# Best Links Between PSA and Passive Safety Systems Reliability


Christian Kirchsteiger, Ricardo Bolado Lavín

European Commission
DG JRC - Institute for Energy
Nuclear Safety Unit
Probabilistic Risk & Availability Assessment Sector

August 2004

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

EUR 21303 EN

Mission of the Institute for Energy

The Institute for Energy provides scientific and technical support for the conception, development, implementation and monitoring of community policies related to energy.
Special emphasis is given to the security of energy supply and to sustainable and safe energy production.

**European Commission**
Directorate General Joint Research Centre (DG JRC)
Institute for Energy
Petten
The Netherlands

**Contact:**
Christian Kirchsteiger Tel.: +31 (0) 224 56 5118
E-mail: christian.kirchsteiger@jrc.nl
Ricardo Bolado Lavin Tel.: +31 (0) 224 56 5349
E-mail: ricardo.bolado-lavin@jrc.nl

http://ie.jrc.cec.eu.int/

http://www.jrc.cec.eu.int/



Luxembourg: Office for Official Publications of the European Communities, 2004

**EUR 21303 EN**



Printed in The Netherlands, Institute for Energy – JRC IE, PR & Communication

COVER: JRC IE, PR & Communication

# Best Links Between PSA and Passive Safety Systems Reliability

Christian Kirchsteiger, Ricardo Bolado Lavín

European Commission
DG JRC - Institute for Energy
Nuclear Safety Unit
Probabilistic Risk & Availability Assessment Sector

**August 2004**

*DISTRIBUTION LIST*

**JRC**
*(in alphabetical order)*

M. Becquet
M. Bieth
R. Bolado
M. Fütterer
R. Hurst
C. Kirchsteiger
J. Kubanyi
K. Müller
M. Patrik
M. Steen
K. Törrönen
H. Weißhäupl
H. Wider
R. Zeyen, Cadarache

P. Frigola, DG JRC

Secretariat NSU/PSA (10 copies)

**External to JRC**
*(in alphabetical order)*

S. Casalta, EC - DG RTD
J. Cleveland, IAEA
G. Van Goethem, EC - DG RTD
H. Zatlkajova, EC - DG TREN

For Endorsement:

Head of Unit: NSU

Name: H. Weißhäupl

Date: 24/09/04

Signature:

Competent Director: JRC-IE

Name: K. Törrönen

Date: 24.9.04

Signature:

# Preface

This report addresses the topic of incorporation of passive safety systems, as currently proposed for advanced reactor designs, into future Probabilistic Safety Assessment (PSA) studies of accordingly designed future nuclear power plants and discusses, for the different degrees of passiveness of such systems, some basic problems with regard to numerical estimation of their reliabilities and inclusion of such estimates in plant-specific PSA models.

Further RTD needs to overcome these problems for practical applications are identified.

The relevance of this topic is due to the strong role which PSA is likely to play in future for safety verification of advanced reactor designs, such as Generation IV, after it has become international consensus among safety experts in the last years that passive safety systems do not have a "quasi-zero" failure probability, as was previously often claimed (unreliabilities resulting from the case studies performed are in the order of $10^{-3}$-$10^{-2}$).

# Contents


1. Advanced Reactors and Passive Safety Systems 1

2. Passive System Reliability 4

2.1 Background 4

2.2 An Approach to Quantify Reliability of T-H Passive Systems 5

3. Inclusion of Passive Safety Systems in PSA 9

3.1 Approaches discussed within RMPS 9

3.2 Inclusion of Passive Safety Systems in Classical PSA Models 11

3.3 Inclusion of Passive Safety Systems in Dynamic PSA Models 12

4. Conclusions 14

References 15

# 1. Advanced Reactors and Passive Safety Systems

Forecasted future needs of energy supply in Europe and other developed countries triggered during the late 1980's the first research and development activities on **advanced reactors**, which encompass reactor designs of the so-called Generations III, III+ and IV types, as shown in Figure 1.

