Open Issues Associated With Passive Safety Systems Reliability Assessment

L. Burgazzi

ENEA, Italian National Agency for New Technologies, Energy and Sustainable Economic Development
Bologna, Italy

Abstract. The efforts conducted so far to deal with and evaluate the reliability of passive safety systems (as the thermal-hydraulic passive systems), being implemented in advanced water cooled reactor designs, has aroused an amount of open issues. They should be addressed and conveniently worked out, since it is the major goal of the international community (e.g IAEA) to strive to harmonize the different approaches and to reach a common consensus, in order to add credit to the underlying models and the eventual outcoming reliability figures. The main open points are presented and discussed and a viable path towards the implementation of the research efforts is delineated as well.

1. INTRODUCTION

In order to address the issues posed by the development of advanced nuclear technologies, the reliability of passive systems has become an important subject and area under discussion, for their extensive use in future nuclear power plants. [1]

Following the IAEA definitions, [2], a passive component does not need any external input or energy to operate and it relies only upon natural physical laws (e.g. gravity, natural convection, conduction, etc.) and/or on 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.). The term "passive" identifies a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation.

Inclusion of failure modes and reliability estimates of passive components for all systems is recommended in probabilistic safety assessment (PSA) studies. This has aroused the need for the development and demonstration of consistent methodologies and approaches for their reliability evaluation and eventually for their integration in the accident sequences, within the community of the nuclear safety research. Special emphasis has been placed on the reliability of the systems based on thermal-hydraulics (i.e. resting on natural circulation), for which there isn't yet an agreed approach and for which different methods have been conceived and implemented. [3]

IAEA recently coordinated a reserarch project, denoted as "*Natural Circulation Phenomena, Modelling and Reliability of Passive Systems"* (2004-2008), [4,5], while another coordinated research project on "*Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors"* (2008-2011) is currently underway: the objective is to determine a common analysis-and-test method for reliability assessment of passive safety system performance. However, the efforts conducted so far to deal with the passive safety systems reliability, have raised an amount of open issues to be addressed in a consistent way, in order to endorse the proposed approaches and to add credit to the underlying models and the eventual reliability figures, resulting from their application. In fact the applications of the proposed methodologies are to a large extent dependent upon the assumptions underlying the methods themselves.

This paper provides the insights resulting from the analysis on the technical issues associated with assessing the reliability of passive systems in the context of nuclear safety and probabilistic safety analysis, and a viable path towards the implementation of the research efforts in the related areas is delineated as well.

Focus on these issues is very important since it is the major goal of the international research activities (e.g. IAEA) to strive to reach a common consensus about the different proposed approaches. The paper is organised as follows: at first the current available methodologies are illustrated and compared, the open issues coming out from their analysis are identified and for which one of them the state of the art and the outlook is presented.

1.1. Methodologies description and comparison

A very good description of the various methodologies proposed so far and currently available in the open literature is provided in [6]. A more detailed description of these methodologies is given as well in [5].

The earliest significant effort to quantify the reliability of such systems is represented by a methodology known as REPAS (Reliability Evaluation of Passive Systems) [7], which has been developed in late 1990s, cooperatively by ENEA, the University of Pisa, the Polytechnic of Milan and the University of Rome, that was later incorporated in the EU (European Union) RMPS (Reliability Methods for Passive Systems) project. This methodology is based on the evaluation of a failure probability of a system to carry out the desired function from the epistemic uncertainties of those physical and geometric parameters which can cause a failure of the system.

The RMPS methodology, [8], was developed to address the following problems: 1) Identification and quantification of the sources of uncertainties and determination of the important variables, 2) Propagation of the uncertainties through thermal-hydraulic (T-H) models and assessment of passive system unreliability and 3) Introduction of passive system unreliability in accident sequence analyses. In this approach, the passive system is modelled by a qualified T-H code (e.g. CATHARE) and the reliability evaluation is based on results of code runs, whose inputs are sampled by Monte-Carlo (M-C) simulation. This approach provides realistic assessment of the passive system reliability, thanks to the flexibility of the M-C simulation, which adapts to T-H model complexity without resort to simplifying approximation. In order to limit the number of T-H code runs required by M-C simulation, alternative methods have been proposed such as variance reduction techniques, first and second order reliability methods and response surface methods. The RMPS methodology has been successfully applied to passive systems utilizing natural circulation in different types of reactors (BWR, PWR, VVER). The RMPS methodology tackles also an important problem, which is the integration of passive system reliability in a Probabilistic Safety Assessments (PSA). So far, in existing innovative nuclear reactor projects PSA’s, only passive system components failure probabilities are taken into account, disregarding the physical phenomena on which the system is based, such as the natural circulation. The first attempts performed within the framework of RMPS have taken into account the failures of the components of the passive system as well as the impairment of the physical process involved like basic events in static event tree [8].

