Western European
WENRA RHWG
Nuclear Regulators Association

Report
Regulatory Aspects of Passive Systems

A RHWG report
for the attention of WENRA
01 June 2018

Table of Content

Regulatory Aspects of Passive Systems

-

00
Foreword

New nuclear power plant designs propose to rely more heavily on passive systems to fulfill several safety functions. This design choice is usually driven as the passive systems relies less on human actions and support systems than active systems.

Considering that safety expectations for passive and active systems are similar and that only the approaches to implement them may differ, several attributes of passive systems are worthwhile to be considered.

Indeed, passive systems bring promising safety benefits, e.g. increased grace period and autonomy for SBO and LUHS. However passive systems operate differently than active systems. Whilst the existing passive safety systems designs have undergone extensive testing and analysis over the last few decades, the reliability of the passive systems shall be demonstrated for all relevant hazards and accident.

Concerning actuation of passive systems, some passive safety systems need no component state changes at all. The other ones also have advantages associated with a limited number of component state changes and the potential absence of support features. Nevertheless, an in-depth case by case safety assessment similar to active systems is still required for these passive safety systems.

Concerning the performance of safety function, for systems relying on low driving forces the range of conditions necessary to perform the safety function could be narrow. Thus, demonstration that a passive system using low driving forces can ensure a safety function with a high level of reliability should recognize and, when relevant, address the following that could be different compared to other systems:

- failure mode analysis: comprehensive knowledge and understanding of phenomena that could influence the performance or failure of a passive system should be established considering the driving forces involved;
- impact of environmental conditions on passive system performance;
- application of margins, to ensure distance to cliff-edge effects;
- a dynamic behavior of passive systems performance;
- evaluation of potential adverse system interactions with emphasis on the effect that active systems supporting normal operation have on the function of passive systems relied upon to fulfill safety functions.

In general, the performance demonstration could be different from active systems.

In addition, computer codes for system modelling should be able to model the phenomena within the range of operating conditions that are relevant for the performance of passive systems. This may require specific experimental tests to validate the codes. However, in some cases, it could be the same as active systems that may also use low driving force passive cooling mechanism.

Moreover, even if use of passive systems does not impact the safety approach to internal and external hazards, specific attention should be paid to conditions resulting from internal and external hazards to confirm that the necessary boundary conditions to have a successful operation of the passive systems are still met.

Although the performance of passive systems does not rely on operator actions, sensitivity of passive systems to human errors should also be carefully considered.

Within the PSA, the reliability model should consider the occurrence of the root causes which may prevent the safety function being delivered by the passive system due to the range of conditions under which it has to initiate and over which it has to maintain its performance.

The aforementioned concerns especially those related to passive systems using low driving forces show a need for confidence building by all stakeholders involved in the design validation and verification.

01
Introduction / Goal of the report

-

Both innovative and evolutionary new nuclear power plant (NPP) designs propose to rely more heavily on passive systems to fulfill several safety functions. These passive systems are often presented by the designers as highly beneficial for the safety of the plant. The current fleet of NPP already uses passive systems to some extent from which some level of operating experience can be gained.

WENRA has published its safety reference levels for existing nuclear power plants (NPP) and its safety objectives for new NPPs. These documents have been designed to be technology neutral. Thus, by principle, they are relevant for NPP designs relying on any kind of systems. Nevertheless, they are based on an understanding of current designs. The increased emphasis on passive systems and potentially new design concepts for their designs may challenge this basis and the approach for their implementation.

The goal of this report is to draw attention on attributes of passive systems that are worthwhile to be considered with regards to safety in view of current regulatory practices in Europe. This report reviews some of the key features of passive systems and stress on the potential need to provide the regulator with specific justifications.

02
Scope of the Report

International standards do not establish a clear definition of passive systems: the IAEA Safety Glossary (2016) does not include such a definition but an IAEA TECDOC (see [1]) gives a quite flexible definition: *"either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation"*[1].

Many types of systems are claimed as being passive by designers, varying from equipment composed of structures such as static barriers to complex systems. The latter might rely on fluid movement and/or component actuation possibly based on an active I&C signal.

All of these systems comply with the quite flexible definition aforementioned. On the basis of this definition and of the specificities generally enhanced by designers to claim that systems are passive (see [2]), RHWG identifies what it considers to be the main attributes of passive systems in greater detail in the Annex

It is worthwhile to draw attention to these attributes and consequential technical characteristics with regards to safety in view of current regulatory practices within Europe. Thus, in this context, there is no need to refine the definition, neither to dispute the "passivity" of some systems.

The scope of the report includes all systems that contribute to the fulfillment of a safety function and that could be considered as somehow passive, independent of their actuation mode: the annex details essential attributes and consequential technical characteristics of such systems whilst remaining independent of the reactor design.

As a simplified illustration, the following means are relied upon on existing designs of NPP to control an event with loss of active cooling:

- High Temperature Reactor (HTR, gas cooled reactor): heat removal commonly relies only on radiation heat transfer. There is no need of any component movement to be effective to remove the heat from the core to outside of the installation;
- Light Water Reactor: the cooling is guaranteed by a separate system with a heat exchanger. This system is actuated by opening a valve, but the heat removal is performed without any other component than the heat exchanger, just natural circulation.

Both cases are in the scope of the report.

Particularities of structures such as static barriers are well-codified and do not need further discussion. Thus, they are out of scope of this report even though they are obviously credited as passive.

