Transactions, SMiRT 19, Toronto, August 2007 Paper # S02/2

Application of the Stress-Strength Interference Model to the Design of a Thermal-Hydraulic Passive System for Advanced Reactors

Luciano Burgazzi

Italian National Agency for New Technologies, Energy and the Environment, Bologna, Italy

ABSTRACT

A reliability-based approach to the design of a natural circulation thermal-hydraulic passive system designed for advanced reactors is proposed. The concept of functional failure, i.e., the possibility that the load will exceed the capacity in a reliability physics framework, in terms of performance parameter is introduced here for the reliability evaluation of a natural circulation passive system, designed for decay heat removal of innovative light water reactors. Water flow rate circulating through the system is selected as passive system performance characteristic parameter and the related limit state or performance function is defined. The probability of failure of the system is assessed in terms of safety margin, corresponding to the limit state function. Results help designer determine the allowable limits or set the safety margin for the system operation parameters, to meet the safety and reliability requirements.

INTRODUCTION

This paper is focused on natural circulation passive systems, denoted as thermal-hydraulic (T-H) passive systems, to accomplish safety related functions in advanced reactors design and categorized as class B passive systems, according to IAEA classification [1], which pose the most relevant challenges with regard to the relative reliability assessment, as underlined in [2].

The study is aimed at the development of a consistent approach helpful in a reliability-based design of such a passive system, within a probabilistic context.

The reliability model is implemented in the form of the functional failure concept, i.e., the possibility that the load will exceed the capacity in a reliability physics framework, as defined in [3]. Thus, in order to evaluate the system functional reliability, that is the probability to accomplish the requested mission to achieve a generic safety function (e.g. decay heat removal), the well known stress-strength interference model drawn from mechanical reliability is introduced, in the form of performance parameters. As reported in [4], within this functional model, resistance and stress are coined as expression of functional requirement *R* and system state *S*, respectively, and probability distribution functions (pdfs) are assigned to both of them: the assessment of which parameter values are considered a failure is achieved by comparing the corresponding pdfs, according to a defined safety criterion. In the present study the issue related to the reliability of the system is differently addressed, in terms of the safety margin corresponding to the limit state function (LSF) or performance function (PF) for the determination of the allowable window for the system performance output parameters. The study is performed on a passive system which operates in two-phase natural circulation. The selected system is a loop including a heat source and a heat sink where condensation occurs via a heat exchanger. Among the physical parameters (e.g. inlet-outlet difference in coolant fluid temperature, water flow-rate through the loop, heat exchanged through the heat exchanger, pressure differential driving force) suitable for the characterization of the system performance, the physical quantity relative to the water mass flow-rate circulating through the system is accounted for. The probability that the performance parameter meets the safety criterion and doesn't exceed the design margin is quantitatively estimated, in terms of safety margin relative to the PF. In this paper at first the issue relative to natural circulation stability with regard to passive systems and relationship with reliability and safety is addressed; then the approach based on the LSF concept and the implementation of the probabilistic model with the relative safety margin are illustrated; the application of the model to the aforementioned system is shown and the results of the analysis are presented and discussed. Results help designer determine the allowable limits or set the safety margin for the system operation parameters, within a reliability-based and risk-informed design framework.

NATURAL CIRCULATION STABILITY AND SAFETY

A T-H system is identified as a system that doesn't need any external input (that is power, force or signal) to operate (or use it in a very limited way to initiate subsequent passive operation) and relies only upon natural physical laws (e.g., gravity, natural circulation, heat conduction, internally stored energy, etc.) and/or intelligent use of the energy inherently available in the system (e.g., chemical reaction, decay heat, etc.). Its reliability refers to the ability of the system to carry out the required function under the prevailing condition when required, rather than the classical component mechanical and electrical failures. During its lifetime it is subjected to events of phenomenological nature or changes of the boundary/initial conditions likely to cause deviations from the nominal expected conditions: these actions or loads may cause a change of condition or state of the system, going from the predictable nominal performance of the system to a state of degradation of the physical principle in varying degrees, up to the failure of the system. It's worth noting that, while passive systems are very sensitive to these impairing factors, active systems, as well, are subject to the same phenomenological events and changes in boundary/initial conditions that deviate the system from nominal behaviour, but is easy to compensate shifting the operating point of the active component.

