisation process, the modeling and the evaluation of the passive system, new failure modes can be identified (such as flow oscillations, plugs phenomena due to non-condensable gases, . . .) which must also be taken into account.

2.4. Identification of the sources of uncertainties

First of all, the method requires the identification of the potentially important contributors to uncertainty of the code results. These contributors are:

- Approximations in modeling the physical process: for instance, the treatment of a liquid steam mixture as a homogeneous fluid, the use of empirical correlation, ...

- Approximations in modeling the system geometry: simplification of complex geometry features and approximation of a three-dimensional system.
- The input variables: initial and boundary conditions, such as plant temperatures, pressures, water levels and reactor power, dimensions, physical properties, such as densities, conductivities, specific heats, and thermal–hydraulic parameters, such as heat transfer coefficients or friction factors.

This identification of the relevant parameters must be based on the opinion of the experts of physical processes and thermal–hydraulic codes. Different methodologies have been developed to evaluate the overall uncertainty in the physical model predictions and some efforts have been made for the internal uncertainty assessment capacity of thermal–hydraulic codes (D'Auria and Giannotti, 2000). However, in the present study, the uncertainties pertaining to the code are not accounted for, focusing the attention on the uncertainties relative to the input parameters of the code, characteristic of the passive system or of the overall system.

2.5. Identification of the relevant parameters

Among all the sources of uncertainties, the evaluation of the reliability of a passive system requires the identification of the relevant parameters which really affect reaching the system goal. The tool chosen here for this task is the Analytic Hierarchy Process (Zio et al., 2003). This method consists of three major steps: the building of a hierarchy to decompose the problem at hand, the input of pairwise comparison judgments on the relevance of the considered parameters and the computation of priority vectors to obtain their ranking. The hierarchy is built in three steps:

- Accurately define the most important goal (i.e. the mission) of the passive system and place it at the top level.
- Build the hierarchy downward into different levels by putting in each level those factors directly influencing the elements of the level just above and directly influenced by the elements of the level just below.
- At the bottom of the hierarchy, place the basic parameters.

Then, for each element of each level, a pairwise comparison matrix is build by expert elicitation to assess the influence of the relevant entries of the level below in relation to the element under analysis. The proper question in the pairwise comparison is of the form: "Considering entries X and Y of level $s-1$, how much more important is entry X compared to entry Y with respect to their influence on element k of level s?" The principal eigenvector of the comparison matrix provides the priority vector of the element under consideration. Once all the priority vectors are available, they are multiplied appropriately through the branches of the hierarchy in order to determine the overall weights of the bottom-level basic parameters with regards to the previously defined top goal. The major advantage of the pairwise comparison approach to quantification is the simple and intuitive way of expressing judgments on the relative importance of the different constituents of the hierarchy, and the possibility of checking for consistency in the judgment entries.

2.6. Quantification of the uncertainties

A key issue in this methodology is the selection of the distributions for the input parameters. The main objective is that the selected distribution for each input parameter must quantify the state of knowledge and express the reliable and available information about the parameter. The choice of distribution may highly affect the reliability evaluations of the passive system. Different points of view have to be considered for this quantification.

2.6.1. The amount of data

When the data on a parameter are abundant, statistical methods can be used such as the maximum likelihood method or the method of moments to adjust analytical density functions and different goodness-of-fit tests can be used (Chi square, Kolmogorov–Smirnov, . . .) to find the best analytical fit to the data. When the data are sparse or non-existent and this is generally the case when we consider the uncertainties affecting the passive system performance, the evaluation of the probability functions of the uncertain parameters must be based on the expert judgments. Thus, a subjective approach is used where the uncertainty is characterised as a probability density function that shows the range of values where the actual value of the parameter may be

and what parts of the range the analyst considers more likely than others. In the case where no preferences can be justified, a uniform distribution will be specified, i.e. each value between minimum and maximum is equally likely. These distributions are quantitative expressions of the state of knowledge and can be modified if there is new evidence. If suitable observations become available, they can be used consistently to update the distributions. As a consequence of probability distributions of input parameters, the computer code results also have a subjective probability distribution, from which uncertainty limits or intervals are derived.

2.6.2. The dependence between the parameters

If parameters have contributors to their uncertainty in common, the respective states of knowledge are dependent. As a consequence of this dependence, parameter values cannot be combined freely and independently. Instances of such limitations need to be identified and the dependencies need to be quantified, if judged to be potentially important. If the analyst knows of dependencies between parameters explicitly, multivariate distributions or conditional probability distributions may be used. The dependence between the parameters can be also introduced by covariance matrices or by functional relations between the parameters.

2.7. Sensitivity analysis

2.7.1. Objectives

An important feature of the methodology is to evaluate the sensitivity of the input parameters uncertainties on the uncertainty of the passive system performance. The sensitivity measures give a ranking of input parameters. This information provides guidance as to where to improve the state of knowledge in order to reduce the output uncertainties most effectively. If experimental results are available to be compared with calculations, the sensitivity measures provide guidance as to where to improve the models of the computer code.

2.7.2. Qualitative sensitivity analysis

Sometimes the lack of operational experience and significant data concerning the passive system performance forces the analysis to be performed in a qualitative way aiming at the identification, for each failure mode, of both the level of uncertainty associated with the phenomenon and the sensitivity of failure probability to that phenomenon (Burgazzi, 2002). For example, even if a phenomenon is highly uncertain (because of deficiencies in the physical modeling), this may not be important for the overall failure probability. Conversely, a phenomenon may be well understood (therefore the uncertainty is small) but the failure probability may be sensitive to small variation in this parameter. The grading scheme is given in Table 1. The worst case is characterised by "high" rankings relative to either sensitivity or uncertainty (e.g. presence of non-condensable gas or thermal stratification), making the corresponding phenomena evaluation a critical challenge.

Table 1
Grade rank for qualitative uncertainty and sensitivity analyses

Grade	Definition
Uncertainty	
H	The phenomenon is not represented in the computer modeling or the model is too complex or inappropriate which indicates that the calculation results will have a high degree of uncertainty
M	The phenomenon is represented by simple modeling based on experimental observations or results
L	The phenomenon is modeled in a detailed way with adequate validation
Sensitivity	
H	The phenomenon is expected to have a significant impact on the system failure
M	The phenomenon is expected to have a moderate impact on the system failure
L	The phenomenon is expected to have only a small impact on the system failure

2.7.3. Quantitative sensitivity analysis

The quantitative sensitivity analysis necessitates thermal–hydraulic calculations. It consists in ranking the parameters according to their relative contribution on the overall code response uncertainty and quantifying this contribution for each parameter. To apportion the variation in the output to the different input parameters, many techniques can be used (Saltelli et al., 2000), each yielding different measures of sensitivity.

A common approach is to base the sensitivity analysis on a linear regression method, which is based on the hypothesis of a linear relation between response and input parameters. This, in case of passive systems, is obviously restrictive. However, the method is simple and quick, and provides useful insights in case of a restricted number of sampling, as will be often

our case. Three different sensitivity coefficients have been considered, each one providing a slightly different information on the relevance of a parameter: standardized regression coefficients (SRC), partial correlation coefficients (PCC) and correlation coefficients (CC). Small differences between the different coefficients may be due to a certain degree of correlation between the inputs and to the system's non-linearity. These occurrences should be analysed, the first one possibly through the examination of the correlation matrix and the second one by calculating the model coefficient of determination R^2.

