Establishing the Criteria for the Evaluation Active vs Passive Safety Systems

Luciano Burgazzi

ENEA, Via Martiri di Monte Sole 4, 40129 Bologna, Italy, luciano.burgazzi@enea.it

INTRODUCTION

An important measure to enhance the safety in many concepts of the next generation plants is the utilisation of passive systems in a reasonable combination with or instead of "traditional" active systems. The right balance of active and passive systems entails the evaluation of basic criteria for decision-making. If one acknowledges that passive systems/components, due to their inherent features, have the potential for some advantages over the active ones, they pose, however, some challenges as regards the alleged higher reliability, because of the likelihood of physical phenomena leading to pertinent failure modes [1].

The goal of the work is to establish guidelines and criteria for the comparison of either option.

The analysis of a natural circulation system against an active system to accomplish the decay heat removal safety function is performed with respect to a set of factors.

METHODOLOGY

Both active and passive systems have been investigated in terms of the following safety performance and reliability shaping factors.

- Reliability Approach
- Functional Failure
- Uncertainties
- Safety Margin
- Time Response
- External Events
- Human Factor
- Integration within Accident Sequences
- Redundancy, Independence and CCF

Reliability Approach

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) [2]. Distinguishing attribute of this methodology is that it merges the probabilistic and t-h aspects of the problem: a suitable t-h code is used for uncertainty propagation, the uncertainties in parameters are modelled by probabilistic density functions and expert judgement is largely adopted.

Functional Failure

Passive systems display exclusive failure mechanisms, termed functional failures, due to a deviation from expected conditions, rather than the hardware failure of a mechanical component. Functional failures can challenge the performance of passive systems relying on natural circulation, and difficulties arise in modeling the system using classical fault and event trees.

Uncertainties

While the uncertainties related to PSA are appropriate with regard to active systems reliability process, the phenomenological uncertainty becomes particularly relevant when innovative or untested technologies are applied as in case of passive systems, contributing significantly to the overall uncertainty related to the reliability assessment. An adequate treatment of the uncertainties relies on expert elicitation [3].

Safety Margin

The evaluation and characterization of safety margins into risk-informed approaches adopts a basic framework that is represented by the Load-Capacity interference model, through the probability that the capacity exceeds the load, as illustrated in Fig.1. Clearly safety margin in case of passive systems is to be considered lesser as compared to active ones, since it has to accommodate the large amount of uncertainties.

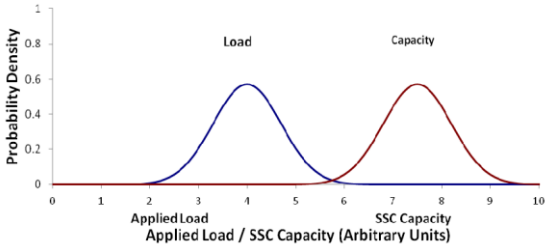

Fig.1 Load-Capacity interference model

Time Response

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 start and run is also required, the establishment of the initial conditions/mechanisms for natural circulation start-up is the prerequisite. Due to the occurrence of the actuation conditions, it appears that the system onset presents some

criticalities for passive systems, because of the proneness to flow instabilities during the start-up transients [4].

External events

One of the important considerations is that, following an extreme external event, 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).

Human Factor

While passive system operation is characterised by no or very limited reliance on human action, implying no inclusion of operator error in the analysis, conversely, in case of active systems reliability, 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 cannot be completely neglected.

Integration within Accident Sequences

Since the reliability figure dependence on the phenomenological nature of failure modes rather than component mechanical and electrical faults, the introduction of passive safety systems into an accident scenario, modelled through the event tree technique, requires the implementation of new approaches.

The strong dependence of passive system operation upon time and state/parameter evolution during the accident progression, makes necessary the application of dynamic methodologies [5]. This is in order to overcome some of the PSA limitations, as the treatment of actual timing of events and the binary representation of states (i.e., success or failure), disregarding the intermediate states, which, conversely, can characterize passive system operation [6].

Redundancy, Independence and CCF

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 a higher level of complexity of the plant that is a risk factor itself. Interaction among redundant loops and modelling of synergistic effects among the systems are important aspects to analyse for NPP designs with multiple passive systems, implying not a passive system operating one at a time.

RESULTS

Table 1 summarizes the above analysis by presenting and comparing the factors in terms of safety performance and reliability shaping factors.

The analysis identifies the functional failure probability and the amount of uncertainties, as most relevant factors to the system performance assessment in passive design. This poses concerns about the claimed higher reliability and availability deriving from their use, even making the passive system positioned at a less reliable point than the active system in the reliability plane, according to the outcomes of companion studies [7].

REFERENCES

1. H. BUCHNER, H. FABIAN, “Comparative Evaluation of Active vs Passive System Design”, Reliability Engineering and System Safety, 45, 195-200, 1994
2. M. MARQUES, et al., “Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment”, Nuclear Engineering and Design 235, 2612-2631, 2005
3. E. ZIO, N. PEDRONI, “Building Confidence in the Reliability Assessment of a Thermal-Hydraulic Passive Systems”, Reliability Engineering and System Design”, 94, 268-281, 2009
4. S. SHI, T. HIBIKI, M. ISHII, “Start-up Instability in Natural Circulation Driven Nuclear Reactors”, Progress in Nuclear Energy, 90, 140-150, 2016
5. E .ZIO, et al. “Identification and Classification of Dynamic Event Tree Scenarios via Possibilistic Clustering: Application to a Steam Generator Tube Rupture Event”, Accident Analysis and Prevention 41, 1180–1191, 2009
6. L. BURGAZZI, “Addressing the Challenges posed by Advanced Reactor Passive Safety System Performance Assessment”, Nuclear Engineering and Design 241, 1834 1841, 2011
7. JIYONG OH and M. GOLAY, “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

Factor	Active	Passive	Remark	Relevance	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; Capability to model passive system performance	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
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
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 a 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 Failure

Table 1 Underlying factors of an approach for passive vs active systems assessment with respect to reliability