ENEA Ricerca Sistema Elettrico	Sigla di identificazione	Distrib.	Pag.	di
	ADPFISS-LP1-071	L	1	27

Titolo

Comparative assessment of passive and active systems for the development of advanced reactors

Descrittori

Tipologia del documento: **Rapporto tecnico**

Collocazione contrattuale: Accordo di programma ENEA-MSE: Piano Annuale di Realizzazione 2015, Linea Progettuale 1, Obiettivo B: Safety Assessment e Valutazioni d'Impatto, Task B2-2

Argomenti trattati: Sicurezza nucleare
Analisi incidentale
Analisi di sicurezza probabilistica

Sommario

This report presents the activities performed in the frame of LP1, Objective B (Safety assessment and accident consequences evaluation), task B2-2 of PAR 2015, ADP ENEA-MSE.
The study touches on the comparative assessment between active and passive systems for the development and design of new advanced reactors.
The study is aimed at developing the methodical approach for the comparative assessment at the system level in terms of performance and reliability aspects.

Note:

This document has been prepared with the following main contributors:

- L. Burgazzi (ENEA)

REV.	DESCRIZIONE	DATA		REDAZIONE	CONVALIDA	APPROVAZIONE
2			NOME			
			FIRMA			
1			NOME			
			FIRMA			
0	EMISSIONE	6/09/16	NOME	L. Burgazzi	F. De Rosa	F. De Rosa
			FIRMA			

Table of contents

Executive Summary

The introduction of passive systems is regarded as one of the most important factors for safety increase of GenIII and GENIV reactors, as well as for the development of small reactor size or the SMR (Small Modular Reactors).

However, more detailed studies reveal how such an advantage deriving from the use of passive safety systems than the active ones is not so obvious: thus the assessment of the benefits and the challenges that the adoption of the two types of systems in the various reactors pose. The study is aimed at developing the methodical approach for the comparative assessment at the system level in terms of performance and reliability regardless in any case by economic factors.

1. Introduction

The utilisation of passive systems in a reasonable combination with or instead of traditional active systems is being considered as the important measure to enhance the safety in many concepts of the next generation plants. The right balance of active and passive systems can be found only for each advanced concept separately, but the basic criteria for decision-making are the same for the most of the concepts. These criteria are mainly based on the weighing of passive and active system's advantages and disadvantages with regard to the designated functions, overall plant safety and cost. There are some aspects in this area which are very plant specific, e.g. the validation of passive systems for plant conditions, integration of passive features in the overall safety systems, in-service inspection of passive components, etc. These problems have to be addressed by each plant designer to propose the optimal combination of active and passive systems and components. Nevertheless, it is generally acknowledged that passive systems/components, due to their inherent features have the potential for some advantages over the active ones, which however are not so manifest as evidenced in two companion reports, refs. 1 and 2. The analysis in refs. 1 and 2 lead to the conclusions that despite they are credited a higher reliability with respect to the “conventional” ones - because of the smaller unavailability due to hardware failure - or even they are claimed to be immune from faults, they pose however some challenges as regards the availability/ reliability issues and more in general their performance assessment, because there is always a nonzero likelihood of the occurrence of physical phenomena leading to pertinent failure modes.

This concern required further evaluation of the issue, aiming mostly at developing a methodology of establishing guidelines and criteria for the comparison of active and passive systems.

Initially main conclusions of the previous work and a literature are briefly recalled together with a literature review.

2. Background

A few efforts over these years have been undertaken to deal with the issue, as summarized in the following.

In ref.3 a probabilistic comparison has been performed between active and passive design as regards the candidate heat removal systems for hot shutdown and cool down of a NPP proposed by a design study for advanced NPP, taken as examples representing passive systems of category D

(that is requiring the opening of a valve, according to IAEA categorization of passive systems), and active systems.

The investigation showed that both with the active and the passive design high safety levels can be achieved. However, the investigation also showed that the achievable safety level of the passive design is limited by its actuation, which requires a mechanical component operation for the start-up. Thus although the passive design needs no further 'activity' after 'start-up' and therefore is extremely reliable after start-up (this is in contrast to the active design where active components are required over the whole mission time) its overall reliability cannot be overwhelmingly better than that of the active system due to the start-up phase.

Ref.4 presents some case studies relative to the PSA of NPPs provided with both active and passive systems and shows that, despite the limitations, PSA in the design of active/passive safety reactors is very useful.

The analysis of plant safety in terms of CDF figures in ref.5 shows that the design with passive safety features appear to have somewhat lower CDF than those with active systems, while both types of new plants generally have lower risk than operating ones.

Ref.6 proposes a comprehensive comparison of reliability and cost taking into account uncertainties and introduces the concept of flexibility using the example of active and passive residual heat removal systems in a PWR. The results show that the active system can have, for this particular application, greater reliability than the passive system. In addition, considering the implications of flexibility upon remedial costs, the active system may more economical than the passive system.

With respect to previous work performed by the author, main conclusion of ref.2 is that passive system reliability is not necessarily better or worse than the active ones: reliability will depend on the overall design and operation of the system, regardless of whether the system is active or passive. A good overall plant design may include active systems, passive systems or combination of both types of systems to meet performance and safety objectives.