Depending on the nature of the model representing the passive system operation and calculating its performances, it can be more accurate to use sensitivity methods developed for non-monotonous or non-linear models. In case of non-linear but monotonous models, we can perform rank transformations and calculate associated indices: standardized rank regression coefficients (SRRCs) and partial rank correlation coefficients (PRCCs). The rank transformation is a simple procedure, which involves replacing the data with their corresponding ranks. We can also calculate a determination coefficient based on the rank R^{2*}. The R^{2*} will be higher than the R^2 in case of non-linear models. The difference between R^2 and R^{2*} is a useful indicator of non-linearity of the model. For non-linear and non-monotonous models, two methods exist: the Fourier Amplitude Sensitivity Test (FAST) and the Sobol method. The general idea of these methods is to decompose the total variance of the response, in terms corresponding to uncertainty on the input parameters taken independently, in terms corresponding to the interaction between two parameters, in terms corresponding to the interaction between three parameters, etc. The Sobol indices are calculated by Monte Carlo simulation. The problem of these methods, and especially the Sobol method, is that a good estimation of these indices requires a great number of calculations (i.e. 10,000 simulations). Thus, it is necessary first to calculate a response surface validated in the domain of variation of the random variables (see Section 2.8.4). Thus, if the model is really not linear, nor monotonous, we propose to:

- adjust non-linear models on the data;
- test the validity of the model (e.g. in calculating R^2, residues, predictive robustness);
- use the model as a response surface in order to evaluate the Sobol or FAST indices.

2.8. Reliability evaluations

Different methods can be used to quantify the reliability of the passive system once a best estimate thermal–hydraulic code and a model of the system are given. The performance function of a passive system according to a specified mission is given by:

$$M = \text{performance criterion} - \text{limit} = g(X_1, X_2, \ldots, X_n)$$

in which the X_i ($i = 1, \ldots, n$) are the n basic random variables (input parameters) and $g(\cdot)$ is the functional relationship between the random variables and the failure of the system. The performance function can be defined in such a way that the limit state, or failure surface, is given by $M = 0$. The failure event is defined as the space where $M \leq 0$, and the success event is defined as the space where $M > 0$. Thus, a probability of failure can be evaluated by the following integral:

$$P_f = \int \int \ldots \int f_{X(x_1,x_2,\ldots,x_n)}\, \mathrm{d}x_1, \mathrm{d}x_2, \ldots, \mathrm{d}x_n \qquad (1)$$

where f_X is the joint density function of $X_1, X_2, \ldots, X_n$, and the integration is performed over the region where $M \leq 0$. Because each of the basic random variables has a unique distribution and because they interact, the integral (1) cannot be easily evaluated. Two types of methods can be used to estimate the failure probability: the Monte Carlo simulation with or without variance reduction techniques and the First and Second Order Reliability Methods (FORM/SORM).

2.8.1. Direct Monte Carlo

Direct Monte Carlo simulation techniques (Rubinstein, 1981; Bjerager, 1989) can be used to estimate the failure probability defined in Eq. (1) (or its complement to 1, reliability). Monte Carlo simulations consist in drawing samples of the basic variables according to their probabilistic characteristics and then feeding them into the performance function. An estimate $\overline{P}_f$ of the probability of failure P_f can be found in dividing the number of simulation cycles in which $g(\cdot) \leq 0$, by the total number of simulation cycles N. As N approaches infinity, $\overline{P}_f$ approaches the

true failure probability. It is recommended to measure the statistical accuracy of the estimated failure probability by computing its variation coefficient (ratio of standard deviation to average of estimations). The smaller the variation coefficient, the better the accuracy of the estimated failure probability. For a small failure probability and a small number of simulation cycles, the variance of $\bar{P}_f$ can be quite large. Consequently, it may take a large number of simulation cycles to achieve a specific accuracy. Then, the amount of computer time needed for the direct Monte Carlo method will be high, especially in our case where each simulation cycle involves a long calculation (several hours) performed by a thermal–hydraulic code.

2.8.2. Variance reduction techniques

Variance reduction techniques offer an increase in the efficiency and accuracy of the simulation-based assessment of the passive system reliability for a relatively small number of simulation cycles (Rubinstein, 1981; Madsen et al., 1986). Different variance reduction techniques exist, such as: importance sampling, stratified sampling, Latin hypercube sampling, conditional expectation, directional simulation, ...

2.8.3. FORM/SORM

An alternative to the Monte Carlo simulation is the use of FORM/SORM methods (Rackwitz et al., 1979; Madsen et al., 1986; Melchers, 1999). They consist of four steps:

- the transformation of the space of the basic random variables X_1, X_2, ..., X_n into a space of standard normal variables;
- the search for, in this transformed space, the point of minimum distance from the origin on the limit state surface (this point is called the design point);
- an approximation of the failure surface near the design point;
- a computation of the failure probability corresponding to the approximating failure surface.

FORM and SORM apply only to problems where the set of basic variables is continuous. For small order probabilities, FORM/SORM are extremely efficient when compared to simulation methods. The calculation time is, for FORM, approximately linear in the number of basic variables and independent from the probability level. The drawbacks of these methods come from the difficulty in identifying the design point when the failure surface is not sufficiently smooth, and from the fact that, contrary to Monte Carlo method, there is no direct way to estimate the accuracy of the provided estimation.

2.8.4. Response surface methods

To avoid the problem of long computer times in the previous methods, it can be interesting to approximate the response $Y = g(X)$ given by the T-H code, in the space of the input random variables, by a simple mathematical model $\tilde{g}(X)$ called response surface (Rajashekhar et al., 1993). Experiments are conducted with the basic random variables X_1, X_2, ..., X_n a sufficient number of times to define the response surface to the level of accuracy desired. Each experiment can be represented by a point with coordinates x_{1j}, x_{2j}, ..., x_{nj} in an n-dimensional space. At each point, a value of y_j is calculated by the T-H code and the unknown coefficients of the response surface $\tilde{g}(X)$ are determined in such a way that the error is minimum in the region of interest. When a response surface has been determined, the passive system reliability can be easily assessed in using the Monte Carlo simulation. Different types of response surfaces can be fitted: polynomial, thin plate splines, neural networks, generalised linear model, partial least squares regression, ... The type of response surface will be chosen depending on the problem (Devictor, 2004).