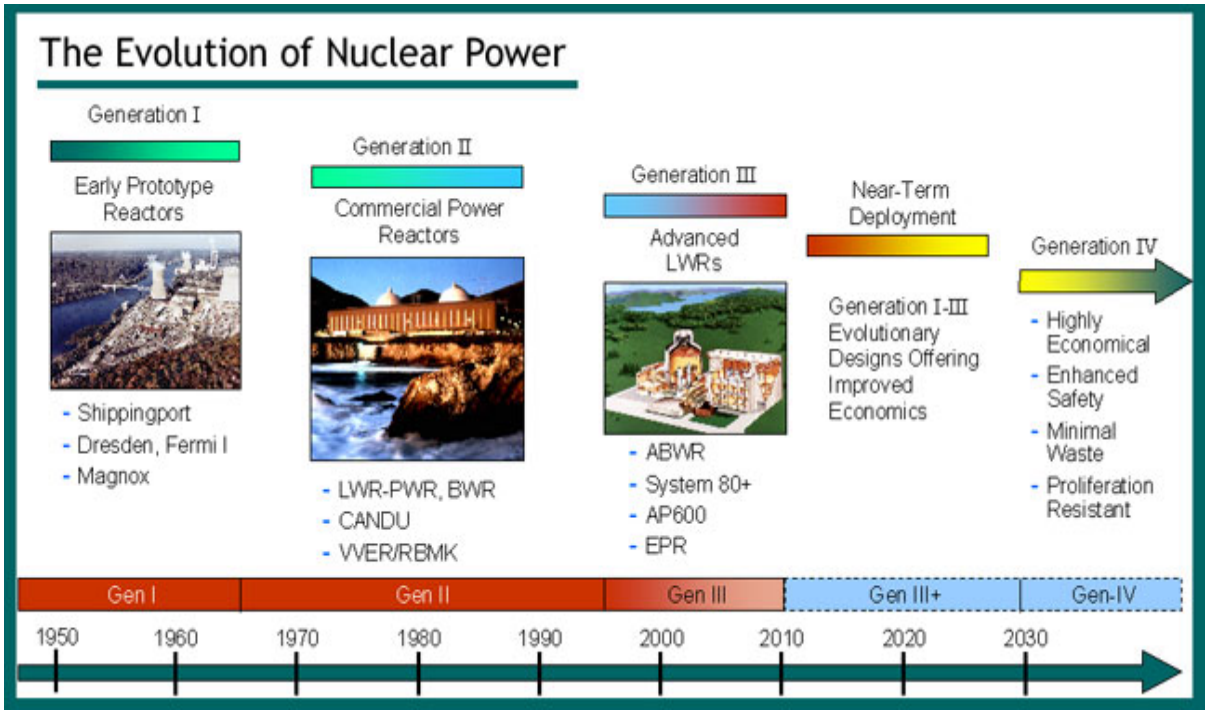


Figure 1: Generation I - IV Reactor Types (from http://gen-iv.ne.doe.gov/)

Regarding safety, specifically for Generation IV, it is consensus that, among other goals, such reactors must have a very low likelihood of core damage, be tolerant of human error and have an extremely low probability of accidental offsite release of radiation. Lower core damage frequency does not necessarily lead to higher costs. In fact, a focus on economics could result in new approaches that simplify the design and operation [1].

Essentially, these goals ask for new safety system designs which are much more reliable, have less human involvement for start-up and operation, and are simpler with regard to functional dependencies, backups etc.

The approach followed for achieving these safety goals consists of:

- Incorporation of **inherent safety characteristics** (larger water inventories, negative Doppler and moderator temperature coefficients and negative moderator void coefficients and larger containment volumes, among other possibilities) and implementation of proven high reliability engineered components.

- Use of **passive safety systems**, at least in some "evolutionary designs"[1] and in most of the "innovative designs"[2], as much for the residual core heat removal as for the mitigation in the containment phase (i.e. passive auto catalytic recombiners and core catchers).

**Passive systems** are defined by the International Atomic Energy Agency (IAEA) as systems that are entirely composed of passive components and structures or that use active ones in a very limited way to initiate subsequent passive operation. Components and structures are considered passive when no reliance on external forces, power or signal exists [2].

Passive systems are normally used as a second line of defence in the event of failure of an active system, though they can also be used as a first line of defence, keeping an active system as a second defence line. In some cases of innovative designs, the **degree of passiveness** in the whole design is very large.

The way IAEA currently classifies passive safety systems is [2]:

Category A, characterized by:
- no signal inputs of "intelligence", no external power sources or forces,
- no moving mechanical parts[3],
- no moving working fluid.

Examples for Category A systems are physical barriers and static structures (e.g. pipe wall, concrete building).

Category B, characterized by:
- no signal inputs of "intelligence", no external power sources or forces,
- no moving mechanical parts, but
- moving working fluids.

The movement of the fluid is only due to the thermo-hydraulic conditions present when activating the safety function. No distinction is made between different types of fluids, although this may have significant impact on the availability of the safety function. Examples for Category B systems are those based on free convection cooling.

Category C, characterized by:
- no signal inputs of "intelligence", no external power sources or forces, but
- moving mechanical parts, independent of presence of moving working fluids.

The movement of the fluid is characterized as for Category B; mechanical movements are due to imbalances within the system (e.g. static pressure in check and relief valves, hydrostatic pressure in accumulators) and forces directly exerted by the process. Examples for Category C systems are check valves.

Category D: This category addresses the transition area between active and passive where the execution of the safety function is made by means of passive methods as described for the previous categories, except that internal "intelligence" is not available here to initiate

[1] Generation III: ABWR, System 80+, AP-600 and EPR.
[2] Generation III+: EPP-1000, WWER-1000, ESBWR, SWR-1000, CANDU-9, AC-600, WWER-640, MS-600, HSBWR, CANDU-6, Indian AHWR, PIUS, ISIS, VPBER-600, JPSR, SPWR; and Generation IV: HTR/VHTR, SCWR, GFR, LFR and MSR.
[3] The no-motion requirement does not extend to unavoidable changes in geometry such as thermal expansion.

the passive process, but an external signal ("passive execution / active initiation"). Additional criteria for such systems which are related to the initiation process are:

- energy must be obtained only from stored sources such as batteries or compressed or elevated fluids, excluding continuously generated power such as normal AC power from continuously operating machinery;
- use of active components to initiate safety system operation is limited to controls, instrumentation and valves (single-action valves relying on stored energy;
- manual initiation is excluded.

Examples for Category D systems are scram systems.

# 2. Passive System Reliability

## 2.1 Background

Theoretically, a passive system should be much more reliable than an active one as it does not need any external input or energy to operate and it relies only upon

- the natural laws of physics (e.g. gravity, natural circulation, convection, etc.) and/or
- inherent characteristics (properties of materials, internally stored energy, etc.) and/or
- "intelligent" use of the energy that is inherently available in the system (e.g. decay heat, chemical reactions, etc.) [2,3].