Maintenance/repair or in service inspection may become necessary, with reference, for instance, to heat exchanger broken or plugged tubes faulted condition, or to water lines undergoing small leakages. In this respect, consideration for human factors, which generally passive systems are credited to dispense with, is envisaged for its potential to play an important role through periodic maintenance and inspection that can significantly affect the system reliability.

The condition of natural circulation performance can vary more or less continuously from the "success" state to a "failure" state, according to the assumed success/failure criteria in terms of performance and allowable limits for the specified output. As a simplification it should be assumed in the design stage that malfunction can occur in only a finite number of modes; each mode of malfunction (or of failure) gives rise to a design inadequacy to be addressed and satisfied during the design phase itself. Most failures should occur under combinations of fairly low, but not exceptional variations of normal conditions required for its performance and the reliability theory indicates how to deal with such a situation. The assumption that no interface problems occur between human elements and the system items, implying that human reliability is not incorporated in the reliability prediction, is stated as an important attribute as compared to active systems, except for the above considerations.

It is important, of course, that the set of modes considered cover all the failure possibilities that can be devised for the system and identified as phenomenological factors; the results of such an analysis in terms of impairing factors and critical parameters driving the failure mechanisms is reported in a recent study [5]: among these the non-condensable gases build up, heat loss, heat exchanger (HX) plugged pipes are of relevant importance.

R-S MODEL

In the following the rationale for building up a sound reliability model inferred from the structural reliability theory is described.

As a fundamental simplification it is assumed that all states of the system can be divided into two sets: the former incorporating the states failed, and the latter the states un failed or safe, separated by a limiting state of the safe set. Failure is the passage of the process parameter *S* through the limit state of safe set, which identifies the functional requirement *R* parameter. Thus the limit state is the boundary between desired and undesired performance of a structure or of a system, as in the present case. This boundary is often represented mathematically by a LSF or PF. In addition the notion of safety margin is being associated with the limit states, as suggested in [6].

The system State *S* parameter defining the physical condition of the system depends on the initial and boundary conditions, materials, layout and other random quantities that can affect the system performance; it further depends on time t, since it is a time dependent evolutionary process, and the design parameters, which conversely are nominal, deterministic variables selected in the design process. In the following, in order to simplify the problem, the temporal dependence is not accounted for. The parameter *S* is thus a random variable affected by both stochastic (e.g. initial conditions, materials, layout) and subjective uncertainties, arising mainly from the models and parameters included in the correlations - analytical and/or experimental - used to describe the thermal hydraulic system behavior, denoted as epistemic uncertainties.

As an illustrative example, let us consider the heat transmission by convection mechanism and the correlation used to depict it

$$q = h\,A\,\Delta T \tag{1}$$

in which q is the rate of convection heat transfer from the surface of area A, when the temperature difference is ΔT and h is the commonly called heat-transfer coefficient. The coefficient h, although it is dependent upon the physical properties of the fluid medium, is function of the shape and dimensions of the interface and of the nature, direction and velocity of the fluid flow. Thus the heat-transfer coefficient is propriety of the particular system under consideration. Another factor which determines h is the exact definition of "Delta T", i.e. the temperature difference between the surface and the fluid. Summarizing the coefficient h is subject to uncertainties regarding geometric properties, material properties and physical parameters.