2.9. Integration of passive system reliability in PSA

The objective of this part of the methodology is the development of a consistent approach for introducing passive system reliability in an accident sequence in a Probabilistic Safety Assessment (PSA). Up to now, in the existing PSA of innovative nuclear reactor projects, are only taken into account the failures of the passive system components, but not the failure of the physical phenomena on which the system is based, such as the natural circulation. The treatment of this aspect of the passive system failure in the PSA models is a difficult and challenging task and no commonly accepted practices exist. In the first approach, we have chosen an event tree (ET) representation of the accident sequences. ET techniques allow the identification of all the different chains of accident sequences deriv-

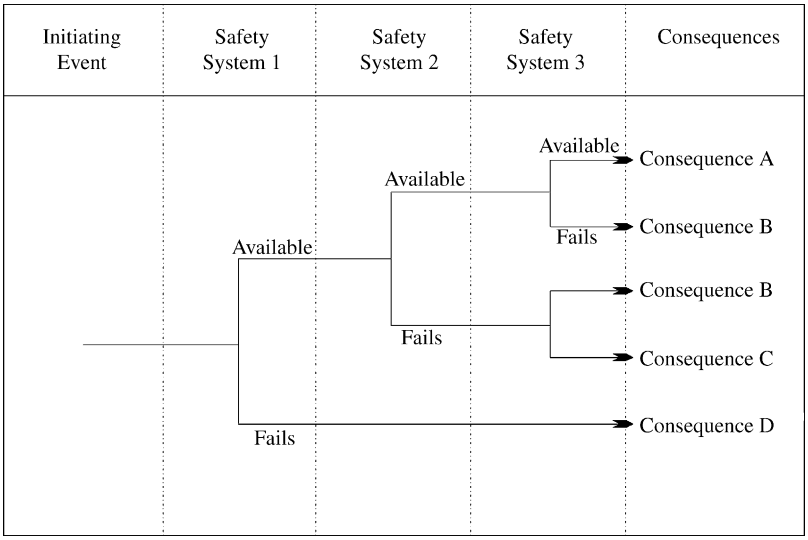

Fig. 2. Example of an event tree.

ing from an initiating event. The initiating event is an event (e.g. equipment failure, transient) that can lead to the accident if no protective action is taken by safety systems. Each sequence of the ET represents a certain combination of events corresponding to the failure or to the success of safety systems. Therefore, ET provides a set of alternative consequences. An example of an event tree is shown in Fig. 2. The consequences in the case of Level 1 PSA of nuclear reactors are usually defined as degrees of reactor core damage, including 'safe' state and 'severe' accident state. These consequences are generally evaluated by T-H calculations carried out in a conservative way.

This choice of the event tree presentation might seem unsuitable because it does not appear to consider the dynamic aspects of the transient progression including dynamic system interactions, T-H induced failure and operator actions in response to system dynamics. In fact, we have treated examples where the overall reactor, including the safety systems and in particular the passive system, is modeled by the T-H code. This results in the fact that the dynamic system interactions are taken into account by the T-H calculation itself. In addition, we have not considered human intervention during the studied sequences, which is coherent with the usual utilization of the passive systems in innovative reactors. So, for the first approach, the event tree presentation seems a good and simple representation for the assessment of accident sequences, including the passive systems.

For the sequences where the definition of envelope cases is impossible, events corresponding to the failure of the physical process are added to the event tree and uncertainty analyses are carried out to evaluate the corresponding failure probability. For this purpose, the T-H code is coupled to a Monte Carlo simulation modulus. The failure probabilities obtained by these reliability analyses are fed into the corresponding sequences.

3. Application of the methodology

The RMPS methodology was successfully applied to several passive systems, such as the Isolation Condenser System of Boiling Water Reactor (Marquès et al., 2002) or the Hydro-Accumulators of the VVER. We present here the example of the Residual Passive heat Removal system on the Primary circuit (RP2) system.

3.1. Description of the RP2 system

The RP2 system is an innovative passive system designed by the CEA (Gautier et al., 1999), which is supposed to be implemented on a 900 MWe Pressurized Water Reactor (PWR). This passive system is

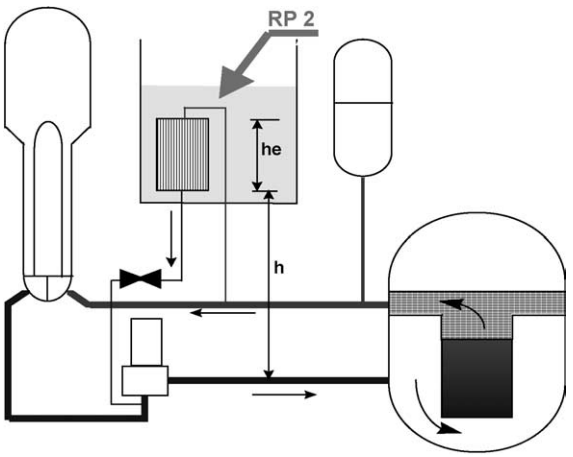

Fig. 3. Sketch of the Residual Passive heat Removal system on the Primary circuit (RP2).

composed of three circuits dedicated to heat removal, each one being connected to a loop in the primary circuit (Fig. 3). Each circuit includes an exchanger immersed in a cooling pool located inside the containment, and a valve to allow it to start. For the study in progress, this valve was put on the cold leg of the system, downstream from the exchanger. The exchanger is located higher than the main piping of the primary circuit to allow a natural circulation between the core and the exchanger. Reaching to a criterion of reactor emergency shutdown, the valve opens and natural circulation starts. The residual power produced by the fuel is transferred to the cooling pool via the RP2 exchanger. This system is quite similar to the passive heat removal system in AP600, but its missions are different. AP600 only rely upon passive systems for design basis accidents. RP2 has been designed within the framework of a new management principle, termed "Base Operation Passive Heat Removal" (BOPHR), where the residual power is removed jointly by active and passive systems, immediately after emergency shutdown. This example highlights the coupling effects between the passive system and the entire Nuclear Power Plant.

3.2. Characterisation of the system

3.2.1. Accidental scenario

The transient of Total Loss of the Power Supplies (TLPS) was selected as a reference accident for the reliability evaluation of the system.

3.2.2. Mission of the system

The objective of the safety systems is to avoid core meltdown under pressure. Thus, the mission of the RP2 system is double, on the one hand to depressurize the primary circuit, and on the other hand to prevent core fusion. For the exercise, the duration of accidental calculation was arbitrarily set at 12 h, relatively long time where no human intervention is simulated.

3.2.3. Failure criteria

The failure of the system is obtained if the maximum temperature of the clad or the temperatures of the fluid at the core output go beyond, respectively, the values of 500 °C and 450 °C, in less than 12 h.

3.3. Modeling of the system

3.3.1. Model development

The modeling with the CATHARE code (Barre and Bernard, 1990) of a complete PWR 900 MWe with the three independently simulated primary and secondary loops has been carried out. Each loop is equipped with a RP2 circuit with its exchanger immersed in a pool. The three cooling pools are modeled independently. Each RP2 circuit is connected to a primary loop between the hot and cold legs. Before the transient evaluation, steady-state calculations are carried out in order to adjust the characteristic parameters identified in the study to their target values. The following assumptions are taken into account for the TLPS reference calculation:

- shutdown of the primary circuit pumps;
- curve ANS 100% NP (2775 MW) for the decay of residual power;
- loss of the Feedwater Flow Control System and the Auxiliary Feedwater System;
- core power at 100% NP: 2775 MW;
- primary pressure: 15.5 MPa;
- level of the pressurizer: 7.3 m;
- initial level of fluid in the steam generators: 12.78 m;
- secondary pressure: 5.8 MPa;
- three RP2 available;
- initial temperature of the water in the pool: 30 °C.