Historically, in the 1980's when passive safety system designs were probably first considered explicitly, the attitude of safety analysts has been to allocate an "almost perfect" reliability, i.e. probability P≅1, to passive systems and consequently ignored the need for their inclusion in PSA or, in general, plant reliability models[4]. Essentially, the argument was that a passive safety system has already a small unavailability to come into operation due to hardware failure and human error and that the likelihood of the occurrence of physical phenomena leading to pertinent failure modes of the system, once it comes into operation, can be considered zero as these phenomena rely entirely on the (deterministic) laws of nature, thus having probability 1 (of intended operation).

Since the 1990's, however, after observing some real deviations from intended operation (failure that control rods fall under gravity, stratification breaking natural convection, environmental phenomena diminishing radiation efficiency, etc.), passive systems were started to be considered like other engineered systems, i.e. through their physical performances under real conditions, and having reliability values P<1. Consequently, a need for inclusion of passive systems and their reliability values in PSA arose, making perhaps in future "deterministic classifications" unnecessary, such as the one done by the IAEA (see above Section 1) [4].

This realization of "non-perfect reliabilities" for passive systems can, in principle, be verified in different ways for the different IAEA Categories:

- For Category A passive systems, structural reliability analysis methods can be applied.
- For Categories C and D, sufficient operating experience should be available in order to apply the classical tools of statistical reliability analysis.
- Only for Category B systems, i.e. those which rely on natural forces and whose accident prevention and mitigation functions are, once the systems are started, not provided by means of external power sources (i.e. essentially thermo-hydraulic (T-H) systems), new

[4] somewhat similar as it is done in most of current PSA studies with regard to inclusion of conventional passive components in PSA models, such as vessels, most of the piping and structures.

methods have to be developed. Here, "non-perfect reliabilities" are generated due to the fact that the natural forces which drive the operation of the passive systems have a relatively small magnitude, thus enabling possible counter-forces, such as friction, to be of comparable, non-ignorable magnitude [5]. For such systems, a need to develop a specific quantitative reliability assessment method has been recognised at EU level and the development work in a corresponding EU research project will be described in Section 2.2.

## 2.2 An Approach to Quantify Reliability of T-H Passive Systems

To address the need to develop a method to quantitatively assess the reliability of Category B passive systems as defined in Section 2.1, a research project has been launched by the European Commission under its 5th Research Framework Program, called "Reliability Methods for Passive Systems" (RMPS), and successfully been concluded in early 2004. Main objective of RMPS was to develop a methodology to quantify the reliability of a T-H passive system. Three applications were done on three different passive safety systems [7]: The Isolation Condenser System (ICS) of a BWR, the Residual Passive heat Removal system of the Primary circuit (RP2) of a PWR, and the Hydro-Accumulator of a VVER.

The originality of RMPS is to gather methods coming from different disciplines (T-H, Structural Reliability, PSA and Monte Carlo simulation among others) and to further adapt and complete them in order to propose an efficient integrated methodology for assessing the reliability of a passive safety system.

The RMPS methodology consists of the following main steps (see also Figure 2), [7]:

1) Definition of the accident scenario of interest;
2) Characterisation of the passive safety system in terms of its mission, failure modes (FMEA) and success / failure criteria;
3) Modelling of the system by using a T-H computer code and performing best-estimate (BE) calculations[5];
4) Identification and quantification of the sources of uncertainties and determination of the important variables by using expert judgement (EJ);
5) Identification of the relevant parameters which affect accomplishment of system mission by using systematic EJ methods such as the Analytic Hierarchy Process (AHP) [8];
6) Quantification of uncertainties and their propagation through the T-H code (or a surrogate model obtained by means of, for example, response surface techniques) used to simulate the physical process and estimation of the passive system reliability (via common statistical estimation or via approximate methods such as FORM/SORM);

[5] Within RMPS, in order to validate reference calculations and to test different approaches to uncertainty analysis, the ICS has been modeled separately by the ATHLET, RELAP5 and CATHARE codes.

7) Incorporation of the estimated reliability of the passive system into the plant-specific PSA[6].

