Reliability Engineering and System Safety 94 (2009) 268–281

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Building confidence in the reliability assessment of thermal-hydraulic passive systems

E. Zio *, N. Pedroni

Department of Energy, Polytechnic of Milan, Via Ponzio 34/3, 20133 Milan, Italy

ARTICLE INFO

Article history:
Received 4 May 2007
Received in revised form
31 January 2008
Accepted 10 March 2008
Available online 16 March 2008

Keywords:
Thermal-hydraulic passive system
Reliability assessment
Monte-Carlo sampling
Uncertainties
Confidence intervals
Binomial distribution
Bootstrap

ABSTRACT

Thermal-hydraulic (T-H) passive systems play a crucial role in the development of future solutions for nuclear power plant technologies. A fundamental issue still to be resolved is the quantification of the reliability of such systems.

The difficulty comes from the uncertainties in the evaluation of their performance, because of the lack of experimental and operational data and of validated models of the phenomena involved. The uncertainties concern the deviations of the underlying physical principles from the expected T-H behaviour, due to the onset of physical phenomena infringing the system performance or to changes in the initial/boundary conditions of system operation.

In this work, some insights resulting from a survey on the technical issues associated with estimating the reliability of T-H passive systems in the context of nuclear safety are first provided. It is concluded that the most realistic assessment of the passive system response to the uncertain accident conditions can be achieved by Monte-Carlo (MC) sampling of the system uncertain parameters followed by the simulation of the accident evolution by a detailed mechanistic T-H code. This procedure, however, requires considerable and often prohibitive computational efforts for achieving acceptable accuracies, so that a limitation on the MC sample size, i.e. on the number of code runs, is necessarily forced onto the analysis. As a consequence, it becomes mandatory to provide quantitative measures of the uncertainty of the computed estimates.

To this aim, two classes of statistical methods are proposed in the paper to quantify, in terms of confidence intervals, the uncertainties associated with the reliability estimates. The first method is based on the probability laws of the binomial distribution governing the stochastic process of system success or failure. The second method is founded on the concept of bootstrapping, suitable to assess the accuracy of estimators when no prior information on their distributions is available. To the authors' knowledge, it is the first time that these methods are applied to quantitatively bracket the confidence on the estimates of the reliability of passive systems by MC simulation.

The two methods are demonstrated by an application to a real passive system of literature.

1. Introduction

In nuclear safety, the expanded consideration of severe accidents, the increased safety requirements and the goal of introducing effective, yet physically transparent, safety functions has led to a growing interest in passive systems for the safety of future nuclear reactors. As a result, all innovative reactor concepts make use of passive safety features, to a large extent in combination with active safety and operational systems.

Passive systems are expected to contribute significantly to safety by combining peculiar characteristics of simplicity, reduction of human interaction and reduction or avoidance of external electrical power and signals input.

On the other hand, a fair evaluation of the effectiveness of passive systems must face, besides their economic competitiveness, the difficulty of assessing their reliability due to lack of data on some underlying phenomena, scarce or null operating experience over the wide range of conditions encountered during operation and an overall less effective and guaranteed performance as compared to active safety systems [1,2].

According to the International Atomic Energy Agency (IAEA) definitions, a passive component does not need external input (especially energy) to operate [3]. Then, the term "passive" identifies a system that is composed entirely of passive components and structures, or a system that uses active components in a very limited way to initiate subsequent passive operation.

---

* Corresponding author. Tel.: +39 2 2399 6340; fax: +39 2 2399 6309.
E-mail address: enrico.zio@polimi.it (E. Zio).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.03.006

The currently accepted categorization of passive systems, developed by the IAEA, is summarized in Table 1 [3].

Notwithstanding that passive systems are credited a higher reliability with respect to active ones, because of the reduced unavailability due to hardware failure and human error, in practice there is a non-zero probability that the physical phenomena involved in the passive operation lead to failure of the intended function. In fact, deviations in the natural forces and in the conditions of the underlying physical principles from the expected ones can impair the performance of the system itself.