3.3.2. Identification of the sources of uncertainties

A set of 24 parameters likely to be more or less uncertain at the time of the RP2 passive system start-

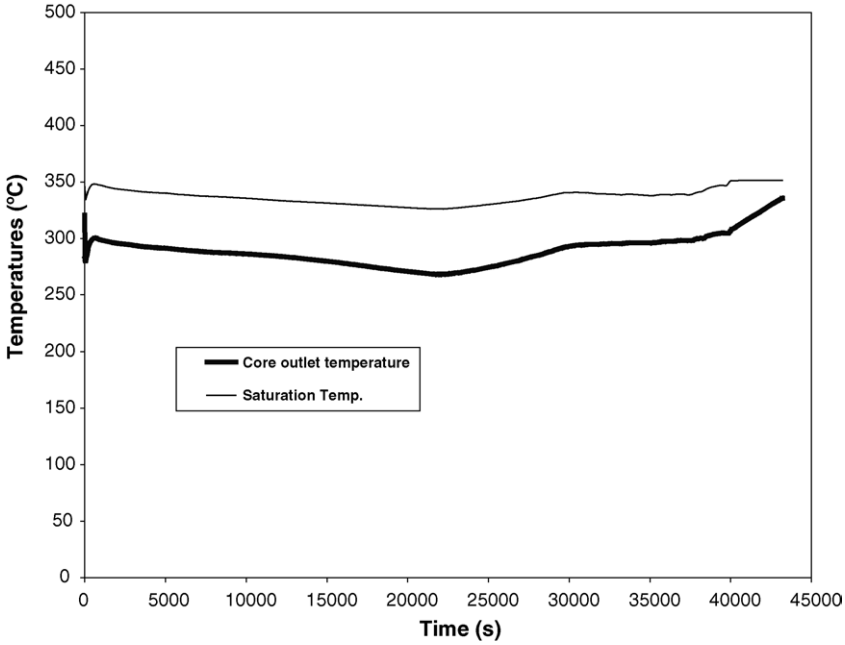

Fig. 4. Result of the nominal CATHARE calculation with two RP2 systems available.

up and significantly influencing the performances of the system was identified by expert judgment. These parameters are called the characteristic parameters and are listed below.

For each of the three RP2 circuits ($i = 1, 3$):

- I_i: instant at which the isolation valve of the RP2 opens;
- X_i: rate of uncondensable at the inlet of the RP2 exchanger;
- L_i: initial pool level;
- T_i: initial temperature of the water in the pool;
- C_i: fouling of RP2 exchanger tubes;
- R_i: number of broken tubes in RP2 exchanger.

For the primary circuit:

- PUI: percentage of nominal core power;
- PP: pressure in the pressurizer;
- ANS: decay of residual power according to the ANS law.

For the secondary circuit ($i = 1, 3$):

- NGV_i: real secondary level in the three steam generators.

3.3.3. Thermal–hydraulic calculations on the reference case

A preliminary calculation was carried out with the nominal values of the characteristic parameters in the case where only two RP2 are available. This case corresponds to the single failure criterion. The calculated transient was satisfactory. Fig. 4 shows the evolution of the outlet temperature of the core in comparison with the saturation temperature. The mission of the RP2 is completely fulfilled. At the end of 12 h (43,200 s), the primary circuit is depressurized, and the cooling of the core is assured.

In addition, with an aim of testing, the response of the CATHARE code for extreme values of the characteristic parameters, calculations were carried out in taking the minimum and maximum values of each parameter for the range of variations specified by experts.

3.4. Sensitivity and reliability analyses of the RP2 system

3.4.1. Global analyses

The first reliability and sensitivity analyses of the RP2 system were carried out by considering broad

Table 2
Probabilistic model of the 24 random variables in the global reliability analysis

Variable	Distribution	Average	Standard deviation	X_{min}	X_{max}	λ	μ
I_1, I_2, I_3	Composed						
X_1, X_2, X_3	Exponential					182	0
L_1, L_2, L_3	Truncated normal	4.5	0.6	2	5		
T_1, T_2, T_3	Truncated normal	303	20	280	368		
C_1, C_2, C_3	Truncated normal	15	5	0	30		
R_1, R_2, R_3	Exponential					7	0
PUI	Truncated normal	100	1	98	102		
PP	Truncated normal	155	4	153	166		
ANS	Truncated normal	10	5	0	20		
NGV_1, NGV_2, NGV_3	Truncated normal	12.78	0.30	12.08	13.91		

ranges of variation for the characteristic parameters. These ranges were supposed to represent the whole set of initial configurations to which the system could be subjected. The idea behind these first evaluations was to make a single reliability analysis of the system and in this way, limit the number of uncertainty calculations. The drawbacks of this unique evaluation were that the obtained results could have been conservative and not realistic and that this method did not allow the testing of the influence of the passive system on different accident situations. The choice of the ranges of variation and probability density functions of the characteristic parameters, given in Table 2, was based on expert judgment. Eighty-eight samples were generated and for each sample, a CATHARE calculation was performed. Among these 88 calculations, we obtained 7 system failures. All these seven failure cases corresponded to cases with one tube rupture in one of the RP2s. Depending on the case, the limit core output temperature is reached between 4100 s and 7100 s. Fig. 5 shows the evolution of the outlet temperature of the core on one of these failure cases. All the other calculations were a success for the system's mission.

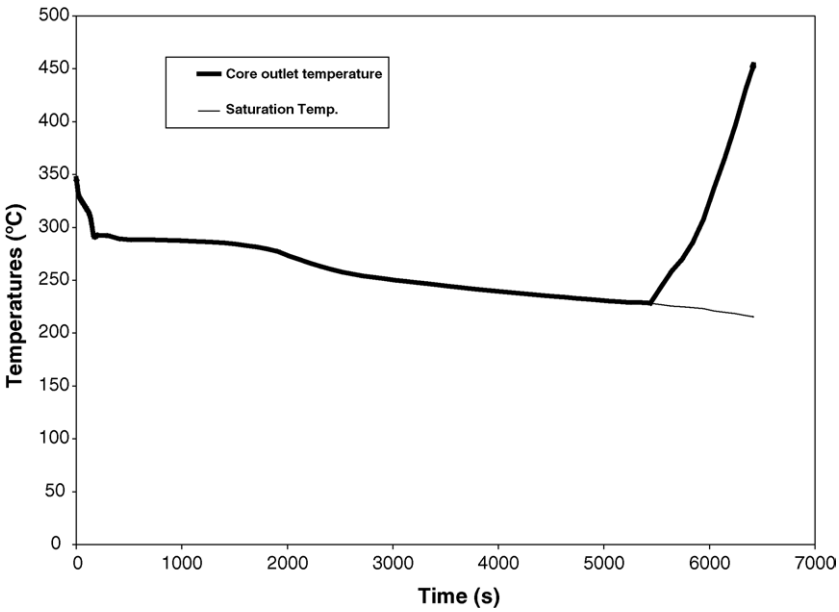

Fig. 5. Result of the CATHARE calculation with one tube rupture in one of the RP2 exchangers.