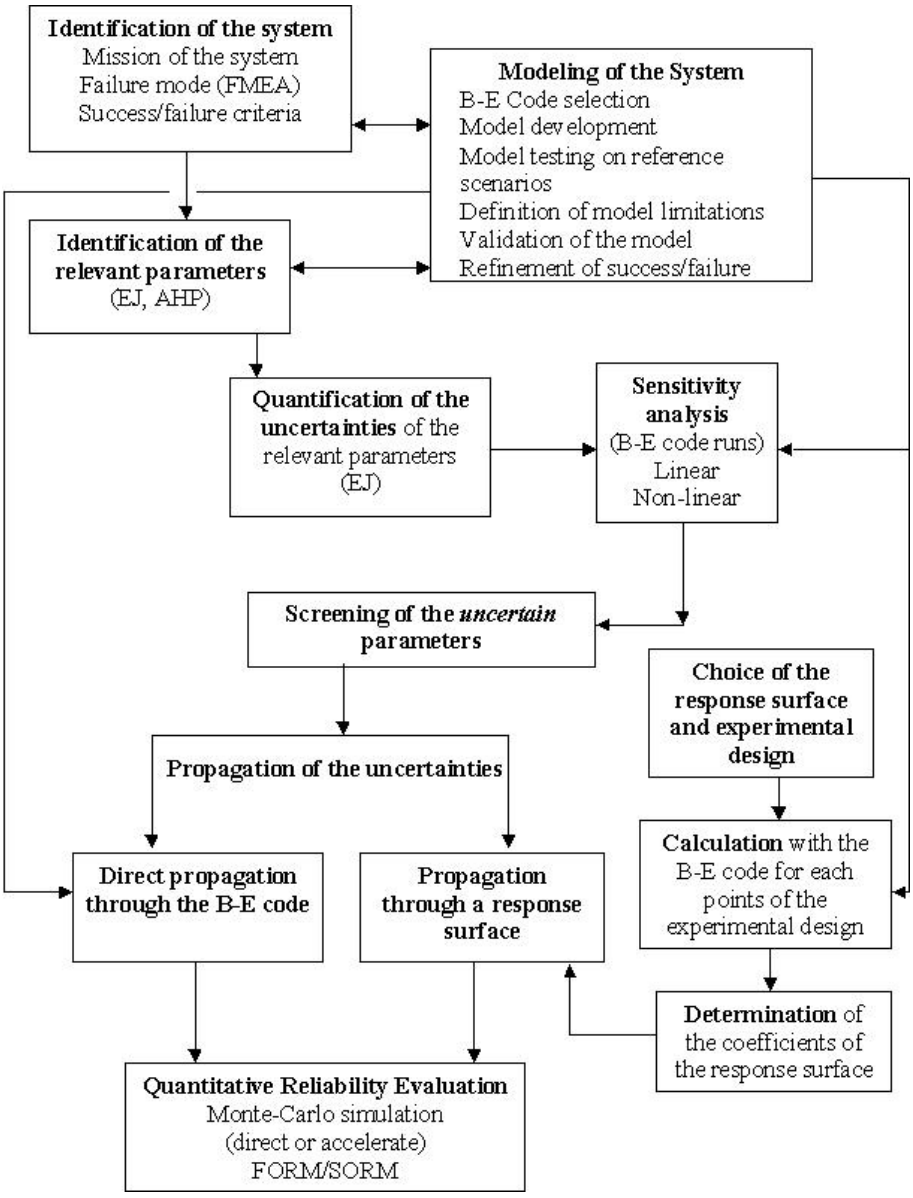


Figure 2: RMPS methodology flowchart [7].

The RMPS reliability assessment approach is based on the Resistance-Stress (R-S) model taken from Structural Reliability Analysis, where, in the present context, R and S represent a system's functional requirement (R) and state (S) and are characterised by their respective probability density functions. The structure is supposed to fail whenever the state does not fit the requirements. For example, water mass flow circulating through the system could be accounted for as physical quantity defining the (passive) system performance; the system could be considered to fail if this performance measure goes below a given reference value. In

[6] Within RMPS, this last point was, however, only touched and, due to project time constraints, no integration of the reliability assessment case studies into a real PSA model could be achieved.

other words, the mission of the passive system defines which parameter values are considered a failure by comparing the corresponding probability density functions with the respective, deterministically defined safety criteria.

Given a best estimate T-H code and a model of the (passive) system to be analysed, the performance function of this system according to its specified mission is given by:

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

in which the $X_i$ $(i=1,\ldots,n)$ are the n basic random input variables (input parameters, split up for methodological purposes in this project in design and critical parameters), and $g(.)$ is the functional relationship between the random variables and the failure of the system [7]. The performance function can be defined such that the limit state, or failure surface, is given by $M = 0$. The failure event is defined as the space where $M < 0$, and the success event as the space where $M > 0$. Thus a probability of failure can be evaluated by the following integral:

$$P_f = \int_{M<0} f_{\mathbf{X}}(\mathbf{x}) d\mathbf{x} \ , \qquad (1)$$

where $f_{\mathbf{X}}(\mathbf{x})$ is the joint density function of $X_1, X_2, \ldots, X_n$, and the integration is performed over the region where $M < 0$. Because each of the basic random variables has a unique distribution and they interact, the integral (1) cannot easily be evaluated. Two types of methods have been identified within RMPS to estimate the probability of failure: The Monte Carlo simulation with or without variance reduction techniques and some approximate methods (FORM/SORM):

- *Direct Monte Carlo simulation techniques* can be used to estimate the probability of failure defined in equation (1) (or its complement to 1, the reliability). Monte Carlo simulation consists of drawing samples of the basic variables according to their probabilistic characteristics and then feeding them into the performance function. An estimate $\hat{P}_f$ of the probability of failure $P_f$ can be found by dividing the number of simulation cycles in which $g(.) < 0$ by the total number of simulation cycles $N$. As $N$ approaches infinity, $\hat{P}_f$ approaches the true probability of failure. The accuracy of the estimation can be evaluated in terms of its variance. For a small number of simulation cycles, the variance of $\hat{P}_f$ can be quite large compared to the actual value of $P_f$. Additionally, as a rule of thumb, failure probabilities $P_f$ demand sample sizes of at least $1/P_f$ in order to get acceptable estimates. Consequently, it may take a large number of simulation cycles, mainly if the system is actually a reliable one ($P_f \approx 10^{-3} \Rightarrow N > 10^3$), to achieve a relevant accuracy and the amount of computer time needed will be large, up to several weeks, especially when each simulation cycle is performed by a T-H code.

- *Variance reduction techniques*, such as importance sampling, stratified sampling, Latin hypercube sampling, control variates, antithetic variates and directional simulation offer an increase in the efficiency and accuracy of the simulation-based assessment of the passive system reliability, providing acceptable estimate uncertainty ranges for small number of simulation cycles [7].