In particular in ref.1 it is roughly stated that:

- for Passive Safety Systems Reactors that:
    - their claimed higher reliability and availability are challenged by some important functional aspects, impairing their performance;
- for Active Safety System Reactors that:
    - the higher level of redundancy causes an higher level of complexity of the plant, that is a risk factor itself,

- using safety systems of the same type makes the plant vulnerable to common cause of failures.

A comparative analysis related to loop configurations of active and passive design shows that their safety function achievement, as the decay heat removal, is comparable to or even less than the active systems' one, since the functional reliability for passive systems is such that it constitutes a challenge for the accomplishment of the safety function.

3. Motivation and objectives

Here some of the benefits and disadvantages of the passive systems that should be evaluated vs. the "equivalent" active system are briefly recalled (ref.7).

- Advantages

  - No external power supply: no loss of power accident has to be considered.
  - The passive nature of the safety systems reduces the reliance on operator action, which could imply no inclusion of the operator error in the analysis. In fact the minimization of the intrinsic complexity of the system results in improved human reliability. The natural circulation core heat removal without, e.g., the incorporation of mechanical pumps results in reduction of operating and maintenance staff requirements, generation of low-level waste, dose rates, and improvement of operational reliability and plant safety and security.
  - Passive systems must be designed with consideration for ease of ISI (In Service Inspections), testing and maintenance so that the dose to the worker is much less.
  - The freedom from external sources of power, instrumentation and control reduces the risk of dependent failures such as the common cause failures
  - Better impact on public 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 high level of uncertainty, and therefore need for t-h uncertainties modelling.

- Licensing requirement (open issue), since the reliability has to be incorporated within the licensing process of the reactor. For instance the PRA's should be reviewed to determine the level of uncertainty included in the models and their potential impact. In fact some accident sequences, with frequencies high enough to impact risk but not predicted to lead to core damage by a best estimate t-h analysis, may actually lead to a core damage when t-h uncertainties are considered in the PRA model.
- They are required to accomplish their mission with a large functional margin in order to address the large amount of uncertainties that may dominate their reliability
- Need for operational tests, so that dependence upon human factor can not be completely neglected
- Time response: the promptness of the system intervention is relevant to the safety function accomplishment. It appears that the inception of the passive system operation, as the natural circulation, is conditional upon the actuation of some active components (as the return valve opening) and the onset of the conditions/mechanisms for natural circulation start-up
- Notwithstanding the fact that passive safety systems are claimed to have higher reliability compared with active safety systems, reliability and performance assessment in any case and their incorporation in the reactor concepts needs to be tested adequately, due to several technical issues as formerly pointed out. Quantification of their functional reliability from normal power operation to transients including accidental conditions needs to be evaluated. Functional failure can happen if the boundary conditions deviate from the specified value on which the performance of the system depends.
- Ageing of passive systems must be considered for longer plant life; for example corrosion and deposits on heat exchanger surfaces could impair their function.
- Economics of advanced reactors with passive systems, although claimed to be cheaper, must be estimated especially for construction and decommissioning.

The question whether it is favourable to adopt passive systems in the design of a new reactor to accomplish safety functions is still to be debated and a common consensus has not yet been reached, about the quantification of safety and cost benefits which would make nuclear power more competitive, from potential annual maintenance cost reductions to safety system response, as put in evidence in ref. 7.

A systemic approach for the comparison of active and passive design is necessary in order to explore the implication of these two arguments: the first argument is related to reliability issues with passive system performance (ref.6), the second argument is related to potential capital cost issues of passive systems. In this respect a potential detrimental effect incurred by inconsistent safety performance of passive designs may require an additional remedial capital cost after the power plant has been built.

While neglecting the second argument, main goal of this study is the development of a methodology allowing to measure and compare the reliability of active and passive systems considering, for the most, the influence of the selected approach and effects of uncertainty in leading to functional failures, providing as well the underlying rationale and points.

4. Methodology for comparative assessment passive vs active

In order to compare the two designs at the system reliability level, a comprehensive evaluation method is required, which includes various aspects.

From the analysis reported in ref.7 and the former list related to pros and cons, main factors acting as drivers for the development of the approach aiming at the comparative assessment of the reliability of passive vs active systems are the following,:

- Reliability method
- Functional failure
- Uncertainties
- Licensing
- Time response
- Mission time
- External events
- Human factor
- Integration within an accident sequence
- Aging
- Redundancy, independence and CCF

These factors are briefly examined in terms of the relative influence on the reliability assessment comparison practice.

4.1. Reliability method

While the “classical” fault tree analysis is well suited to evaluate the reliability of active systems, passive system assessment requires the adoption of more complex approaches, such as the RMPS (Reliability Methods for Passive Systems) which was developed in the frame of the matching European Union funded project (ref.8). 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.

It proposes some essential steps in order to evaluate the functional failure of passive systems. First, a system is modeled using developed computer best-estimated codes which embody basic thermal hydraulic principles of natural circulation. On the other hand, in order to obtain steady state simulations, simplified developed codes could be suitable as well in order to avoid the complexity of proven codes and to reduce the simulation time and endeavours. The second step in the procedure is the selection of critical parameters. These critical parameters have been determined by qualitative analysis, expert opinions, literature reviews, or through sensitivity analysis of the system. On the third step, the uncertainties of these parameters are assigned using probabilistic distributions, which represent the aleatory or epistemic uncertainty of parameter and model. Finally, the propagation of input uncertainty is performed in numerical simulations using simply developed codes.