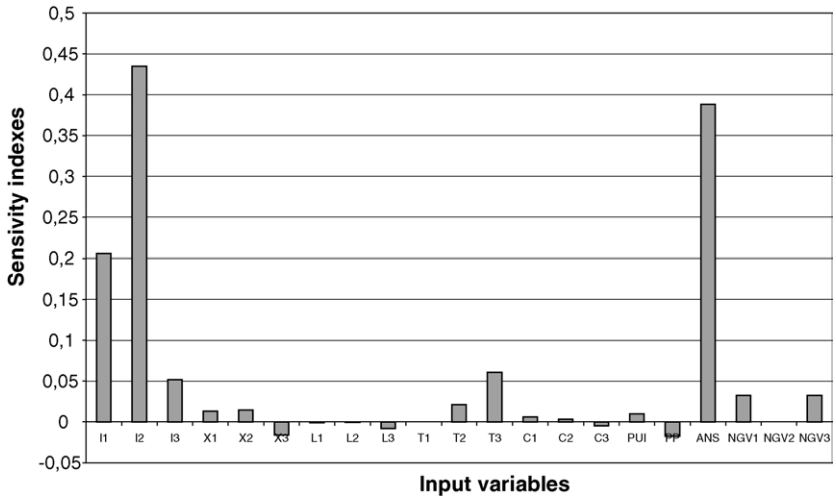

Fig. 6. Global sensitivity analysis on the performance ratio of the RP2 system carried out by calculating SOBOL indices.

In the second step, we decided to suppress the possibility of tube rupture at RP2 start-up. Indeed, the tube rupture could be included in the failure of mechanical components of the system in a Probability Safety Assessment (see Section 3.5). In this case, we only had 21 random variables. Eighty-five samples from the 21 random variables were generated and for each sample, a CATHARE calculation was performed. All these cases lead to a success for the system's mission considering the failure criteria. In order to analyse the performance of the system, we considered the ratio between the sum of the energy extracted by each RP2 during the 12 h of the transient and the energy produced by the core during the transient. To perform a sensitivity analysis on the performance of the system, different types of response surfaces were fitted between the 21 input parameters and the output value of the ratio calculated by the CATHARE code: polynomial response surfaces (up to third degree) and responses surfaces obtained by neural network techniques. Two types of sensitivity analysis were carried out: a sensitivity analysis with standardized regression coefficients although the model is not fully linear ($R^2 = 0.77$) and a sensitivity analysis with Sobol indices calculated by using a response surface based on neural network and by performing 10,000 simulations of this surface (Fig. 6). The results of the calculation of the SRCs or the Sobol indices both give the same indications: the most important variables are ANS, the residual power decay which is mainly due to the state of the fuel in the core when the transient occurs and I_1, I_2, I_3, the instants of opening of the RP2 valves, which directly govern the duration of the heat exchange time in the RP2 system.

3.4.2. Specific analyses

Within the framework of the integration of the system reliability in a PSA (see Section 3.5), the specific ranges of variation and the specific probabilistic density functions of the characteristic parameters have been identified for some sequences. Specific reliability and sensitivity analyses were carried out for these sequences. We present here the example of the sequence with two RP2s available and no broken tube in the RP2 exchangers. In this case, the number of characteristic parameters is reduced to 14 (there are only two RP2 circuits available and the number of broken tubes and the valve failure are no longer considered in the uncertainty analysis, but taken into account in the event tree of the PSA). Besides, a monitoring system was supposed to be implemented on the RP2 system, in order to constantly check that the RP2 loops are available when these are solicited. This led to narrower ranges of variation for the levels and the temperatures of the two pools. The choice of the probabilistic model presented in Table 3 was based on engineer judgment.

The results of the sensitivity analysis performed by calculating the SRCs and the partial correlation coeffi-

Table 3
Probabilistic model of the 14 random variables in the specific reliability analysis of the sequence with two RP2 loops available and no broken tubes in the exchangers

Variable	Distribution	Par 1	Par 2	X_{min}	X_{max}
X_1, X_2	Truncated log-normal	0.12	0.43	0	1
L_1, L_2	Truncated normal	4.5	0.5	4	5
T_1, T_2	Truncated normal	30	20	10	50
C_1, C_2	Truncated log-normal	12	0.4	0	30
PUI	Truncated normal	100	2	98	102
PP	Truncated normal	155	2	153	157
ANS	Truncated log-normal	6	0.4	0	20
NGV_1, NGV_2, NGV_3	Truncated normal	12.78	0.70	12.08	13.91

cients show (Fig. 7) that the most influential parameters on the performance ratio are L_1 and L_2, the initial pool levels and the ANS curve. The objective of the uncertainty calculations was to evaluate the probability p_1 corresponding to the failure of the T-H process, considered as a basic event in the event tree, when only two RP2s are available. We carried out 76 calculations with CATHARE with values for the input variables randomly generated by considering this probabilistic model. Among these 76 calculations, we obtained 18 cases of failure, leading to a rough estimation of the failure probability p_1 to 0.24.

In the same way, we determined a T-H failure probability p_2 equal to 0.04 for the RP2 passive system in the sequence with two RP2s available and at least one broken tube in one of the RP2 exchangers.

3.5. Integration of the reliability of passive system in Probabilistic Safety Assessment

3.5.1. Methodology

This study consists in:

- identifying the different types of malfunction of the RP2 passive system and evaluating their related probabilities;
- including these evaluations in a simplified PSA on a PWR reactor;

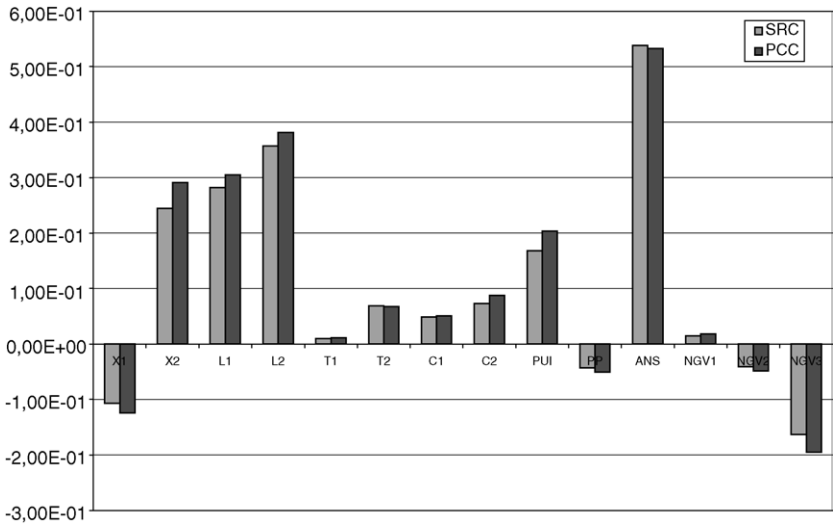

Fig. 7. Sensitivity analysis on the performance ratio of the RP2 system in the case with two RP2s available and no broken tubes on the RP2 exchangers.

- carrying out calculations on a set of CATHARE transients;
- including the CATHARE results in the PSA;
- evaluating the yearly occurrence frequency of core damage for the reactor equipped with safety passive systems, in the case of a TLPS transient.