In addition to the RMPS approach, a number of alternative methodologies have been investigated for the reliability assessment of T-H passive systems.

Three different methodologies have been proposed by ENEA. In the first methodology [9], the failure probability is evaluated as the probability of occurrence of different independent failure modes, a priori identified as leading to the violation of the boundary conditions or physical mechanisms needed for successful passive system operation. In the second [10], modelling of the passive system is simplified by linking to the modelling of the unreliability of the hardware components of the system: this is achieved by identifying the hardware failures that degrade the natural mechanisms upon which the passive system relies and associating the unreliability of the components designed to assure the best conditions for passive function performance. The third approach is based on the concept of functional failure, defined as the probability of the passive system failing to achieve its safety function as specified in terms of a given safety variable crossing a fixed safety threshold [11].

Finally a different approach is followed in the APSRA (Assessment of Passive System ReliAbility) methodology developed by BARC (Bhabha Atomic Research Centre, India), [12]. In this approach, a failure surface is generated by considering the deviation of all those critical parameters, which influence the system performance. Then, the causes of deviation of these parameters are found through root diagnosis. It is attributed that the deviation of such physical parameters occurs only due to a failure of mechanical components such as valves, control systems, etc. Then, the probability of failure of a system is evaluated from the failure probability of these mechanical components through classical PSA treatment. Moreover, to reduce the uncertainty in code predictions, BARC foresee to use in-house experimental data from integral facilities as well as separate.

As highlighted above, all three methods devised by ENEA share with the main RMPS approach the issue related to the uncertainties affecting the system performance assessment process. With respect to the RMPS a greater simplicity is introduced, although detrimental to the relevance of the approaches themselves: this is particularly relevant as far as the approach based on hardware components failure is concerned. The approach based on independent failure modes introduces a high level of conservatism as it appears that the probability of failure of the system is relevantly high, because of the combination of various modes of failure, where a single fault is sufficient to challenge the system performance. The correspondent value of probability of failure can be conservatively assumed as the upper bound for the unavailability of the system, within a sort of “parts-count” reliability estimation. Finally the main drawback in the last ENEA method lies in the selection and definition of the probability distributions that describe the characteristic parameters, based mainly on subjective/engineering judgement.

With reference to the two most relevant methodologies (i.e. RMPS and APSRA), the RMPS consists mainly in the identification and quantification of parameter uncertainties in the form of probability distributions, to be propagated directly into a thermal-hydraulic code or indirectly in using a response surface; the APSRA methodology strives to assess not the uncertainty of parameters but the causes of deviation from nominal conditions, which can be in the failure of active or passive components or systems. In this respect, APSRA incorporates an important effort on qualification of the model and use of the available experimental data. It has to be recognized that these aspects have not been studied within the context of the RMPS project.

1.2. Open issues

From the examination of the various methodologies, which have been developed over these most recent years within the community of the safety research, and are currently available in the open literature, the following open questions are highlighted and consequently needs for research in all related areas are pointed out :

- the aspects relative to the assessment of the uncertainties related to passive system performance: they regard both the best estimate t-h codes used for their evaluation and system reliability assessment itself;

- the dependencies among the parameters, mostly t-h parameters, playing a key role in the whole process assessment;

- the integration of the passive systems within an accident sequence in combination with active systems and human actions;

- the consideration for the physical process and involved physical quantities dependence upon time, implying, for instance, the development of dynamic event tree to incorporate the interactions between the physical parameter evolution and the state of the system and/or the transition of the system from one state to another.

- It’s worth noticing that these two last aspects are correlated, but hey will be treated separately.

- the comparison between active and passive systems, mainly on a functional viewpoint.
- All of these points are elaborated in the following, in an attempt to cover the entire spectrum of issues related to the topic, and capture all the relevant aspects useful for fulfilling a significant advance.