- *Approximate methods*, such as first- and second-order reliability methods (FORM/SORM) consist of 4 steps:
  1. Transformation of the space of the basic random variables $X_1, X_2,...,X_n$ into a space of standard normal variables (N(**0**,**I**));
  2. Determination, in this transformed space, of the point of minimum distance from the origin on the limit state surface (this point is called the design point);
  3. Approximation of the failure surface near the design point;
  4. Computation of the failure probability corresponding to the approximate 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 as compared to simulation methods. The calculation time is for FORM approximately linear in the number of basic variables and independent of the probability level. The drawback of these methods is that when the failure surface is not sufficiently smooth, problems arise in determining the design point. Additionally, the method does not provide error estimates. Response surface methods can help and within RMPS a specific method has been described to build and validate response surfaces [7].

- *Influence of choice of input distribution on output*: Knowledge uncertainty is the main source of uncertainty affecting as much design parameters as critical parameters[7]. This fact forces PSA analysts to use EJ as a main source of information for assigning probability distributions. Experts some times disagree with each other and some other times change their opinion, as more information is available, so that, in many cases, the analysis of the system under different input parameter distributions deserves some attention. The codes used to calculate the T-H performance of a passive system may require several hours for each run. As the evaluation of the reliability of a passive system may require hundreds and even thousands of calculations, this poses a serious practical problem when estimating the effect of changes in the probabilistic distributions of the input parameters on the system reliability. Within RMPS, the efficiency of two methods has been assessed to measure the influence of input distribution changes in the means and the distribution functions of the output variables (distribution sensitivity analysis), without running again the T-H code: the weighting and the rejection methods [9]. Moreover, an extension of the latter method was developed to take as much information as possible from the available sample (extended rejection method) [12]. All these methods are suitable for measuring the sensitivity to the change in one, several or all the input parameters, though with some restrictions. In some way, however, the results provided by these methods have to be considered "qualitative", since, although one gets quantitative estimates, no test is currently available to check for the statistical significance of the differences obtained.

[7] Design parameters are those that come from the connection of the passive system with the rest of the system, while critical parameters are those that characterise the passive system behaviour and account for possible system failure causes.

# 3. Inclusion of Passive Safety Systems in PSA

## 3.1 Approaches discussed within RMPS

As already mentioned, no definitive agreement was reached within the RMPS project on the way how to incorporate passive system reliability into a plant-specific PSA model and only conceptual proposals were provided by some of the participants.

It is important to note that the part of the analysis of the reliability of the passive system function which deals with possible failures of mechanical components (active initiation), was not explicitly included in the RMPS methodology (see also Figure 2), although this is obviously necessary for implementation into a real PSA model. In fact, this part was implicitly taken into account in the case studies considered, so that the passive systems studied were assumed to fail either if the active initiating components failed or if the passive process (here: natural circulation) failed. Figure 3 shows in the form of a simple Fault Tree the way how to combine both types of failures in order to describe the failure of the entire passive system.

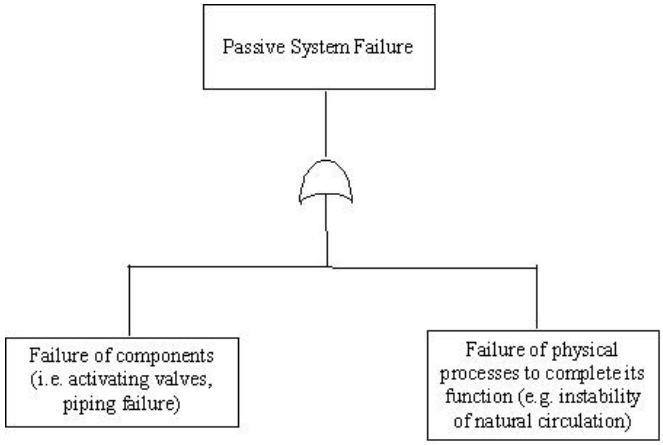


Figure 3: Combination of active components failure and physical process failure to describe passive system failure [7].

An alternative approach was provided by one of the participants in the RMPS project [3], consisting of two parts: The first part deals with the classical reliability analysis of components, the second part with the passive function which is evaluated by means of reliability analysis of the components designed to ensure the best conditions for the passive safety function (which is the innovative aspect of the proposed method).

This approach is essentially the same as the simple Fault Tree combination proposed in Figure 3, but there is a clear difference in the way how to estimate the probability of failure of the physical process: In order to achieve the mission of the passive system, there is a set of "conventional" devices and components which should perform their respective tasks as

intended (heat exchanger, pipes, vent lines to purge non-condensable gases, etc.) and there is a set of physical parameters that could affect the performance of the physical process (proportion of non-condensable gases, heat exchanger pipe fouling, etc.). It is suggested in reference [3] that relevant failure modes for both types of "components" should be found from operating experience and the whole physical process can then be modelled as a classical Fault Tree containing these "components". Figures 4-5 show an example of application of this method to the case of the ICS treated within RMPS [3].