Distinguishing attribute of this methodology is that it merges the probabilistic and t-h aspects of the problem: the t-h code is adopted for uncertainty propagation, the uncertainties in parameters are modelled by probabilistic density functions and expert judgement is adopted to a large extent, although statistical analysis should be exerted when experimental data exist.

4.2. Functional failure

Passive systems exhibit unique failure mechanisms, termed functional failures (ref.9). In essence, a functional failure is the failure of the passive system to complete its desired role due to a deviation from expected conditions, rather than the failure of a physical component. Functional failures are a real possibility in passive systems that rely on natural circulation, and modeling the system using classical fault and event trees is difficult.

It may help to describe functional failures using an example:

Consider a decay heat removal system operating under natural circulation whose objective is to maintain adequate core cooling to prevent the cladding temperature from exceeding some specified failure limit. In this case, it is helpful to think of the cladding temperature as a load acting on the system, with the failure limit representing the system's capacity to withstand that load.

Hence, failure will occur when the load exceeds the capacity. This is the load-capacity failure model, also known as the resistance-stress (R-S) failure model, familiar to structural reliability.

For our example, the flow rate, and hence the maximum cladding temperature, may depend strongly on pressure losses in the natural circulation loop; as a result, minor alterations in the total pressure drop, due to corrosion or fouling, for instance, may sufficiently decrease coolant flow to an unacceptable level, resulting in cladding temperature exceeding the failure limit.

In this example, no physical component has failed, but the passive system was unable to complete its desired function. When the total pressure drop was altered due the geometry changes caused by corrosion and fouling, the natural circulation flow rate was negatively affected, resulting in a higher peak cladding temperature, and a higher load on the system. With the load now exceeding the capacity, the system fails.

The functional failure concept is a consequence of the small driving forces that are characteristic of passive systems. Unlike active systems, which usually involve large driving forces, such as powerful motors, passive systems relying on natural circulation have only buoyancy forces powering the system. These forces are roughly of the same magnitude as those countering against the flow, such as friction. While these counter forces are present in active systems, the power of pumping motors is so much greater than these losses that they can essentially be ignored.

4.3.Uncertainties

While the uncertainties related to PSA are appropriate with regard to the active systems reliability process, the aspects relative to the assessment of the uncertainties related to passive system performance regard both the best estimate t-h codes eventually used for their evaluation and system reliability assessment itself, but with many differences.

Indeed the quantity of uncertainties affecting the operation of the t-h passive systems affects considerably the relative process devoted to reliability evaluation, within a probabilistic safety analysis framework.

These uncertainties stem mainly from the deviations of the natural forces or physical principles, upon which they rely (e.g., gravity and density difference), from the expected conditions due to the

inception of t-h factors impairing the system performance or to changes of the initial and boundary conditions, so that the passive system may fail to meet the required function. Indeed a lot of uncertainties arise, when addressing these phenomena, most of them being almost unknown due mainly to the scarcity of operational and experimental data and, consequently, difficulties arise in performing meaningful reliability analysis and deriving credible reliability figures. This is usually designated as phenomenological uncertainty, which becomes particularly relevant when innovative or untested technologies are applied, eventually contributing significantly to the overall uncertainty related to the reliability assessment.

Actually there are two facets to this uncertainty, i.e., “aleatory” and “epistemic” that, because of their natures, must be treated differently. The aleatory uncertainty is that addressed when the phenomena or events being modeled are characterized as occurring in a “random” or “stochastic” manner and probabilistic models are adopted to describe their occurrences. The epistemic uncertainty is that associated with the analyst’s confidence in the prediction of the PSA model itself, and it reflects the analyst’s assessment of how well the PSA model represents the actual system to be modeled. This has also been referred to as state-of-knowledge uncertainty, which is suitable to reduction as opposed to the aleatory which is, by its nature, irreducible. The uncertainties concerned with the reliability of passive system are both stochastic, because of the randomness of phenomena occurrence, and of epistemic nature, i.e. related to the state of knowledge about the phenomena, because of the lack of significant operational and experimental data.

It has to be pointed 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 and impinge on the final sought reliability figure.

As is of common use when the availability of data is limited, subjective probability distributions are elicited from expert/engineering judgment procedure, to characterize the critical parameters.

Three following classes of uncertainties to be addressed are identified:

- Geometrical properties: this category of uncertainty is generally concerned with the variations between the as-built system layout and the design utilized in the analysis: this is very relevant for the piping layout (e.g. suction pipe inclination at the inlet of the heat exchanger, in the isolation condenser reference configuration) and heat loss modes of failure.

- Material properties: material properties are very important in estimating the failure modes concerning for instance the undetected leakages and the heat loss.

- Design parameters, corresponding to the initial/boundary conditions (for instance, the actual values taken by design parameters, like the pressure in the reactor pressure vessel).

- Phenomenological analysis: the natural circulation failure assessment is very sensitive to uncertainties in parameters and models used in the thermal hydraulic analysis of the system.