3.5.2. Types of malfunctions

The reliability analysis of the RP2 passive system underlines the existence of two types of failures which could affect the system:

- failures on passive system components, which lead, directly or indirectly, to the loss of the system;
- the occurrence of an initial configuration of the passive system, which is not standard and leads to the loss of the system, mainly for thermal–hydraulic reasons.

For this second type of failures, we can consider two possibilities:

- A monitoring system could detect, before the occurrence of the TLPS event, the existence of the non-standard configuration of the passive system (for instance, the cooling pool level is lower than the threshold level). It is considered that, as soon as the non-standard configuration is detected, the automatic safety systems or the operators shutdown the reactor in safety state. The occurrence of this type of configuration lies in the failure of monitoring systems.
- No monitoring system can detect, before the occurrence of the TLPS event, the existence of a non-standard configuration of the passive system (for instance, presence of non-condensable gas at the inlet of the RP2 exchanger). In this case, it is not considered that operators shutdown the reactor in a safety state.

Table 4
Failure probability of the RP2 components

Failure type	Failure probability (per demand)
Non-opening per demand of the RP2 valve (for each RP2 loop)	3×10^{-3}
Broken tubes in the RP2 exchanger (for at least one of the three RP2 loops)	3×10^{-3} (hypothesis: 10^{-3} per RP2 loop)

3.5.3. Probability for each type of malfunction

This section aims to evaluate the probabilities for each of the three types of failures previously identified. For the first and the second types of failures, the analysis consists in taking into account the failure in the form of a probability of occurrence. The failure probabilities are evaluated by analogy with similar components existing on PWR reactors. Failure probabilities of the RP2 system components are given in Table 4 and the occurrence of initial non-standard configurations of the RP2 system, detectable by a monitoring system, in Table 5.

The existence of an initial non-standard configuration for the passive system, regarding a monitored parameter, requires the combination of two simultaneous failures:

- the occurrence of the non-standard configuration (for instance, low level for the RP2 pool);
- the lack of detection of this non-standard configuration by the monitoring system.

The related probability is then the product of the probability of occurrence of the non-standard config-

Table 5
Probability of occurrence of an initial non-standard configuration of the RP2 system, detectable by monitoring systems

Initial non-standard configuration type (detectable by a monitoring system)	Monitoring system failure type	Failure probability (per demand)
Pool water level lower than the low level threshold (defined for each RP2 loop)	Failure of the pool water level measure (sensor, calculator)	3×10^{-3}
Pool water temperature higher than the high temperature threshold (defined for each RP2 loop)	Failure of the pool water temperature measure (sensor, calculator)	3×10^{-3}
Steam generator level lower than the low level threshold (defined for each RP2 loop)	Failure of the steam generator level measure (sensor, calculator)	Negligible (reactor safety system)
Primary pressure level higher than the high level threshold	Failure of the primary pressure measure	Negligible (reactor safety system)

Table 6
Failure probabilities per demand of the RP2 system

Failure type	Failure probability (per demand)
Two RP2 loops available and one RP2 loop in failure	$3Pf_{loop} = 3 \times 10^{-2}$[a]
One RP2 loop available and two RP2 loops in failure	$3Pf^2_{loop} = 3 \times 10^{-4}$[a]
No RP2 loop available	$Pf^3_{loop} = 10^{-6}$[a]

[a] For each RP2 loop, the failure probability per demand Pf_{loop} is roughly equal to $10^{-2} \approx 3 \times 10^{-3}$ (non-opening per demand of the RP2 valve) + 3×10^{-3} (failure of the pool water level measure) + 3×10^{-3} (failure of the pool water temperature measure).

uration by the probability of occurrence of the non-detection by the monitoring system.

The evaluation of the probability of occurrence of the non-standard configuration is not possible at the present level of operation studies on RP2 system. Thus, the probability of occurrence of the non-standard configuration is set at 1 under conservative assumption. The failure probability of the system, following the non-standard configuration, is considered as the probability of non-detection of the situation by the monitoring system.

For each RP2 loop, the failure probability is equal to 10^{-2} per demand. This value is obtained in summing up the probability that the valve does not open and the probabilities of failure of the monitoring systems for the pool water level and the pool water temperature. The RP2 system is made of three RP2 loops. Thus, three types of failure, depending on the number of loops available, have to be analysed. The failure probabilities obtained in each case are given in Table 6.

The evaluation of the probability of occurrence of an initial non-standard configuration for the RP2 system, undetectable by any monitoring system, is estimated through a reliability analysis taking into account the probability density functions of the characteristic parameters of the process. The association of the CATHARE code with a Monte Carlo simulation modulus allows the estimation of the failure probability of the physical process in this case (see Section 3.4.2).

3.5.4. Simplified PSA including the RP2 passive system

The simplified PSA carried out in this project consists in analysing an accident, defined as an initiating event (TLPS, when the reactor is in full power), and the associated accident management based on the application of two passive safety systems: the RP2 passive system (made up of three RP2 loops) and the safety injection by accumulators. The seal LOCA breaks in case of TLPS are not taken into account in this study but they should be taken into account in a more detailed study.

The accidental sequences are defined using an event tree, taking into account the success or the failure of the components and of the physical process involved in the RP2 system. Knowing the occurrence of each accident sequence frequency and considering that all the events are independent, the estimation of the core damage probability can be carried out by summing up the probabilities of each sequence leading to a core damage.

This analysis is an illustrating exercise, dedicated to the test and the validation of the reliability methodology applied to the passive system. It should be noted that the PSA result obtained has several limitations, which should be eliminated as much as possible in a real PSA. These specific limitations are:

- The analysis concerns only one initiating event, the TLPS, even if this transient is the reference transient having been used for the design basis of the safety systems dedicated to residual power removal; other initiating events have to be analysed.
- The consequences of a system failure, when it is not in demand (valve opening, valve leak, rupture of a primary nozzle), are not considered (i.e. the initiating events created by a failure of the RP2 are not taken into account), even if this failure could have a potential effect on the safety.
- No aggravating event is considered, relative to the initiating event of TLPS, apart from the RP2 passive system failures (component failures or T-H process failure) and the safety injection.
- The human factor (operator errors) are not explicitly taken into account (the presence of a crisis team limits error possibilities).
- No “mechanical” common cause failure between the three RP2 loops have been considered. Only the “thermal–hydraulic” common cause failure has been taken into account through the global CATHARE modeling of the three RP2 loops. Thus, the mechanical failure of one RP2 loop has no consequence on the operation of the others.

- The common cause failure between the monitoring systems of the RP2 loop is considered as negligible.
- No common cause failure is considered between the RP2 passive system and the safety injection.
- Only one failure is considered for each RP2 loop.

3.5.5. Initiating event and associated event tree

The accidental transient of TLPS, when the reactor is in full power, has been chosen, as it is the reference transient used for the design basis of the safety systems dedicated to the residual power removal. The probability of occurrence of this initiating event is 10^{-5} per year. This value has been obtained by a fault tree analysis carried out on an analog real reactor. Starting from the initiating event, the analysis is carried out through the method of event tree, integrating the RP2 loops and the safety injection by accumulators. The event tree is presented in Fig. 8. To simplify the representation, the four possibilities concerning the number of RP2 loops available are presented in the same event tree, whereas a real event tree is always binary.