Similarly the heat exchange surface area depends upon geometric characteristics and dimensional values and the temperature values are not the real but the mean values of the surface and coolant temperature which are considered constant, while, in reality, there is a continuous fluctuation in a certain range. Analogously, the same considerations are valid for almost all the thermal hydraulic correlations for whom either the coefficients (heat transfer coefficient, thermal conductivity coefficient, friction factor), or the physical quantities and parameters (e.g. pressure, temperature, mass flow, etc.) are respectively affected by uncertainties or are fluctuating during the reactor operation. An extensive treatment of this issue, both in terms of model and parameter uncertainties, in order to define the pdfs of the input variables to the passive system reliability assessment process in a thermal-hydraulic model, is reported in [3].

Indeterminations concern as well the failure modes and related causes and consequences such as leaks (e.g. from pipes, pools, etc.), deposit thickness (e.g. on pipe surfaces, etc.), presence of non-condensable gases, stresses, blockages (valves, if foreseen) and material defects as pointed out in [5]. Analogously uncertainties impact on the determination of the *R* parameter.

The qualitative concept of reliability assessment of passive safety functions has been introduced above. As outlined in [4], the quantitative assessment is achieved by the introduction of the LSF or PF, denoted as g(x) and defined as:

$$g(z) = r(z)-s(z) \qquad \begin{cases} > 0 \text{ for safe function} \\ = 0 \text{ at limit state} \\ < 0 \text{ for mission failure} \end{cases} \qquad (2)$$

z unit of the system performance physical parameter e.g. flow rate, heat removal rate, pressure differential
r(z) functional requirement (required value of system parameter) function
s(z) system state ("operating" system parameter) function

If 'r' and 's' denote the random variables of the system output parameters, as defined above, the failure distribution curve can be constructed, according to the safety criterion expressed by eq. 2. The characteristic parameters for the probabilistic distribution are represented by the mean value and the statistical variance which represents the uncertainty associated with the mean value. Based on the uncertainties defined above and the mean value represented by the best estimate value of the characteristic parameter in nominal conditions and under the various failure modes (estimated from the results of the thermal hydraulic codes, like RELAP), the statistic distributions which would be suitable to describe the failure probabilities for each failure mode can be constructed.
In figure 1 the generic load and strength model is shown.

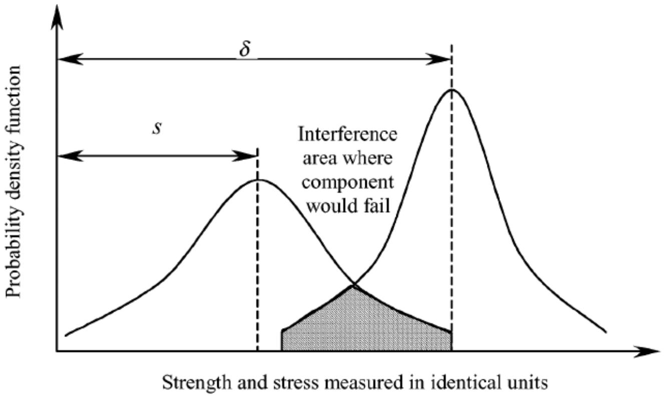

Fig. 1 Load (s) and strength (δ) interference diagram

The corresponding safety margin M is a random variable defined as M = g(z) and represents the reliability index of the system. The boundary between the sets of safe states and failed states in the z-space identifies the limit state for the safe operation (and equivalently identifies the reliability of the system) and the limit state is included for convenience in the failure set.
Therefore the probability of failure P_F is defined in terms of the LSF or alternatively of the reliability index M:

$$P_F = P\,(g(z) < 0) \quad \text{or} \quad P_F = P\,(M < 0) \qquad (3)$$

Accordingly the reliability of the system P_R will be:

$$P_R = P\,(g(z) > 0) \quad \text{or} \quad P_R = P\,(M > 0) \qquad \text{with } P_F = 1- P_R \qquad (4)$$

According with the analysis performed in ref [4], the application of the stress-strength model and the safety margin to the reliability of passive systems issue entails a subtle difference in the treatment of the main variables *R* (system Requirement) and *S* (system State).