This has been found especially true for type B passive systems, i.e. those involving moving working fluids and referred to in the jargon as thermal-hydraulic (T-H) passive systems. The reason lies behind the small driving forces engaging passive operation and the complex and delicate T-H phenomena determining the system performance [4]. For performing their accident prevention and/or mitigation functions, these passive safety systems rely exclusively on natural forces, e.g. gravity or natural convection, not generated by external power sources. Because the magnitude of the natural forces that drive operation is relatively small, counter-forces (e.g. friction) cannot be ignored because of comparable magnitude. This leads to uncertainty in the actual T-H system performance, which must be evaluated by a specific, systematic and rigorous methodology reliability assessment.

In this work, for completeness the four methodologies currently available in the open literature for this task are first reviewed. In the first methodology, 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 and/or physical mechanisms needed for successful passive system operation [1]. In the second, modelling of the passive system is simplified by linking to the modelling of the unreliabilities 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 relative unreliabilities of the components designed to assure the best conditions for passive function performance [5]. 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 [1,6,7]. Finally, in the reliability method for passive safety (RMPS) functions approach, the passive system is modelled by a qualified T-H system code (e.g. RELAP) and the reliability evaluation is estimated based on a Monte-Carlo (MC) simulation sample of code runs for different input conditions [2].

This latter approach provides in principle the most realistic assessment of the T-H system reliability, thanks to the flexibility of the MC simulation approach, which does not suffer from any T-H model complexity and, therefore, does not force one to resort to realistic simplifying approximations. On the other hand, the repeated T-H code runs required by the MC simulation can be computationally quite burdensome, so that a limited sample is necessarily considered. The estimates based on this limited sample must then be appropriately bracketed by confidence intervals that provide information on their robustness and significance for safety uses.

Table 1
Categorization of passive systems [3]

Category	Description
A	Physical barriers and static structures (e.g. concrete building)
B	Moving working fluid (e.g. cooling by free convection)
C	Moving mechanical parts (e.g. check valves)
D	External signals and stored energy (e.g. scram systems)

In this respect, two classes of known statistical methods for constructing confidence intervals of passive systems reliability estimates are here investigated: the first method is based on the probability laws of the binomial distribution [8]; the second method is based on the bootstrap techniques often adopted for assessing the accuracy of parameter estimators when no prior information is available on their distributions [9].

The proposed methodologies are tested and compared on a case study concerning the reliability evaluation of a two-phase natural circulation loop of an isolation condenser (IC) [10].

The remainder of the paper is organized as follows. In Section 2, the main sources of uncertainty related to T-H passive systems performance are recalled. Section 3 provides a detailed and updated survey of the methodologies and approaches for T-H passive system reliability evaluation. In Section 4, the two statistical methods proposed for the construction of confidence intervals for reliability estimates are described. Section 5 presents the results of the application of these methodologies to a real passive system. Finally, some conclusions are proposed in the last Section.

2. Uncertainties in thermal-hydraulic passive system performance

Uncertainties in the operation of T-H passive systems impact their performance: this must be accounted for in the reliability evaluations within a Probabilistic Safety Analysis (PSA) framework [7,11,12].

To effectively model these uncertainties, it is useful to separate the two kinds of uncertainty, i.e. "aleatory" and "epistemic", which, because of their nature, must be considered differently [13]. Aleatory uncertainty refers to phenomena occurring in a stochastic way: probabilistic modelling offers a sound and efficient way to describe such occurrences. Epistemic uncertainty captures the analyst's confidence in the probabilistic safety assessment (PSA) model by quantifying the degree of belief of the analysts on how well it represents the actual system; it is also referred to as *state-of-knowledge* or *subjective* uncertainty and can be reduced by gathering information and data to improve the knowledge on the system behaviour.

As might be expected, the uncertainties affecting the operation of passive systems (Table 2) are both of aleatory kind, because of the stochasticity in the occurrence of some phenomena, and of epistemic nature, because of the limited knowledge on some phenomena and processes and the paucity of the relative operational and experimental data available [12].

Aleatory uncertainties concern, for instance, the variability in the actual geometrical properties (due to differences between the

Table 2
Categories of uncertainties associated with T-H passive systems reliability assessment

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)