The first, second and third groups are part of the category of aleatory uncertainties because they represent the stochastic variability of the analysis inputs and they are not reducible.
The fourth category is referred to the epistemic uncertainties, due to the lack of knowledge about the observed phenomenon and thus suitable for reduction by gathering a relevant amount of information and data. This class of uncertainties must be subjectively evaluated, since no complete investigation of these uncertainties is available.
As highlighted above, clearly the epistemic uncertainties address mostly the phenomena underlying the passive operation and the parameters and models used in the t-h 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. With this respect, it is important to underline, again, that the lack of relevant reliability and operational data imposes the reliance on the underlying expert judgment for an adequate treatment of the uncertainties, thus making the results conditional upon the expert judgment elicitation process. This can range from the simple engineering/subjective assessment to a well structured procedure based on expert judgment elicitation.
Conversely probability models to be applied to active systems provide estimates for the frequencies of initiating events, the failure probabilities of technical components to start on demand, the failure rates of technical components to run, the unavailability of system functions, the human error probabilities, the probabilities for common cause failures, etc. (ref.10)
Two general sources contribute to the epistemic uncertainty on the predictions of the above-mentioned models. These are the so-called parameter or data uncertainty and the so-called model uncertainty.

Parameter or data uncertainty exists, if the true values cannot be definitely determined and, therefore, must be estimated. For instance, parameters or input data derived from measurements may be uncertain due to measurement errors. Model parameters resulting from the fitting of model predictions to experimental data are uncertain, if the underlying experimental data is subject to variation. Usually the probabilities of basic events of component failures are modelled by means of the lognormal distribution.

Model uncertainty exists, if there is uncertainty on how well the model applied describes the true relationship: for instance model assumptions on the true relationship can be inadequate, incomplete or even invalid with the consequence that uncertainty exists on how well the model prediction represents the true value.

4.4. Licensing

The evaluation and characterization of safety margins into risk-informed approaches adopts a basic framework which is represented conceptually by the relationship

$P(C>L)$

which depicts the evaluation of a parameter (in this case a load L) versus an acceptance guideline (or capacity C), through the probability P that the capacity exceeds the load. Although in practice, this assessment has generally been simplified to the comparison of point estimate values, in reality these parameters are better represented as distributions that account for the uncertainties associated with prediction of both the load and capacity. Figure 1 illustrates the relationship between a calculated load (for example, temperature, pressure, etc.) distribution and the capacity distribution for a structure, system or component (SSC). In this paradigm the concept of “margin” is transformed from a simple “distance” between the point estimates of the load and capacity to that of a probability that the load experienced will exceed the installed capacity to handle it, that is overlapping of the resulting load and capacity distributions.

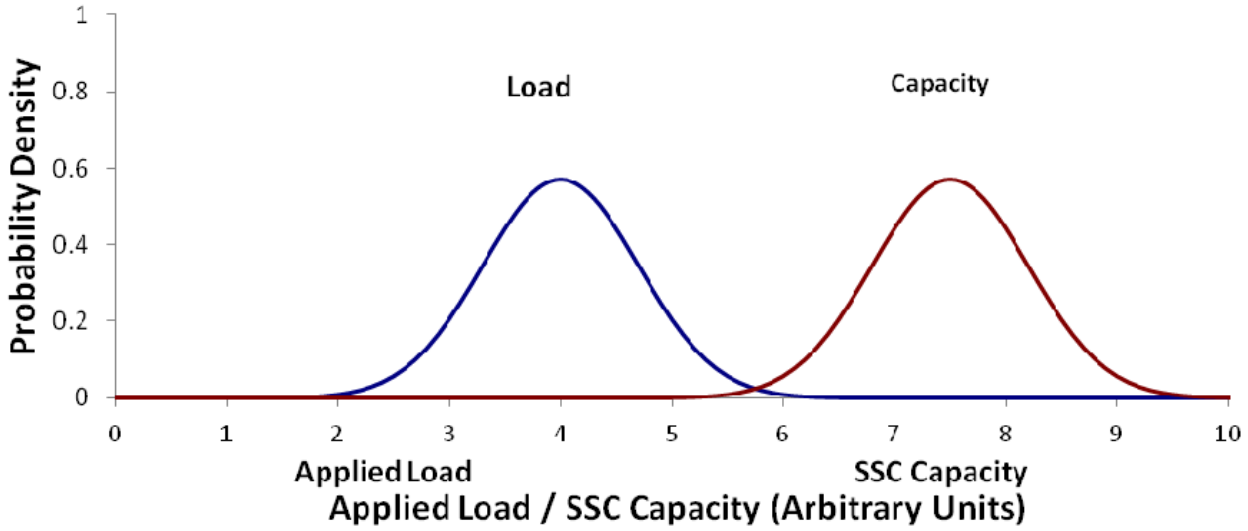

Figure 1 Load Capacity interference model

This concept well applies to the case of passive systems, as regards, for instance to the approach based on the concept of functional failure, within the reliability physics framework of load-capacity exceedance (ref.9). The functional reliability concept is 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, leading the load imposed on the system to overcome its capacity. In this framework, probability distributions are assigned to both safety functional requirement on a safety physical parameter (for example, a minimum threshold value of water mass flow required to be circulating through the system for its successful performance) and system state (i.e., the actual value of water mass flow circulating), to reflect the uncertainties in both the safety thresholds for failure and the actual conditions of the system state. Thus the mission of the passive system defines which parameter values are considered a failure by comparing the corresponding probability distributions according to defined safety criteria.