In fact assuming e.g. *S* and *R* respectively as the effective mass flow rate and its critical value below which free convection is stopped, implies the reversal of the conditions discriminating the safe function from the mission failure defined by eq. 2, that is safe function condition is satisfied when *S* is greater than *R* and, on the contrary, mission failure occurs when *S* is less than *R*. Accordingly the new notation for g(z) tailored for the natural circulation gets the form ($g(z) = s(z)-r(z)$). The same consideration hold in case of consideration for other physical variables as performance outputs, like for instance the pressure differential driving force and the heat removal rate. This implies that, intuitively, one considers the failure of the system only in case of actual flow rate falling below the lower critical value, while, on the other side, failure may occur as well in case of actual flow rate above the critical upper value. In such a case the two kinds of probability of failure should be combined according to the reliability laws, as will be shown subsequently.

The application of the approach allows for calculation of reliability and probability of failure: unfortunately good data on the variability of the parameter indicator of the system performance are not available: in this case engineering judgment can be prudently used to obtain the distribution, [5].

It is easy to show that for normally distributed *R* and *S* the correspondent safety margin M is normally distributed as well and the expressions for reliability P_R and probability of failure P_F in terms of the reliability index are such that [7]:

$$P_R = \Phi(M) \tag{5}$$

and

$$P_F = 1 - P_R = 1 - \Phi(M) = \Phi(-M) \tag{6}$$

where $\Phi(M)$ is the normal cumulative distribution function in the standardized form.

In case of normally distributed variables the safety margin is suitable to be defined as well as the ratio of the difference between the mean values to the square root of the sum of the variances of the random variables s and r:

$$M = [E(s)-E(r)]/[Var(s)+Var(r)]^{1/2} \tag{7}$$

This expression for the safety margin or reliability index shows the relative difference between the mean values for the *S* and *R* variables: the larger the safety margin, the more reliable the system will be, as shown in figure 2, with reference to the same generic stress- strength interference model of figure 1.

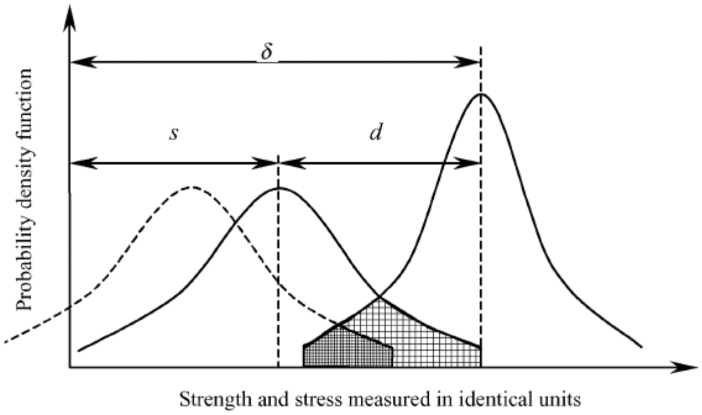

Fig. 2 Effects of safety margin on system reliability

Finally the single failure probability distributions related to the various failure modes should be considered, including eventually the two kinds of probability of failure for each failure mode, as previously pointed out, and combined in order to finally evaluate the overall system failure probability.

In fact, assuming the system fails if at least one failure mode occurs when the parameter is outside the allowable range, the probabilities of failure of the system are calculated from the probabilities of the failure modes, from eq. 6 and eq. 7. In the weakest-link model the system failure probability and reliability can be expressed respectively by the expressions, considering the single events independent and not mutually exclusive:

$$P_t = 1- \Pi_i\,(1-P_i),\ \text{where } P_i \text{ is the failure probability for each failure mode} \tag{8}$$

$$R_t = \Pi_i\, R_i,\ \text{where } R_i \text{ is the single reliability related to every failure mode} \tag{9}$$

Therefore for a T-H passive system with n mutually independent modes of failure, the total probability is computed as for a series system with n critical elements, so that the likelihood of each failure sums up to the system probability of failure. Based on the above considerations about the range of system performance, identified by a lower and an upper values respectively, each P_i , in turn, is made up of two contributors, which are combined in the fashion of two critical independent, but mutually exclusive, failures, that is summing them up.