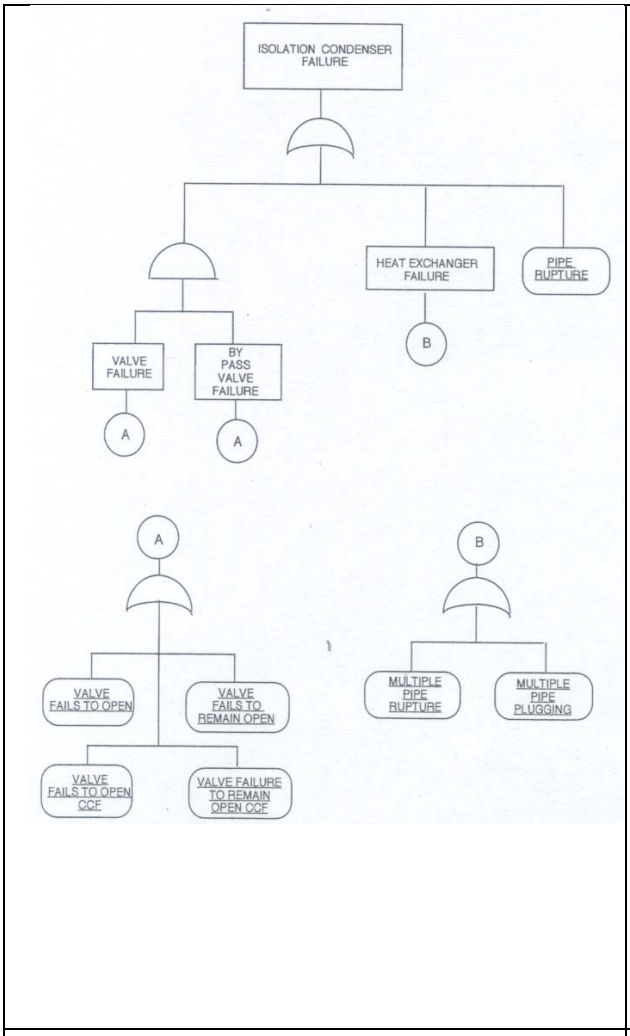


Figure 4: Fault Tree to describe the modelling of the active components failures [3].

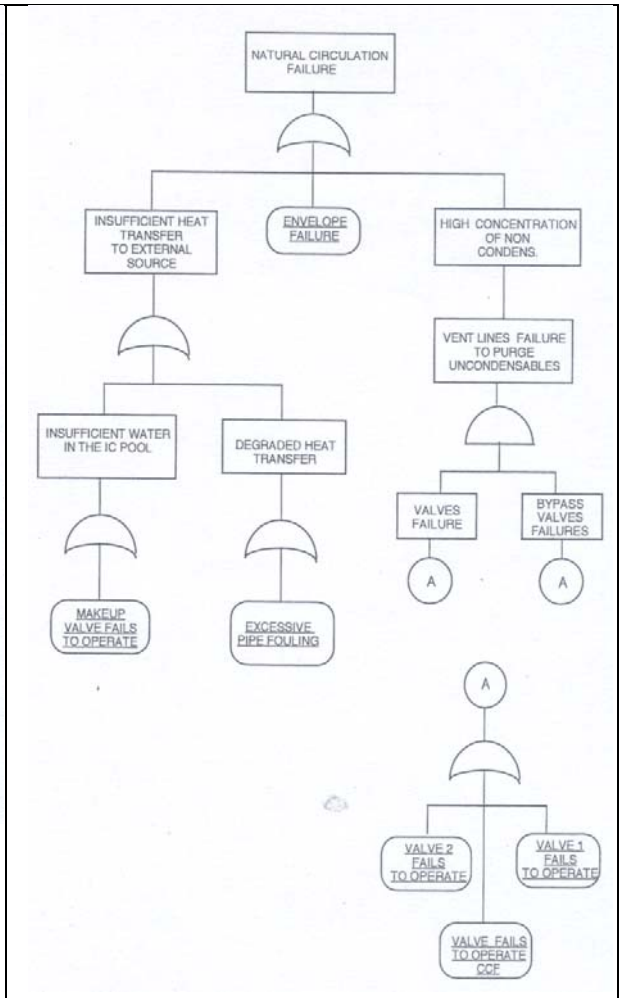


Figure 5: Fault Tree to describe the modelling of the physical process failures [3].

The example in Figure 5 defines the failure of the physical process as either due to an insufficient heat transfer to the external heat sunk or due to envelope failure (loss of primary boundary) or due to high concentration of non-condensable gases. The different parts of the Fault Tree are further developed by taking into account some physical phenomena that could impair natural circulation as well as other (active) components. Those physical phenomena are further decomposed into failures of other components that could be either active or passive (valves, pipes, etc.) following again Fault Tree structures. Later on, failure frequencies are assigned to all those components, either through common statistical tools or through EJ.

The two main shortcomings of this approach are:

- Failure of the physical process is always (eventually) related to failures of active and passive components, not acknowledging any possibility of failure just because of unfavourable initial or boundary conditions;
- The Fault Tree used for the decomposition of the physical process is used as surrogate model for a complex T-H code that models system behaviour. This decomposition is not good in foreseeing interactions among physical phenomena and makes it extremely difficult to realistically assess the impact of parametric uncertainty on the performance of the system.

**From the quantitative evaluation of the examples studied in the RMPS project [7] and in the alternative approach summarised in [3], it becomes clear that the previously suspected non-perfect reliabilities of passive safety systems are clearly confirmed (resulting unreliabilities in the order of $10^{-3}$-$10^{-2}$).**

## 3.2 Inclusion of Passive Safety Systems in Classical PSA Models

On the basis of a classical PSA model, i.e. consisting of largely static Event Trees and Fault Trees, the incorporation of a passive safety system into a PSA model could straightforwardly be achieved by introducing either an additional heading in the respective Event Tree to incorporate the success or failure of the passive safety system or two headings, the first one for the (active) initiation components of the passive safety system and the second one for the passive execution of the safety function (physical process). This represents incorporation of the top event in Figure 3 or of the two events in the lower level of the same figure in the respective Event Tree, respectively (see Figures 6-7).