3.5.6. Event tree description

The generic events taken into account in the event tree express the main actions to take, in order to protect the reactor, in case of TLPS event:

Event 1: Failure per demand of the RP2 system—after the TLPS event, the RP2 system is required to remove the residual power, because normal means, which require an energy source, are not available. The management of the transient is different according to the number of RP2 loops available. The failure probabilities obtained in each case are given in Table 6.

Event 2: Broken tubes on RP2 exchangers—in the case of a broken tube on at least one of the RP2 exchangers, the break in the primary circuit involves the uncovering of the core and requires the start-up of the safety injection. This event corresponds to the probability of occurrence of broken tubes on at least one of the three RP2 exchangers. The probability of this event is 3×10^{-3} per demand for the three RP2 loops.

Event 3: Failure of the T-H process—this event corresponds to an undetected configuration which leads to a lack of efficiency of the RP2 system, and eventually to core damage. The probability of the failure of the T-H process is evaluated by uncertainty calculations (see Section 3.4.2).

Event 4: Failure of the safety injection by accumulators—in the case of a break on the RP2 exchanger tubes, the start-up of the safety injection by accumulators maintains the feedwater mass in the primary circuit, and the reaching of a satisfactory state at 12 h (recovering of the active means of safety injection). But the mechanical failure of the safety injection system directly results in core damage. Its probability is equal to 10^{-3} per demand.

3.5.7. Accident sequences description

Only the sequences leading to a core damage are detailed here:

Sequence 3 (three RP2s available, one broken tube): in the case of one broken tube in the exchanger, even when taking into account the uncertainties of the characteristic parameters, the depressurization is sufficient to allow the start-up of the safety injection system. But the failure of the safety injection leads to low pressure core damage by uncovering the core.

Sequence 5 (two RP2s available, no broken tube): taking into account the variations of the characteristic parameters around the nominal values, it is not possible to conclude to a success or to a failure of the RP2 system for this situation. An event corresponding to the failure of the thermal–hydraulic process is therefore considered. In Sequence 5, the thermal–hydraulic process fails so that the sequence leads to high pressure core damage.

Sequences 7 and 8 (two RP2s available, one broken tube): as a result of T-H calculations, the proximity between the time (≈4500 s) when the depressurization reaches 40 bar (i.e. the necessary pressure to start the safety injection) and the beginning of core damage (≈5500 s) does not allow us to conclude to a success or to a failure of the RP2 system for this situation. An event corresponding to the failure of the thermal–hydraulic process is therefore considered. In Sequence 7, the thermal–hydraulic process is running well (the depressurization of the primary circuit is sufficient to obtain 40 bar before core damage) but the safety injection fails so that the sequence leads

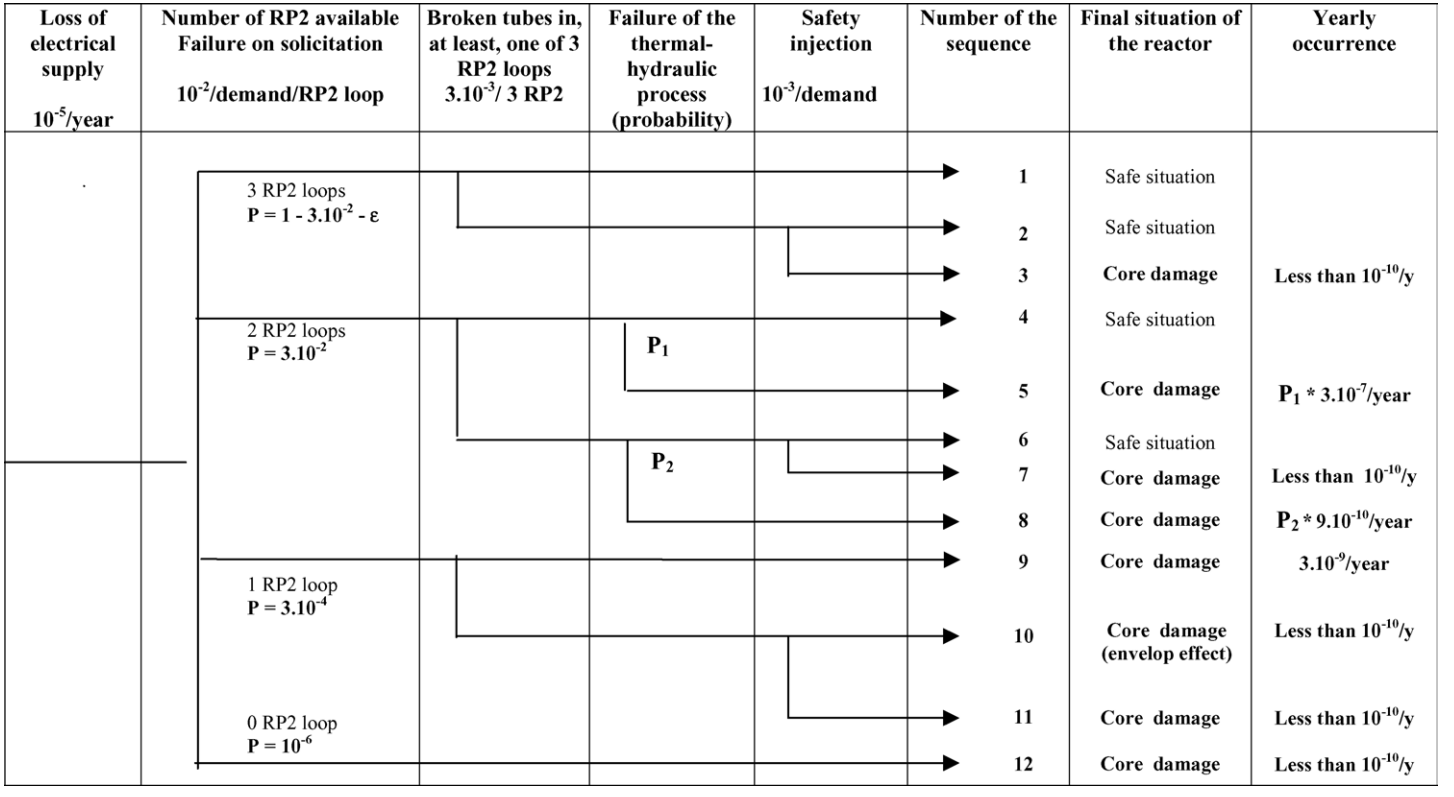

Fig. 8. Simplified event tree of Total Loss of Power Supply on a PWR equipped with the RP2 system.

to a high pressure core meltdown. In Sequence 8, the thermal–hydraulic process fails (the primary pressure stays above 40 bar) and the sequence leads to a high pressure core meltdown.

Sequences 9–11 (one RP2 available) and *Sequence 12* (no RP2 available): with only one RP2 loop available, the power extracted is not sufficient and the situation leads to a core damage. If there is one broken tube in the exchanger, it is possible that the depressurization will be sufficient to allow the start-up of the safety injection system. However, we have also considered this situation as a situation leading to core damage, because from a conservative point of view, the addition of two unfavourable events cannot lead to a satisfactory situation. Thus, the three Sequences 9–11 lead to a core damage. With no RP2 loop available, we are in the case of no safety system available and core damage is reached in less than 1 h.