1.3. Uncertainties

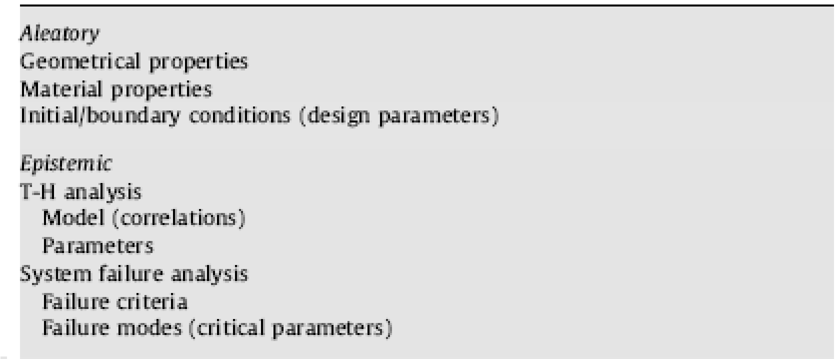
Since the magnitude of the natural forces, which drive the operation of passive systems, is relatively small, counter-forces (e.g. friction) can be of comparable magnitude and cannot be ignored as is generally the case with pumped systems. The relative uncertainties, mainly due to the lack of operational and experimental data address the deviations of the system performance from the expectation, mainly because of the onset of thermal-hydraulic phenomena that may defy the physical principle upon which the system is relying [13], so that the passive system may fail to meet the required function. The approach described in [13] allows identifying the uncertainties pertaining to passive system operation in terms of critical parameters driving the modes of failure, as, for instance, the presence of non-condensable gas, thermal stratification and so on.

There are two facets to uncertainty that, because of their natures, must be treated differently when creating models of complex systems. They have recently been termed aleatory and epistemic uncertainty. The aleatory uncertainty is that addressed when the events or phenomena being modelled are characterized as occurring in a "random" or "stochastic" manner, and probabilistic models are adopted to describe their occurrences. It is this aspect of uncertainty that gives PRA the probabilistic part of its name. The epistemic uncertainty is that associated with the analyst's confidence in the predictions of the PRA model itself, and it reflects the analyst's assessment of how well the PRA model represents the actual system being modelled. This has been referred to as state-of-knowledge uncertainty. In this context the critical parameters are recognized as epistemic uncertainties.

Ref. [13] points out, as well, the difference between the uncertainties related to passive system reliability and the uncertainties related to the t-h codes (e.g. RELAP), utilized to evaluate the performance itself, as the ones related to the coefficients, correlations, nodalization, etc.: these specific uncertainties, of epistemic nature, in turn affect the overall uncertainty in t-h passive system performance.

A further step of the matter can be found in [9], which attempts to assign sound distributions to the critical parameters, to further develop a probabilistic model. Refs [6] and [9] provide a clear prospect of the uncertainties, taking into account that the overall uncertainty are both of aleatory and epistemic character, as shown in Table I.

Table 1. Categories of uncertainties associated with T-H passive systems reliability assessment [6]



Aleatory
Geometrical properties
Material properties
Initial/boundary conditions (design parameters)
Epistemic
T-H analysis
Model (correlations)
Parameters
System failure analysis
Failure criteria
Failure modes (critical parameters)

As highlighted above, clearly the epistemic uncertainties address mostly the phenomena underlying the passive operation and the parameters and models used in the thermal-hydraulic analysis of the system (including the ones related to the best estimate code) and the system failure analysis itself. Some of the sources of uncertainties include but are not limited to the definition of failure of the system used in the analysis, the simplified model used in the analysis, the analysis method and the analysis focus of failure locations and modes and finally the selection of the parameters affecting the system performance.

1.4. Dependencies

As observed in [12], both REPAS and RMPS approaches adopt a probability density function (pdf) to treat variations of the critical parameters considered in the predictions of codes. To apply the methodology, one needs to have the pdf values of these parameters. However, it is difficult to assign accurate pdf treatment of these parameters, which ultimately define the functional failure, due to the scarcity of available data, both on an experimental and operational ground. Moreover, these parameters are not really independent ones to have deviation of their own. Rather deviations of them from their nominal conditions occur due to failure/malfunctioning of other components or as a result of the combination with different concomitant mechanisms. Thus the hypothesis of independence among the failure driving parameters appears non proper.

With reference to the functional reliability approach set forth in [11], the selected representative parameters defining the system performance, for instance coolant flow or exchanged thermal power, are properly modelled through the construction of joint probability functions in order to assess the correspondent functional reliability.
A recent study shows how the assumption of independence between the marginal distributions to construct the joint probability distributions to evaluate system reliability adds conservatism to the analysis [14]: for this reason the model is implemented to incorporate the correlations between the parameters, in the form of bivariate normal probability distributions. That study has the merit to highlight the dependence among the parameters underlying the system performance: further studies are underway, with regard, for instance to the approach based on independent failure modes [9]. As described in the previous section 2, this approach begins by identifying critical parameters, properly modelled through probability functions, as input to basic events, corresponding to the failure modes, arranged in a series system configuration, assuming mutually non-exclusive independent events. It introduces a high level of conservatism as it appears that the probability of failure of the system is relevantly high to be considered acceptable, because of the combination of various modes of failure, where a single fault is sufficient to challenge the system performance.