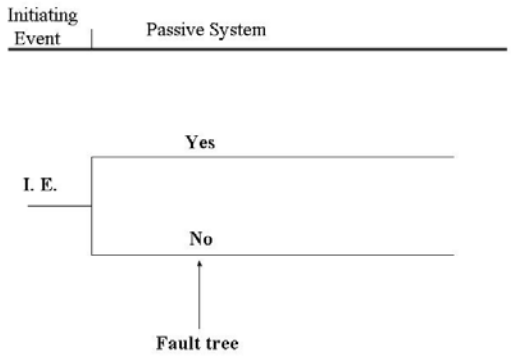


Figure 6: Incorporation of a whole passive system to an Event Tree as only one heading.

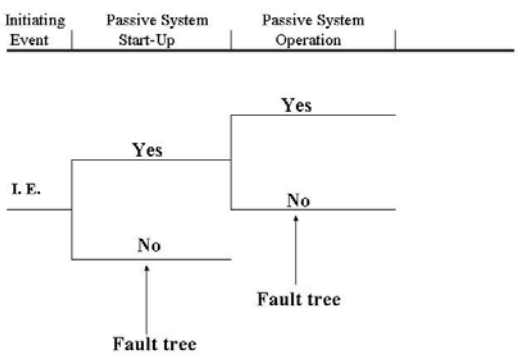


Figure 7: Incorporation of a passive system into an Event Tree as two headings.

If the estimate to be used for the Event Tree heading results from a methodology such as RMPS, one should recall the significant computational burdens related to application of such methods. For each Initiating Event there could be different initial and boundary conditions, in addition to different probability distributions for relevant physical parameters, resulting in the need for different sets of computational runs in order to assess with some acceptable accuracy the reliability of the system for each Initiating Event. Although the use of variance reduction techniques or distribution sensitivity techniques might help, this definitely needs further research in order to make "RMPS-type of reliability estimates" applicable for practical implementation in plant-specific PSAs.

## 3.3 Inclusion of Passive Safety Systems in Dynamic PSA Models

Static system models, represented by classical Event Tress / Fault Trees ("static PSA approach"), fail to reflect correctly the dynamic behaviour of a system. For a large number of systems encountered in modern industries, both the process physics and the system configuration even under normal operation can change as a result of the complex interaction between the components, process variables and the operator actions. It is not clear that the static models used in current PSA studies can correctly describe system disturbances distributed over time. This basically motivated the development of the time-dependent models to complement the classical PSA approach. The need for dynamic system reliability modelling was argued in many papers and conferences, showing its advantages against the static PSA models [10] and several methods to describe probabilistic system evolution in time were proposed during the last decade.

A dynamic system in the context of a reliability study is defined as the system in which physical processes are important system characteristics and explicitly define success criteria for the system performance. Contrary to static system models (e.g. Event Tress / Fault Trees approach), where time determines only chronology of the events, the time variable plays an essential role in reliability computations of dynamic systems: The deterministic trajectories of the physical processes are influenced at random times by the stochastic changes in the structure of the system, by failure, controls or operator actions [11].

One of the fundamental problems dealing with risk of a technical installation is to evaluate possibilities that physical variables representing the system will go across specified (safety) performance boundaries. Many practical examples can be given as, for instance, water level in a dam reservoir (overtopping may lead to dam breach), temperature of fuel cladding in a nuclear reactor (high temperature may lead to fuel melt) or pressure inside a containment of a nuclear reactor (high pressure may lead to containment break leading to radioactive release to the environment).

In the context of the static PSA approach this problem is hidden within the success criteria for the specific systems. Success criteria are defined according to the engineering judgement of required system resources to perform a specific task (e.g. to reduce pressure). The engineering judgment is usually supported by deterministic calculations of the process behaviour under specific accident conditions and component states. The common problem when defining

success criteria is that due to a large number of component states, it is impossible to cover all possible scenarios. However, the judgement based on the most evident and conservative scenarios may lead to the omission or incorrect scheduling of the functions in the Event Tree.

A nuclear power plant under accident conditions is a dynamic system in which a physical process, characterized by a set of partial differential equations and a set of physical variables and parameters, interacts with protection systems and random failures of components. In the case of a fully passive system, the dynamic approach to reliability analysis would not make much sense, since the evolution of the system should sufficiently well be characterised by the deterministic equations describing the physical process (see also Section 2.1).

In general, passive systems are not typical systems to be included into dynamic plant models at system level. The main feature of passive systems is that once started with some specific values of system parameters (e.g. number of trains in operation, percentage of non-condensable gases, initial pressure, temperature, etc.), the outcome of the system performance is deterministic and can be predicted by T-H computations.

As many of the so-called passive safety systems have usually some active components included to perform their intended function or have interactions with active systems, some parts of such systems are subject to potential failures (tube rupture in heat exchangers, valves, etc.) and their inclusion into a "dynamic PSA", i.e. a PSA model consisting essentially of dynamic Event Trees, is, in principle, a reasonable option.

Also, there should be no potential problem with the inclusion of passive systems in dynamic reliability studies since they do not provide additional simulation problems. Computer codes used to simulate natural circulation and similar passive processes are widely used in such types of analysis.