Clearly safety margin in case of passive system is to be considered much lesser as compared to active ones, since it has to accommodate the large amount of uncertainties, as previously pointed out.

In fact safety margin is defined as $M=[E(C)-E(L)]/[Var(C)+Var(L)]^{1/2}$ where E and Var are respectively the mean value and the variance associated with the distributions. This expression for the safety margin or reliability index shows the relative difference between the mean values for the C and L variables: the larger the safety margin, the more reliable the system will be, as shown in Figure 2, with reference to the same generic load-capacity interference model of Figure 1, (ref.11).

Large uncertainties and consequent high variances related to passive systems make small values of the safety margin, posing therefore more stringent requirement on licensing requisites.

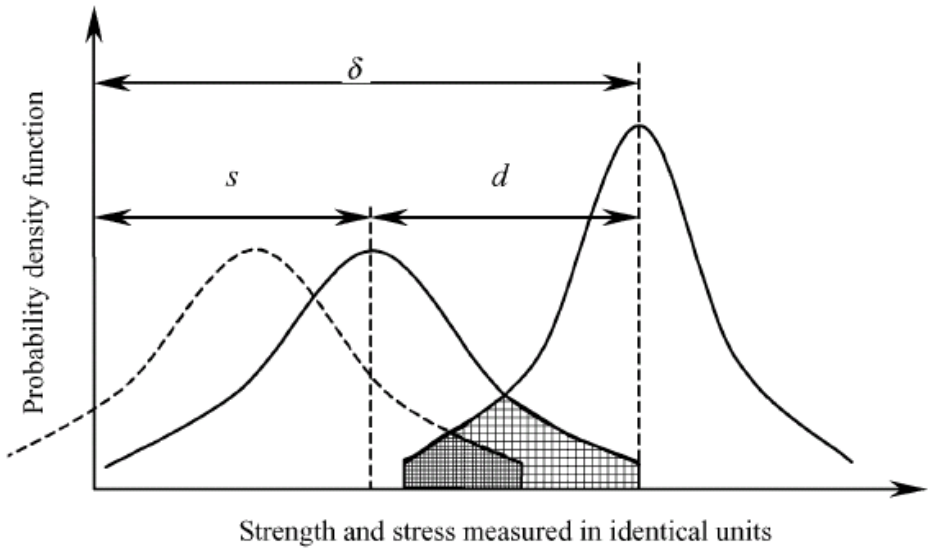

Figure 2 Effects of safety margin on system reliability

4.5. Time response

The readiness of the system intervention is relevant to the safety function achievement.

Activation of both active and passive systems is conditional upon a mechanical component operation (e.g., opening of a valve) and, while in case of active loop, pump to run is required, the initial conditions/mechanisms for natural circulation start-up is the prerequisite. It appears that the system initiation is more critical for passive systems.

This is well illustrated by the fault tree in Figure 3 below, with regard to active(including valve and pump)/passive loop configuration.

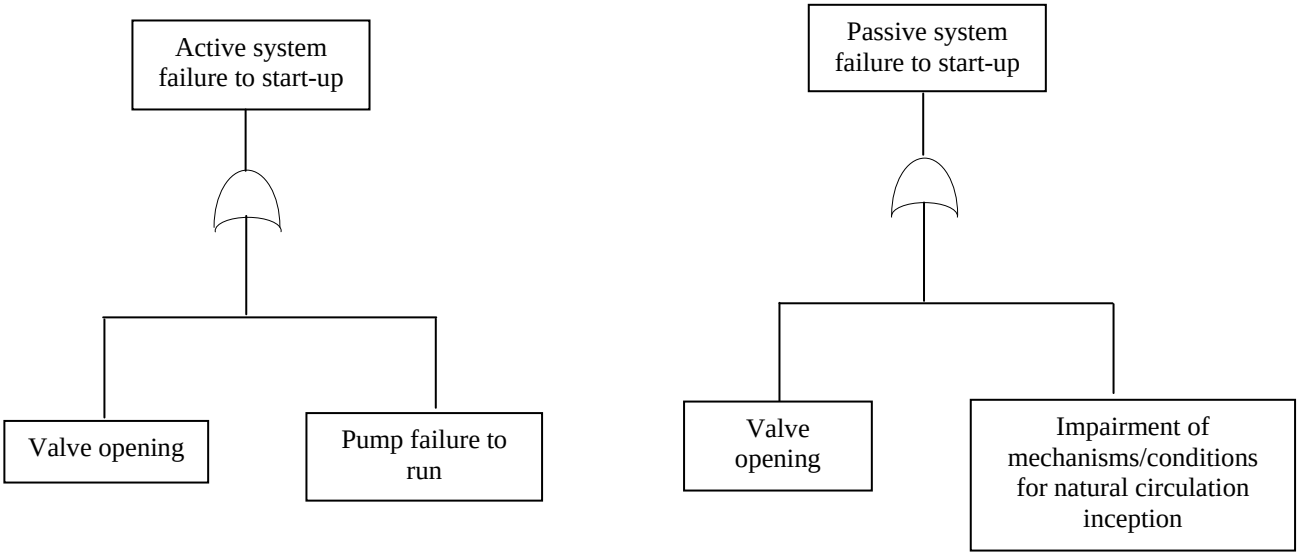

Figure 3 Fault tree model for active/passive system start-up

4.6. Mission time

Fukushima event underlined the necessity to reconsider mission time span for its extension in PSA studies: in fact the “usual” mission time of 24 hours has been proved to be unrealistic so that the required mission time should be not only longer than 24 hours as usual Level 1 PSA mission time, but be extended beyond the 72 hours corresponding to the grace period (ref.12).