3.5.8. PSA results and analysis

Core damage frequency, after a TLPS event, is estimated at 7.5×10^{-8} per year. This frequency corresponds to the sum of the probabilities of each accident sequence leading to the core meltdown in pressure for the TLPS transient with the assumption that all the events are independent. The main accident sequence (Sequence 5) has a frequency equal to 7.2×10^{-8} per year which represents 96% of core damage frequency. This sequence corresponds to a T-H process failure when one RP2 loop is not available. This frequency is at the limit of the acceptability, as it does not respect the probabilistic objectives set at 10^{-7} per year for all the transient families with respect to core meltdown in pressure. Given that there are 10 great transient families, this global objective corresponds for 1 family to a frequency of 10^{-8} per year. This result does not affect the design of the RP2 system which is efficient in preventing high pressure core meltdown. But it would be desirable to re-examine the design basis of the RP2 system, in order to obtain a more satisfying process, when one RP2 loop is not available. In this case, the probabilistic objective to reach for the T-H process failure would be 0.03 and not 0.24. This value would allow reaching a yearly core damage frequency of 10^{-8} with respect to high pressure core damage for the studied transient family (TLPS). This objective can easily be reached by slightly increasing the size of the cooling pool. The RP2, designed in this way, would reach the probabilistic safety objectives set for a reactor integrating passive systems. These results underline the importance of taking into account the T-H process failure probability when evaluating the reliability of a passive safety system.

4. Conclusions

A methodology has been developed to evaluate the reliability of passive systems characterised by a moving fluid and whose operation is based on T-H principles, such as natural circulation. The obtained methodology addresses the following problems:

- identification and quantification of the sources of uncertainties and determination of the important variables;
- propagation of the uncertainties through T-H models and assessment of T-H passive system unreliability;
- introduction of passive system unreliability in the accident sequence analysis.

The methodology shows the importance of the definition of T-H passive system reliability, which implies the definition of the performance function of the system and the analysis of the uncertainties.

The methodology has been successfully applied to several passive systems among which is the RP2 passive system. The results obtained on these examples have shown the advantages of sensitivity analysis for the determination, among the uncertain parameters, of the main contributors to the risk of failure of the passive system. They have also shown that it is possible to evaluate the reliability of the systems for specific situations, once the probability density functions of the input parameters are defined, by using the Monte Carlo or FORM/SORM methods. In order to reduce the number of T-H calculations, it often appears useful to approximate the T-H model by a response surface.

A consistent approach, based on an event tree representation, has been developed to incorporate in a Probabilistic Safety Assessment, the results of reliability analyses of passive systems obtained on specific accident sequences. In this approach, the accident sequences are analysed by taking into account the success or the failure of the components and of the

physical process involved in the passive systems. This methodology allows the probabilistic evaluation of the influence of a passive system on an accident scenario and could be used to test the advantage of replacing an active system by a passive system in specific situations. On the example of the RP2 system, the methodology has led to a proposal of a new design basis of the system.

The developed methodology participates to the safety assessment of reactors equipped with passive systems and could be a tool for the designers who define the architecture of safety systems and for the regulatory authorities in the safety evaluation of passive system.

The results of the analyses made show that, in spite of the inherent characteristics of passive systems, which are a priori considered as advantages (simplicity, decrease of the need for human interaction, reduction or avoidance of external electrical power or signals), the decision for the designers to replace an active safety system by a passive system is not easy from a safety point of view. Before making a final decision, other points which have not been addressed within the framework of the RMPS project, due to limited time and resources, should be studied in future work. In particular, a very important issue concerns the human factors, which play an important role in the reliability assessment of a passive system. Indeed, the periodic maintenance and inspection of such systems introduce particular constraints; unlike an active system that can be more easily isolated or inspected during the shutdown periods, a passive system requires to be tested under its real physical conditions of utilization, and this can generate implementation and safety problems. In addition, the question of whether it is an advantage or a disadvantage that passive systems do not allow operator intervention during its operation, should be investigated.

Acknowledgment

The RMPS project has been supported by the European Commission within the framework of the fifth R&D program.

References

Barre, F., Bernard, M., 1990. The CATHARE code strategy and assessment. Nuclear Eng. Des. 124, 257–284.

Bjerager, P., 1989. Methods for Structural Reliability Computations. Technical Report. Lecture Notes for the Course Structural Reliability: Methods and Applications. University of California, Berkeley, 27–29 April.

Burgazzi, L., 2002. Passive system reliability analysis: a study on isolation condenser. Nuclear Technol. 139 (July), 3–9.

D'Auria, F., Giannotti, W., 2000. Development of a code with the capability internal assessment of uncertainty. Nuclear Technol. 131 (2), 159–196.

Devictor, N., March 2004. Advances in methods for uncertainty and sensitivity analysis. In: Proceedings of the Workshop "Level 2 PSA and Severe Accident Management", OECD/NEA/CSNI/WGRISK, Köln.

Gautier, G.-M., Bazin, P., Chataing, Th., Gully, Ph., Lavialle, G., 1999. Passive heat removal system with the "base operation passive heat removal" strategy application with primary heat exchangers. In: Proceedings of the International Conference ICONE, vol. 7, 20–23 April.

Gläser, H., 2002. Experience in application of uncertainty methods and review of methods used in licensing. In: Exploratory OECD Meeting of Experts on Best Estimate Calculations and Uncertainty Analysis, Aix-en-Provence, France, 13–14 May.

IAEA, 1991. Safety Related Terms for Advanced Nuclear Plant, IAEA TECDOC-626.

Jafari, J., D'Auria, F., Kazeminejad, H., Davilu, H., 2003. Reliability evaluation of a natural circulation system. Nuclear Eng. Des. 224, 79–104.

Madsen, H., et al., 1986. Methods of Structural Safety. Prentice Hall.

Marquès, M., Pignatel, J.F., D'Auria, F., Burgazzi, L., Müller, C., Cojazzi, G., La Lumia, V., 2002. Reliability methods for passive safety functions. In: Proceedings of the International Conference ICONE, vol. 10, Arlington, VA, USA, 14–18 April.

Melchers, R.E., 1999. Structural Reliability Analysis and Prediction. John Wiley & Sons.

OECD, 2002. Passive system reliability. A challenge to reliability engineering and licensing of advanced nuclear power plants. In: Proceedings of an International Workshop, OECD/NEA/CSNI/R(2002)10, Cadarache, France, 4–6 March.

Rackwitz, R., et al., 1979. Structural reliability under combined random load sequences. Comput. Struct. 9, 489–494.

Rajashekhar, et al., 1993. A new look at the response surface approach for reliability analysis. Struct. Safety 12, 205–220.

Rubinstein, R.Y., 1981. Simulations and Monte-Carlo Method. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons.

Saltelli, et al., 2000. Sensitivity Analysis. John Wiley & Sons.

Zio, E., Cantarella, M., Cammi, A., 2003. The analytic hierarchy process as a systematic approach to the identification of important parameters for the reliability assessment of passive systems. Nuclear Eng. Des. 226, 311–336.