Initial evaluations [15] reveal that the critical parameters are not suitable to be chosen independently of each other, mainly because of the expected synergism between the different phenomena under investigation, with the potential to jeopardize the system performance. This conclusion allows the implementation of the proposed methodology, by properly capturing the interaction between various failure modes.

1.5. Integration of Passive System within PSA

Ref.[16] lays the foundations for the integration of a passive system in the form of a front line system and in combination with active ones and/or human actions, within a PSA framework.

In [8] 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 a definite accident scenario and could be used to test the advantage of replacing an active system by a passive system in specific situations.

However in order to generalise the methodology, it is important to take into account the dynamic aspects differently than by their alone modelling into the T-H code. Indeed in complex situations where several safety systems are competing and where the human operation cannot be completely eliminated, this modelling should prove to be impossible or too expensive in computing times. It is thus interesting to explore other solutions already used in the dynamic PSA, like the method of the dynamic event trees, in order to capture the interaction between the process parameters and the system state within the dynamical evolution of the accident. This aspect is treated in the following.

1.6. Dynamic reliability

In order to overcome some important limitations associated with event tree development in PRA studies, such as the binary representations of system states (i.e., success or failure), disregarding the intermediate states, and the time treatment in terms of chronology of events instead of actual timing, considerations for dynamic reliability come up. This item emerges from the reflection that thermal hydraulic natural circulation passive system operation is strongly dependent, more than other safety systems, upon time and the state/parameter evolution of the system during the accident progression. Merging probabilistic models with thermal-hydraulic models, i.e. dynamic reliability, is required to accomplish the evaluation process of thermal-hydraulic passive systems in a consistent manner: this is particularly relevant with regard to the introduction of a passive system in an accident sequence, since the required mission could be longer than 24 h as usual level 1 PSA mission time.

The goal of dynamic PRA (Probabilistic Risk Assessment) is to account for the interaction of the process dynamics and the stochastic nature/behaviour of the system at various stages: it associates the state/parameter evaluation capability of the thermal hydraulic analysis to the dynamic event tree generation capability approach. The methodology should estimate the physical variation of all technical parameters and the frequency of the accident sequences when the dynamic effects are considered. If the component failure probabilities (e.g. valve per-demand probability) are known, then these probabilities can be combined with the probability distributions of estimated parameters in order to predict the probabilistic evolution of each scenario outcome.
Some important features of this methodology are:

- It would provide risk informed insights for a sort of probabilistic accident management strategy, devoted to choose the actions to prevent or mitigate the consequences of the possible accident scenarios.
- It can allow the estimation of the uncertainties in the system state, through the evaluation of uncertainties relative to input and modelling thermal hydraulic analysis by best estimate codes.
- Fewer branching are needed in the dynamic event tree generation, thus reducing the problem and any computational efforts.

For instance, the dynamics aspect comes out from the functional reliability approach [11], since each comparison in the model should be at each time t.

A preliminary attempt in addressing the dynamic aspect of the system performance in the frame of passive system reliability is shown in [17], which introduces the t-h passive system as a non-stationary stochastic process, where the natural circulation is modelled in terms of time-variant performance parameters, (as for instance mass flow-rate and thermal power, to cite any) assumed as stochastic variables. In that work, the statistics associated with the stochastic variables change in time (in terms of associated mean values and standard deviations increase or decrease, for instance), so that the random variables have different values in every realisation, and hence every realisation is different.

1.7. Comparative assessment between active and passive systems

An important point is the comparative assessment between passive and active systems [18] required to accomplish the same safety function both on an economic and functional view. Here are some of the cons and pros of the passive systems, that should be evalauted vs the corresponednt active system.