This implies a realistic consideration of the event under investigation, in terms of accident progress and safety systems timing intervention, to figure the relative degree of mission time increase, to be considered for the extended scenario (e.g., including long-term station blackout and loss of ultimate heat sink assessment) assessment. The main issues that need attention in mission times re-definition, concern, in particular, prolonged accidental situations, implying, for instance, the protracted losses of AC power and residual heat removal.

Fukushima accident progress over time justifies the consideration for the duration of mission times for safety systems and components longer than 24 hours in a realistic way and, more generally for prolonged mission times to a very large extent (up to one month for instance), as it has been demonstrated that 24 hours recovery concept as for internal initiating events is not good for some external events.

4.6.External events

One of the important considerations in the treatment of external events is the possibility of disruption of external sources of electricity, cooling water, other essential supplies and possibly prompt operator action following an extreme external event. In such a situation, some innovative reactor designs take advantage of passive safety features provided within the protected reactor building or inner containment, disregarding the availability of external sources of supply of electricity, cooling water, etc.

In this context, several passive systems enable prolonged grace period to the operator during which the reactor is maintained in a safe state without any operator intervention. This, in essence, implies availability of a large heat sink within the reactor building, and its highly reliable uninterruptible thermal communication with the reactor core to facilitate continued removal of core heat for prolonged durations without any involvement of active systems or operator interventions (e.g. natural convection, radiation, and conduction cooling). This feature too, is highly relevant for some extreme external events when, on account of possible devastation outside the protected reactor building, it is quite likely that all the external sources of cooling water, electricity, and instrumentation air and ventilation system become non-available. In such scenarios, it is also conceivable that the operators may not be in a position to act in an efficient or effective manner.

This is quite relevant as far as specific situations are concerned (for example, a specific combination of initiating events), implying, for instance, wired system incorporating sensors or actuators or a control system relevant to safety are assumed to be disabled in a manner that the desired safety function could not be performed in the absence of required signals or power supplies. Of particular relevance are the thermal hydraulic passive systems implementing natural circulation to accomplish the decay heat removal function.

4.7. Human factor

While passive system operation is characterised by no or very limited reliance on external input including the human action, implying no inclusion of operator error in the analysis, the Technique for Human Error Rate Prediction (THERP) (ref. 13) method is used to evaluate human error probabilities in case of active system reliability analysis, where, conversely, human failure plays a relevant role as a risk factor in plant core damage frequency.

However, in case of passive systems, if operational tests are required, the dependence upon human factor can not be completely neglected.

4.8. Integration in accident sequence

Classically in Probabilistic Risk Assessment (PRA) studies accident scenarios are modelled through the Event Tree (ET) technique, which allows identifying all the different chains of accident sequences deriving from the initiating events. ET development implies each sequence represents a certain combination of events, corresponding to failed or operating safety or front-line systems: thus ETs, starting from the initiators, branch down following success or failure of the mitigating features, which match the ET headings, providing therefore a set of alternative consequences. Systems analysis adopting the Fault Tree (FT) method is the simplest way to assess the unreliability of passive system as a safety feature, required to operate for stopping the sequence or mitigating the consequences. The construction of a system fault tree is based on system success/failure criteria and relies upon the system modeling: system model requires the identification of the relative boundaries and interfaces and includes components required for system operation, support systems required for actuation and operation of the system components, and other components that could degrade or fail the system. In addition the system model includes the relevant and possible failure modes for each component required for system operation. These should include component failures (as, for instance, stand-by failure, failure on demand and operational failure) and dependent failures (intersystem dependencies and intercomponent dependencies or common cause failures).

The introduction of passive safety systems into an accident scenario, in the fashion of a safety or front line system, deserves particular attention. The reason is that its reliability figure depends more on the phenomenological nature of occurrence of the failure modes rather than on the classical component mechanical and electrical faults. This makes the relative assessment process different as regards the system model commonly adopted in the fault tree approach as depicted before.

In PSA, the status of individual systems such as a passive system is assessed by an accident sequence analysis to identify the integrated behavior of a nuclear system and to assign its integrated system status, i.e. the end states of accident sequences. Because of the features specific of a passive system, it is difficult to define the status of a passive system in the accident sequence analysis. In other words, the status of a passive system does not become a robust form such as success or failure, since “intermediate” modes of operation of the system or equivalently the degraded performance of the system (up to the failure point) is possible.