However, as dynamic reliability models are more complicated and corresponding computations time-consuming, further research is needed in the area of the computational challenges posed by dynamic reliability in order to develop more cost-effective methods.

# 4. Conclusions

**Regarding reliability evaluation,** the strong reliance of passive safety systems on inherent physical principles makes quantification of the reliability of such systems difficult as compared to classical systems analysis. As discussed in Section 2 of this report, the main problems related to the generation of dependable reliability values for passive safety system functions[8] are:

- large T-H uncertainties in the system modelling,
- the necessary large numbers of simulation cycles and thus long calculations times in practical applications,
- theoretical gaps in the development of uncertainty/sensitivity analysis methodological approaches, e.g. missing tests for significance, etc.

**One of the most important results from the studies performed so far is the confirmation of non-perfect reliabilities of passive safety systems (resulting unreliabilities are in the order of $10^{-3}$-$10^{-2}$).**

**Future RTD efforts here** should focus on systematic identification, quantification and reduction of uncertainties that appear in the reliability process as well as corresponding fundamental research in statistical methods. On this specific topic, JRC-IE is participating in a new (November 2004) IAEA Coordinated Research Project on "Natural Circulation Phenomena, Modeling and Reliability of Passive Systems that Utilize Natural Circulation" with the main task to perform a systematic classification of uncertainties related to the modelling of natural circulation phenomena in passive systems (see also *http://www.energyrisks.jrc.nl*).

**Regarding inclusion of passive systems reliability estimates in future PSA studies,** as the discussions in Section 3 of this report have shown, merging probabilities with T-H models, i.e. dynamic reliability, is necessary for realistic plant safety modelling since the operation of a passive safety system in the context of all the other systems of a nuclear power plant is strongly dependent on time and its required mission time could be much larger than the 24 hours typically used in conventional PSA Level 1 applications.

**Future RTD efforts here** should focus on the further development of dynamic PSA models in order to make corresponding applications less time-consuming in terms of computational effort involved.

[8] i.e. essentially for Category B systems (see Sections 1 and 2).

# References


[1] http://gen-iv.ne.doe.gov/pdf/workshop.pdf

[2] SAFETY RELATED TERMS FOR ADVANCED NUCLEAR PLANTS, TECDOC-626, IAEA, Vienna, 1991.

[3] L. Burgazzi, PASSIVE SYSTEM RELIABILITY ANALYSIS: A STUDY OF THE ISOLATION CONDENSER, Nuclear Technology, Vol. 139, July 2002.

[4] Personal Communication with G.L. Fiorini, CEA, France, 2004.

[5] L. Burgazzi, TECHNICAL OPINION PAPER ON RELIABILITY OF PASSIVE SYSTEMS, Contribution to OECD Working Group Risk, OECD/NEA, Paris, 2004.

[6] M. Marquès, J.F. Pignatel, F. D'Auria, L. Burgazzi, C. Müller, R. Bolado-Lavin, V. Kopustinskas, C. Kirchsteiger, V. La Lumia, I. Ivanov, RELIABILITY METHODS FOR PASSIVE SAFETY FUNCTIONS, Proceedings of FISA-2003 Symposium on EU Research in Reactor Safety, EC, Luxembourg, 10-13 November 2003.

[7] M. Marques, J.F. Pignatel, F. D'Auria, L. Burgazzi, C. Mueller, R. Bolado Lavín, V. La Lumia, I. Ivanov, RELIABILITY METHODS FOR PASSIVE SAFETY FUNCTION PROJECT, Contract Nr FIKS-CT-2000-00073, Final Report, July 2004 (for RMPS related information, see also: *http://www.energyrisks.jrc.nl*).

[8] T.L. Saaty, THE ANALYTIC HIERARCHY PROCESS: PLANNING SETTING PRIORITIES, RESOURCE ALLOCATION, McGraw-Hill, New York, 1980.

[9] R. Bolado, NOTES ON TWO MONTE CARLO METHODS FOR ESTIMATING THE INFLUENCE OF DIFFERENT INPUT DISTRIBUTIONS ON THE OUTPUT DISTRIBUTION FROM A COMPUTER CODE SIMULATION, JRC technical note TN.P.03.84, Petten, April 2003.

[10] N. Siu, RISK ASSESSMENT FOR DYNAMIC SYSTEMS: AN OVERVIEW, Reliability Engineering and System Safety, Elsevier Science, Vol. 43, p.43-73, 1994.

[11] V. Kopustinskas, MEMO ON DYNAMIC RELIABILITY EXTENSION TO RMPS PROJECT, JRC, Petten, February 2004.

[12] R. Bolado, J. Valero, DISTRIBUTION SENSITIVITY ANALYSES FOR THREE DIFFERENT SCENARIOS WITHIN THE RP2 SYSTEM CASE STUDY, JRC technical report EUR 20980 EN, September 2003.

European Commission

# EUR 21303 EN Best Links Between PSA and Passive Safety Systems Reliability

Christian Kirchsteiger
Ricardo Bolado Lavin

Luxembourg: Office for official Publications of the European Communities

2004 – 23 pp. – 21 x 29.7 cm

Scientific and Technical Research series

EUR 21303 EN

The mission of the Joint Research Centre is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of European Union policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Community. Close to the policy-making process, it serves the common interest of the Member-States,while being independent of commercial or national interests.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Publications Office
Publications.eu.int