With this respect a deeper analysis, applying the expression for the stress-strength interference model, yields the following relationships to be accounted to evaluate the system unavailability P_i , for each single failure mode:

$$P_i = P_{il} + P_{i\,u} = \int_0^{\infty} f(w_s)\, d\, w_s \left[\int_{w_r}^{\infty} f(w_r) d\, w_r\right] + \int_0^{\infty} f(w_r)\, d\, w_r \left[\int_{w_s}^{\infty} f(w_s) d\, w_s\right] \tag{10}$$

Where the indexes l and u stand for lower and upper thresholds, respectively.

It is important to note that a mutual statistical independence between the basic variables driving the system modes of failure is assumed in the present analysis for simplicity, without excluding the possibility of correlations among the variables, as noticed also in [8]. In fact the assumption of independence among the degradation measures means that the covariance among the critical parameter distributions is zero or is very low to be judged unimportant, so that the assessment of the failure probability is quite straightforward. If parameters have contributors to their uncertainty in common, the respective states of knowledge are dependent. As a consequence of this dependence, parameter values can not 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 subjective probability distribution function may be used. The dependence between the parameters can be also introduced by covariance matrices or by functional relations between the parameters. Conversely adoption, for instance, of joint pdfs (e.g. multivariate distributions) of the physical variables or conditional subjective probability distribution functions, in case of dependence among the degradation measures, would add a significant burden to the present study, in terms of degradation data analysis, functional relation analysis between the parameters or variance-covariance matrix development.

Finally, with reference to the limit state function and corresponding safety margin concept, one may, as well, conveniently define a failure function:

$$g = \min\,(g_1, g_2, \ldots, g_n) \tag{11}$$

where the indexes i are referred to the single modes of failure. It appears, however, that the construction of such a function presents relevant difficulties and thus, despite its worth for consideration, it is not developed in the present treatment.

MODEL APPLICATION

In this study the attention is directed towards a natural circulation loop including an Isolation Condenser which represents the heat sink and the Reactor Pressure Vessel where power production occurs. The system includes all the main features of the Isolation Condenser designed for the Simplified Boiling Water Reactor (SBWR), as reported in ref. [9].

First step of the analysis is the definition of the performance parameters, relative allowable limits and failure criteria. Assuming mass flow rate w at the reactor inlet as characteristic parameter of the system output, the deterministic failure criteria expressed by relations 12 and 13, identify the lower and upper limits for the physical variable; in accordance with the assumption consisting in neglecting the upper limit of the interval, failure criterion is chosen according to relationship 11, [4].

$$w_s / w_n \le 0.8 \quad \text{for the lower critical value} \tag{12}$$

$$w_s / w_n \ge 1.2 \quad \text{for the upper critical value} \tag{13}$$

Where w_n is the mission requested nominal value of the mass flow rate for natural circulation, estimated, for instance, from the output of a thermal hydraulic analysis, [2], and w_s is the actual value of the mass flow rate, referring to the state of the system. Note that the equality condition corresponds conservatively to the failure of the system.

Therefore the minimal flow rate value w_r required for natural circulation becomes from eq. 12,

$$w_r = w_n * 0.8 \tag{14}$$

The basic random variables to construct the model are w_s and w_r , characterized by distributions $f(w_s)$ and $f(w_r)$, respectively: the failure function becomes from eq. 2:

$$g(z) = f(w_s) - f(w_r) \qquad \begin{cases} > 0 \text{ for safe function} \\ = 0 \text{ at limit state} \\ < 0 \text{ for mission failure} \end{cases} \tag{15}$$

Note that the limit state function g(z) is representing, actually, the performance function for the system, with respect to the failure of the system.