The current PSA framework has some limitations in handling the actual timing of events, whose variability may influence the successive evolution of the scenarios, and in modeling the interactions between the physical evolution of the process variables (temperatures, pressures, mass flows, etc.,) and the behavior of the hardware components. Thus, differences in the sequential order of the same success and failure events and the timing of event occurrence along an accident scenario may affect its evolution and outcome; also, the evolution of the process variables (temperatures, pressures, mass flows, etc.,) may affect the event occurrence probabilities and thus the developing scenario. Another limitation lies in the binary representations of system states (i.e., success or failure), disregarding the intermediate states, which conversely concern the passive system operation, as illustrated above.

To overcome the above-mentioned limitations, dynamic methodologies have been investigated which attempt to capture the integrated response of the systems/components during an accident scenario (ref.14).

The most evident difference between dynamic event trees (DETs) and the event trees (ETs) is as follows. ETs, which are typically used in the industrial PSA, are constructed by an analyst, and their branches are based on success/ failure criteria set by the analyst. These criteria are based on simulations of the plant dynamics. Instead, DETs are produced by a software that embeds the models that simulates the plant dynamics into stochastic models of components failure. A challenge arising from the dynamic approach to PSA is that the number of scenarios to be analyzed is much larger than that of the classical fault/event tree approaches, so that the a posteriori information retrieval can become quite burdensome and difficult.

This is even more relevant as far as thermal hydraulic natural circulation passive systems are concerned since their operation is strongly dependent, more than other safety systems, upon time and the state/parameter evolution of the system during the accident progression.

Thus the goal of dynamic PRA is to account for the interaction of the process dynamics and the stochastic nature/behavior 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.

4.9. Aging

This aspect is mostly related to life extension requirement of the plant and license renewal process. In general if passive SSCs are considered those that do not move to function (such as, structures, heat exchangers, cables, valve and pump bodies, and piping), their age related degradation can only be monitored and trended by performing periodic condition assessments (such as inspections, testing, and measurements). An aging evaluation is typically required to identify the degradation mechanisms and to select the effective inspections and tests.

On the contrary the aging management of active SSCs should be part of the plant maintenance program. Good maintenance practices should identify and correct any aging degradation issues of the active SSCs and that no special license renewal aging management requirements are necessary for extended operational approval.

However ageing of passive systems must be considered for longer plant life, since some aging mechanisms can be detrimental to their operation, for example corrosion and deposits on heat exchanger surfaces could impair their function.

4.10. Inspection and tests

This aspect is strictly related to the previous one. In general active systems will undergo a more significant inspection and test program than passive ones, which should be conceived for ease of inspection, testing and maintenance so that the dose to the worker would be much less. However operational tests are required, in order to ascertain the promptness of system intervention, its functionality and its quality of being suited to serve as required for the expected range of operations and conditions.

4.11. Redundancy, independence and diversification

It is evident that both alternatives have to comply with the requisites of redundancy to meet the single failure principle, independence and diversification to the possible extent in order to cope with the common cause failures among the loops.

In particular, given that active systems include a greater number of components, this aspect is more relevant to the active configuration since the higher level of redundancy causes an higher level of

complexity of the plant, that is a risk factor itself; in addition using safety systems of the same type makes the plant vulnerable to common cause of failures.

Table here below summarizes the above discussion.

Table 1. Underlying factors of a methodology for passive vs active system assessment with respect to reliability

Factor	Active	Passive	Remark	Relevance	Pros/cons qualitative assessment
Reliability method	"Conventional" fault tree analysis	Combination of t-h and probabilistic aspects, e.g., RMPS*	Reliability assessment of passive systems as a challenging and burdensome task	The choice of the approach greatly influences the passive system assessment procedure	Cons for passive systems
Functional failure	Not considered	High significance	somewhat "innovative" mode of failure	Functional failure very relevant in case of passive systems, much less in case of active systems	Cons for passive systems
Uncertainties	• parameters • modelling • completeness	Large amount of uncertainties	Uncertainties largely affect confidence in reliability figure for passive systems	Most relevant factor affecting system response prediction	Cons for passive systems
Licensing	Safety margin	Safety margin	Lesser safety margin to accommodate for uncertainties in case of passive systems		Cons for passive systems
Time response	Mechanical component operation for system inception	Mechanical component operation / initial conditions for system inception	Start-up stage more critical for passive system	Most significant factor for passive system	Cons for passive systems

Mission time	"Conventional" 24 hours	Grace time of 72 hours	Extension of mission time to recover from the accident for extended accident scenarios	Mission time to be lengthened according to extended scenarios and long term station black-out as Fukushima accident	Pro for passive systems
External events	Design to withstand external events	Design to withstand external events	Role of passive systems relevant for the mitigation of external events	Implementation of passive systems to cope with external events, see Fukushima event	Pro for passive systems
Human factor	Human error probability evaluation methods, e.g., THERP**	Human factor to be almost disregarded		Human failure very relevant in case of active system, much less in case of passive system	Pro for passive systems
Integration in accident sequence	"Conventional" event tree analysis	Dynamic event tree	Not mature technique yet	High significance of passive system performance in accident sequence definition and assessment	Cons for passive systems
Aging	Relevant for life extension	Low relevance	Applies as well to passive systems but to a lesser extent	More relevant to active systems than passive ones	Pro for passive systems
Inspection and Tests	Tests for system operability	System degradation monitored by testing and measurements	Applies as well to passive systems but to a lesser extent	More relevant to active systems than passive ones	Pro for passive systems