– Advantages
- No external power supply: no loss of power accident
- No human factor
- Better impact on pubblic acceptance, due to the presence of "natural forces"
- Less complex system than active and therefore economic competitiveness

– Drawbacks
- Reliance on "low driving forces", as a source of uncertainty
- Licensing requirement (open issue)
- Need for operational tests (human factor?)
- Reliability assessemnt in any case

2. CONCLUSIONS

Due to the specificities of passive systems that utilize natural circulation (small driving force, large uncertainties in their performance, lack of data…), there is a strong need for the development and demonstration of consistent methodologies and approaches for evaluating their reliability. This is a crucial issue to be resolved for their extensive use in future nuclear power plants. Recently, the development of procedures suitable for establishing the performance of a passive system has been proposed: the unavailability of reference data makes troublesome the qualification of the achieved results. These procedures can be applied for evaluating the acceptability of a passive system, specifically when nuclear reactor safety considerations are important for comparing two different systems having the same mission and, with additional investigation, for evaluating the performance of an active and passive system on a common basis. The study while identifying limitations of the achieved results or specific significant aspects that have been overlooked has suggested areas for further development or improvements of the procedures:

- the reduction of the so identified level of uncertainty pertaining to the passive system behaviour, and regarding in particular the phenomenological uncertainty. In fact, it's worth noting that these uncertainties are mainly related to the state of knowledge about the studied object/phenomenon, i.e., they fall within the class of epistemic uncertainties, thus suitable for reduction by gathering and analyzing a relevant quantity of information and data,

- the determination of the dependencies among the relevant parameters adopted to analyse the system reliability,

- the study of the dynamical aspects of the system performance, because the inherent dynamic behaviour of the system to be characterized: this translates into the development of the dynamic event tree,

- the comparison against the active system, also to evaluate the economical competitiveness, while assuring the same level of safety.

- Future research in nuclear safety addressing this specific topic relevant to advanced reactors should be steered towards all these points in order to foster and add credit to any proposed approach to address the issue, and to facilitate the proposed methods endorsement by the scientific and technical community.

REFERENCES

[1] NEA CSNI/WGRISK Workshop on Passive Systems Reliability—A Challenge to Reliability, Engineering and Licensing of Advanced Nuclear Power Plants, Cadarache, (F), 4-6/03/'02, NEA/CSNI/R(2002)10.

[2] IAEA TEC-DOC-626. Safety Related Terms for Advanced Nuclear Power Plants, 1991

[3] Burgazzi, L,. State of the Art in the Reliability of Thermal-Hydraulic Passive Systems, Reliability Engineering and System Safety, 92 (2007), 671-675.

[4] TECDOC-XXXX, "Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants", ready for publication.

[5] TECDOC-XXXX, "Natural Circulation in Water-Cooled Nuclear Power Plants: Phenomena, Modelling, and Reliability of Passive Systems that Utilize Natural Circulation", under preparation.

[6] Zio, E., Pedroni, N., "Building Confidence in the Reliability Assessment of Thermal-hydraulic Passive Systems", Reliability Engineering and System Safety, 94 (2009), 268-281.

[7] Jafari, J., D'Auria F., et al., "Reliability Evaluation of a Natural Circulation System", Nuclear Engineering and Design, 224 (2003), 79–104.

[8] Marques, M., Burgazzi L., et al., "Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment", Nuclear Engineering and Design, 235 (2005), 2612-2631.

[9] Burgazzi, L., "Addressing the Uncertainties related to Passive System Reliability", Progress in Nuclear Energy, 49 (2007), 93-102.

[10] Burgazzi, L., "Passive System Reliability Analysis: a Study on the Isolation Condenser", Nuclear Technology, 139 (2002), 3-9.

[11] Burgazzi, L., "Reliability Evaluation of Passive Systems through Functional Reliability Assessment", Nuclear Technology, 144 (2003, 145-151.

[12] Nayak, A.K., et al., "Passive System Reliability Analysis using the APSRA Methodology" Nuclear Engineering and Design, 238 (2008), 1430-1440.

[13] Burgazzi, L., "Evaluation of Uncertainties related to Passive Systems Performance", Nuclear Engineering and Design, Volume 230, (2004), pp 93-106.

[14] Burgazzi, L., "Reliability Prediction of Passive Systems based on Bivariate Probability Distributions", Nuclear Technology, 161 (2008), pp. 1-7.

[15] Burgazzi, L., "Evaluation of the Dependencies related to Passive System Failure", accepted for publication in Nuclear Engineering and Design.

[16] Burgazzi, L., "Incorporation of Passive Systems within a PRA Framework", PSAM9, 9th International Probabilistic, Safety Assessment and Management Conference, Hong Kong, 18-23 May 2008.

[17] Burgazzi, L., "About Time-variant Reliability Analysis with Reference to Passive Systems Assessment", Reliability Engineering and System Safety, 93 (2008), 1682-1688.

[18] JiYong Oh and Golay, M., "Methods for Comparative Assessment of Active and Passive Safety Systems with respect to Reliability, Uncertainty, Economy and Flexibility", poceedings of PSAM9, Hong Kong, 18-23 May 2008.