In order to achieve the safety margin for the failure prediction, it is necessary to construct the pdf suitable to describe the characteristic parameter (in terms of mean value and variance): due to the lack of pertinent formulation, the information of $f(w_s)$ and $f(w_r)$ is rather subjective and therefore subjective/engineering judgment is used for both the variables.

Let both w_s and w_r be normally distributed with mean values and standard deviations μ_s, σ_s and μ_r, σ_r respectively. From equations. 3, 5 and 7 the probability of failure is given by:

$$P_F = P(M \leq 0) \tag{16}$$

Hypothesizing that a design of the system with a probability of failure less than 10^{-2} is sought, means that
$F= \Phi((0- \mu_M)/\sigma_M))) < 10^{-2}$, since M is normally distributed
which, inferring from the standard normal table gives us
$\mu_M/\sigma_M > 2.33$
And being $\mu_M = (\mu_s - \mu_r)$ and $\sigma_M = (\sigma^2_s + \sigma^2_r)^{1/2}$
$(\mu_s - \mu_r)/(\sigma^2_s + \sigma^2_r)^{1/2} > 2.33$ and

$$\mu_s > \mu_r + 2.33 \, (\sigma^2_s + \sigma^2_r)^{1/2} \tag{17}$$

This expression gives us a lower limit on the (mean) value of the flow rate as a function of the minimal required value and the variances, in order to achieve a probability of failure less than 10^{-2}. If, for instance $\mu_n = 20$ Kg/sec and $\mu_r = 16$ Kg/sec from eq. 14, and if $\sigma_r = 2\ \sigma_s = 2$, from eq. 17 $\mu_s > 22.6$ Kg/sec.

The table below summarizes the lower limits for different target probabilities of failure (or equivalently target reliability indexes): results clearly show that the lower flow rate boundary increases as the sought probability of failure decreases, as expected. They help designers address the natural circulation system conception if a reliability based approach is adopted, during the design phase of the system.

For instance one of the major points of tests and analysis to be performed in order to assess the heat removal by natural circulation and to reduce the related uncertainties should be focused on the heat transfer coefficient of the heat exchangers (e.g. isolation condenser, which are foreseen to be submerged in a cooling pool): attention should be paid to the two main phenomena driving the component performance. That is the condensation behavior inside the heat exchanger tubes - including the presence of non-condensable gases - and heat transfer form these tubes to the water pool, which impact the design of the tube bundle of the heat exchanger, in the form of provisions to reduce the thermal resistance of the wall and increase the heat coefficient transfer through the reduction of the tube wall thickness and the use of material with higher thermal conductivity.

It has to be noted that, as regards the upper threshold value, the PF becomes $g(z) = f(w_r) - f(w_s)$, and the procedure is equivalent to the previous one, but with the reversal of the conditions for system safety, implying the actual flow rate above the upper limit. For a target probability of failure of 10^{-1} relationship 17 becomes $\mu_s < \mu_r - 1.28\ (\sigma^2_s + \sigma^2_r)^{1/2}$.
For instance if $\mu_n = 20$ Kg/sec and $\mu_r = 24$ Kg/sec from eq. 14, and if $\sigma_r = 2\ \sigma_s = 2$, the maximum allowable value for the mean value of the mass flow rate μ_s is 20.38, to achieve a system unavailability figure around 10%.