Redundancy, independence and diversification	Reliability improvement (single failure criterion); independence, separation and diversification to cope with CCF***	Reliability improvement (single failure criterion); independence, separation and diversification to cope with CCF***	Great relevance of loop configuration; higher level of redundancy causes an higher level of complexity of the plant	Safety analysis affected by the configuration; system configuration is more relevant to active systems	Pro for passive systems

* Reliability Methods for Passive Systems ** Technique for Human Error Rate Prediction *** Common Cause Failur

5. Conclusions

The concern arising from the factors impairing their performance and the related high level of uncertainty and low driving forces for heat removal purposes, justify the comparative evaluation between passive and active options, with respect to the accomplishment of a defined safety function (e.g. decay heat removal) and the generally accepted viewpoint that passive system design is more reliable and more economical than active system design has to be discussed. For this purpose a methodology approach has been introduced in order to identify the criteria suitable to drive the assessment process, in terms of highly relevant factors, and to derive the relative guidelines. For this reason both active and passive systems designed to accomplish the required safety functions, as the decay heat removal, have been deeply investigated mainly in terms of their safety performance and reliability shaping factors. The analysis revealed some important insights, calling significant efforts to be invested in new projects to fulfil the ambitious safety goals. With reference to passive systems, it is recognized that their reliability assessment is still an open issue, mainly due to the amount of concerned uncertainties, to be resolved among the community of researchers in the nuclear safety.

Results of our study raise doubts concerning the common understandings about passive design being more reliable than active design, once accounting also for the relative weigh of the underlying factors.

This study has identified some potential detrimental factors in passive design, which can not be overlooked: the first is high functional failure probability and the second is the large amount of uncertainties related to the system performance assessment together with the complexity of the approach itself. That is, when considering the impact of functional failure, the active system becomes more reliable than the passive system.

In particular Table 1 demonstrates this argument by presenting and comparing the factors of the active and passive design on a reliability plane.

This conclusion is consistent with the outcomes of companion studies (ref. 1 and 2), which pose concerns about their claimed higher reliability and availability, making the passive system positioned at a less reliable point than the active system in the reliability plane.

Lastly one can conclude that passive system reliability is not better or worse than the active ones: a good overall plant design may include active systems, passive systems or combination of both types of systems to meet performance and safety objectives.

References

1. Burgazzi L., Giannetti F. et al.,Valutazione della risposta di sistemi attivi e passivi a fronte di sequenze incidentali rilevanti ai fini della sicurezza, ENEA report NNFISS-LP2-066, Agosto 2012
2. Burgazzi L., Giannetti F. et al., Confronto e valutazione della risposta di sistemi attivi e passivi in reattori innovativi a fronte di sequenze incidentali significative ai fini della sicurezza, ENEA report ADPFISS-LP1-004, Settembre 2013
3. Buchner H., Fabian H., Comparative evaluation of active vs passive system designs, Reliability Engineering and System Safety, 45, 195-200, 1994
4. Sato T., Tanabe A., PSA in Design of Passive/Active Safety Reactors, Reliability Engineering and System Safety, 50, 17-32, 1995
5. Dube D., Comparison of New Light-Water Reactor Risk Profiles, Proceedings of *ANS PSA 2008 Topical Meeting* Knoxville, Tennessee, September 7–11, 2008, , American Nuclear Society, LaGrange Park, IL (2008)
6. JiYong Oh and Golay M., Methods for Comparative Assessment of Active and Passive Safety Systems with respect to Reliability, Uncertainty, Economy and Flexibility. Proceedings of PSAM9, 9th International Probabilistic, Safety Assessment and Management Conference Hong Kong, 18-23 May 2008
7. Burgazzi L., Addressing the Challenges posed by Advanced Reactor Passive Safety System Performance Assessment, Nuclear Engineering and Design 241, 1834-1841, 2011
8. Marques M. and Burgazzi L. et al., 2005. Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment. Nuclear Engineering and Design 235, 2612-2631.
9. Burgazzi L., 2003. Reliability Evaluation of Passive Systems through Functional Reliability Assessment, Nuclear Technology 144, 145-151.
10. Kloos M. and Peschke J., Model uncertainties in a PSA for a nuclear power plant, Proceedings of ESREL 2009, September 2009, Prague, Czech republic
11. Burgazzi L., 2007, Thermal–hydraulic passive system reliability-based design approach, Reliability Engineering and System Safety 92 (2007) 1250–1257
12. Matzie R. A. and Worrally A., The AP1000 reactor—the Nuclear Renaissance Option. Nuclear Energy, 2004, 43, No. 1, Feb., 33–45

13. Swain A.D. and Guttmann H.E., "*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*", NUREG/CR-1278, Sandia National Laboratories (1983).
14. Mercurio D., Podofillini L., Zio E., Identification and Classification of Dynamic Event Tree Scenarios via Possibilistic Clustering: Application to a Steam Generator Tube Rupture Event. Accident Analysis and Prevention 41 (2009), 1180–1191