Table 1 Lower flow rate limits for different probabilities of failure

Probability of failure	μ_s	μ_s (Kg/sec)
10^{-1}	$\mu_s > \mu_r + 1.28\ (\sigma^2_s + \sigma^2_r)^{1/2}$	19.6
10^{-2}	$\mu_s > \mu_r + 2.33\ (\sigma^2_s + \sigma^2_r)^{1/2}$	22.6
10^{-3}	$\mu_s > \mu_r + 3.1\ (\sigma^2_s + \sigma^2_r)^{1/2}$	24.7
10^{-4}	$\mu_s > \mu_r + 3.72\ (\sigma^2_s + \sigma^2_r)^{1/2}$	26.5

SYSTEM DESIGN

This is, of course, a rather crude model of the system and the calculated reliability is undoubtedly subject to considerable errors. For example flow rate varies with time, but it would make sense to consider the time variations as deterministic, in the sense that the probability of falling or exceeding any particular value of the characteristic parameter should be referred to that particular time. In any case, this means that the parameter distribution is dependent on the variable time t. In fact, as regards the ageing effects for instance, changes on surface roughness have a n impact on the friction factor and hence on the natural circulation. In addition, safety systems are normally required on-demand, which means that natural circulation has to be built up any time is required and variations over this transients are relevant to reliability assessments. Furthermore the values reported in the table are assessed with reference to a “generic” state of the system independently of the fact that it can result from the occurrence of a particular failure mode or from an event enveloping the combination of various modes of failure, hampering the natural circulation stability. Thus the sought probability of failure values appearing in the first column, may refer indifferently to different circumstances. To be accurate the procedure illustrated in section 3 should be followed, the single failure probability combined to achieve the whole system reliability according to eq. 8 and the permissible parameter interval established through eq. 16.

Accurate modeling of the process variables would require empirical data, presently not available, and in general the parameter distribution function modeled as normally distributed adds a parameter uncertainty to be taken into account, and attention should be paid to other kinds of distributions, as for instance the lognormal: in this regard, no finalized study has been carried out to propose the relevant probability distributions.

However the present assumption complies with the criterion chosen for the selection of the distributions in ref. [4]. In that work, in order to duly characterize the representative parameter on the probabilistic standpoint (i.e. ranges and distributions), as a general rule, a central pivot has been identified, and then the range has been extended to higher and lower values. The pivot value represents the nominal condition for the parameter, and the limits have been chosen in order to exclude unrealistic values or those representing a limit zone for the operation demand of the passive system. Probability values are peaked to the nominal value and decrease gradually towards the minimum and maximum allowed values: thus the lower the probability values, the wider the “distance” from the nominal value. In addition to the discrete probability distribution, on one hand a uniform probability would be suitable to describe the parameter if one considers the design range of the parameter (that is the pdf would be uniform); on the other hand the values of the flow rate could correspond to the end status of a system transient or accident or to the case of the situation simply deriving from the malfunction of the system, as a result of a probabilistic analysis.

SUMMARY AND CONCLUSIONS

Probabilistic design is a methodology aimed at producing robust and reliable products. A common mistake made by design engineers is not considering variations of the factors that affect the reliability or performance of their product and instead using only the nominal or mean values of these factors. By understanding the probability distributions of the design parameters, the design engineer can design for a specific reliability or quality level by producing designs that are robust to variations.

Safety against failure is the overriding objective of this study, where safety is a probabilistic concept and system mal performances are classified into modes of failure. With respect to such modes, it is assumed that the system is in either a failed or a safe state. The state is dependent on uncertain quantities, i.e., thermal-hydraulic parameters mostly, which affect the output parameter of the system performance. Sometimes process modeling with uncertainties is necessary, with reference, for instance, to the thermal-hydraulic correlations governing the system process. The system state is quantified in terms of a failure function, which is a function of the basic random variables. The system passes form safe state to failed state in each failure mode through the limit states. In limit state design the nominal values of the random variables involved are representative of failure conditions.

In this study reliability analysis is of interest mainly as a tool in the design process. For each failure mode a desirable or acceptable value of the reliability must be available to the designer: this reliability target may be chosen by judgment or rational analysis, and the relative approach is presented. In addition to technical aspects, the economic loss component is important and the expected loss should figure in the reliability target. The probabilistic design approach for the T-H passive systems has been followed, by considering the distribution model of a characteristic parameter resulting from the distributions of the relevant factors (i.e., design and critical parameters) and estimating deviations from the goal or specifications, and finally an analytical solution is obtained.

In this paper the transfer of the structural methodology assessment methodology (i.e. for passive A systems) is considered for its applicability for the thermal hydraulic passive systems, relying on natural convection.

The $R-S$ (Resistance – Stress) model elicited from the structural reliability analysis is tailored to the specific case of the type B passive systems, through the definition of a proper system reliability index which is based on the safety margin concept, with reference to the relevant process output variables (in the specific case the mass flow rate is considered). The objective is the development of a model aiming at assessing the probability of the flow being less than required for natural circulation, to provide insights for a reliability based design of the system.

The methodology is applied to the Isolation Condenser of the SBWR. The results of the analysis, in terms of minimal output parameter requirement as a function of the desired reliability, help designer determine the allowable limits for the system performance parameters, within a probabilistic framework.

The study is conditional on the assumptions adopted to model the system for such an analysis. In summary model assumptions and simplifications are:

- the performance function is defined in the form of the flow instability;

- in accordance with the fact that fairly all failure modes are likely to happen when the flow is being less than required, the upper value of the characteristic parameter is nearly overlooked; nonetheless the proposed failure model implies both lower and upper values;

- normal distribution has been selected to construct the parameter distributions, for its “good manageability”, from the analytical point of view. The appropriateness of the distribution should be verified and considered for each failure mode; consideration of lognormal distribution for the characterization of the variables appear to be a reasonable choice, but the analytical treatment would be more complex;

- the evolution of the physical parameter with time is not considered;

- according to the main idea of the study to propose the approach, results are presented for illustrative purposes and conclusions are made on the basis of generic numerical values assigned to an oversimplified model, albeit related to the Isolation Condenser configuration designed for SBWR.

- safety factors in terms of design limiting values are assessed for a range of target reliability values: the purpose is to provide consistency with a reliability-based approach, in a risk informed framework.

Despite the preliminary character, the research tracks a viable path to natural circulation passive systems reliability evaluation that complements the methodology suggested in [4]: the objective is to provide useful input to similar but more comprehensive studies. Further development and endorsement are needed, in order to settle all the open points, which are highlighted above.

References

1. IAEA-TECDOC-626, *Safety Related Terms for Advanced Nuclear Power Plants*, 1991.
2. Burgazzi, L., “State of the art in reliability of thermal-hydraulic passive systems”, *Reliability Engineering and System Safety* , Vol.92, 2007, pp. 671-675.
3. Apostolakis, G.E., Hejzlar, P. and Pagani, L., ”The impact of uncertainties on the performance of passive systems”, *Nuclear Technology*, Vol. 149, 2005, pp. 129-140.
4. Burgazzi, L., “Reliability evaluation of passive systems through functional reliability assessment”, *Nuclear Technology*, Vol.144, 2003, pp. 145-151.
5. Burgazzi, L., “Evaluation of uncertainties related to passive systems performance”, *Nuclear Engineering and Design*, Vol. 230/1-3, 2004, pp. 93-106.
6. Santosh., “Reliability analysis of pipelines carrying H_2S for risk based inspection of heavy water plants”, *Reliability Engineering and System Safety*, Vol. 91, 2006, pp.163-170.
7. Ebeling, C.E., *An Introduction to to Reliability and Maintainability Engineering*, Mac Graw-Hill Companies, Inc., 1997.
8. Burgazzi, L., “Addressing the uncertainties related to passive system reliability”, *Progress in Nuclear Energy*, Vol. 49, 2007, pp. 93-102.
9. Burgazzi L., “Passive System Reliability Analysis: a Study on the Isolation Condenser, *Nuclear Technology*, Vol. 139, 2002, pp. 3-9.