[1] The European Utility requirements provide also a quite flexible, even if more accurate definition.

This report is generally based on the knowledge of passive heat removal systems as an example of a passive system. Whilst it is expected that the majority of the outputs will be applicable to all passive systems, this may not be the case for all systems. Moreover, it should be noted that some of the topics of this report are mainly relevant only for the subset of passive systems implying low driving forces. A case by case study may have to be conducted for those systems, taking into account the insights of this report.

03
Safety Assessment

The safety assessment of any system, independent of its active or passive nature, should consider both the correct actuation and performance of the system stating that passive systems are not immune to failures. Same as for active safety systems, the contribution of passive safety systems to the achievement of defense in depth needs to be assessed, including addressing single and common cause failure. On this basis, this section addresses actuation and performance of the system when passive systems are considered.

03.1 Actuation of a passive system

The actuation of a passive system is often characterised by a limited use of components that need to change state and generally by not relying on support features. Such characteristics are expected to be favourable to safety, notably because they could lead to lower actuation failure likelihood, and they could simplify the safety assessment. However, this low failure likelihood needs to be demonstrated by a comprehensive analysis and needs to be ensured by verification of the components' operational availability[2] as well as the availability of the necessary I&C and support systems needed for their actuation, if any. In addition, if driving forces necessary to actuate a component in a passive system are low[3] (see for example foreword of [2] and [3]), there may even be a need of in-depth analysis of traditional approach to failures of some components[4]. The inadvertent actuation of a passive feature may also have sometimes major consequences, e.g. the depressurisation of a primary circuit or the loss of containment integrity. The consequences of inadvertent actuations should be studied.

The actuation of passive systems, even if there are advantages associated with a limited number of component state changes and the potential absence or lower utilization of support features, still requires an in-depth case by case safety assessment similar to active systems. These are covered by existing framework.

This section does not apply to passive safety systems that do not need component state changes for actuation at all.

03.2 Performance of safety function

Specific range of conditions and consequences on safety analysis

International scientific literature generally mentions low driving forces as typical for passive systems with fluids, e.g. see foreword of [2] or [3]. Low driving forces may challenge the per-

[2] For example, the testability of a component that relies on stored energy could be challenging while release of this energy could mean destruction of the component (e.g. a squib valve)

[3] For example gravity driven flow compared to pump driven flow.

[4] To illustrate this position, a check-valve can be considered. This is a component whose failure might be considered as particularly unlikely when the pressure differential over the valve is sufficiently high, as is the case for active systems. Nonetheless, the pressure differential generated by natural circulation and the related uncertainties may invalidate this conclusion.

formance of the system to fulfill a safety function, in particular when associated with uncertainties in the model correlations, in the initial conditions and in the boundary conditions. Thus, care has to be taken to the specific range of conditions necessary to perform the safety function, taking into account that this range of conditions could be narrow.

Therefore, demonstration that a passive system can ensure a safety function with a high level of reliability should recognize and, when relevant, address the following:

- **The failure mode analysis could be different compared to active systems**, while some phenomena that can be usually neglected could jeopardize the safety function (e.g. non condensable gases[5], leakages). **Comprehensive knowledge and understanding of phenomena and parameters that could influence the performance or failure of a passive system should be established considering the driving forces involved.** This specific set of failure modes should be particularly assessed with regards to the independency of the different levels of defence-in-depth when passive systems are credited for different levels. Its establishment is also necessary for the definition of the relevant failure to consider in events assessment, such as aggravating or common cause failure.
- **The impact of environmental conditions on system performance needs to be considered and a passive system could be particularly sensitive to these environmental conditions[6]:** it may be necessary to fulfill not only a specific range of internal conditions, but also a specific range of external ones (e.g. external temperature for a system that relies on condensation phenomena).
- **The application of concept of margins, especially to ensure distance to cliff-edge effects, could be more demanding considering, notably, the uncertainties in the performance of passive systems.** It is generally expected that safety demonstration shows that a limited change in the magnitude of a parameter could not challenge the satisfactory performance of the safety function. Taking into account that the range of conditions necessary to perform the safety function could be narrow for passive systems, a limited change of these conditions may be more or less challenging. Depending on the type of passive systems and the involved driven forces, case by case analyses are recommended. During safety analysis, consideration should be given to parameters which may change and to the potential causes of these changes (e.g. due to impact induced deformation) with due consideration of uncertainties. For example, changes of parameters due to ageing should notably be considered and, if necessary, ageing management should be adapted accordingly.

[5] Non condensable gases in a steam-water mixture that cannot be condensed in a heat exchanger do not contribute to the driven term. Furthermore they can accumulate as such blocking the flow in a steam-water natural circulation system. For a single phase natural circulation, accumulation of non-condensable gases could form a plug. These concerns may be addressed by gas venting mechanism using pressure difference. This concern is also applicable to some active systems that rely on natural circulation of primary coolant via SG tubes (e.g. hydrogen).

[6] Particularly true for passive systems using direct air cooling of a heat exchanger or a containment. In other cases, the impact may be moderate.

- **It is necessary to consider that passive systems performance may show a dynamic behavior.** The operation of a passive system can change the boundary conditions and thus influence the driving forces (e.g. during natural circulation the system is being cooled, reducing the temperature difference with the cold source, thus reducing the driving forces). Because of that, the conclusions about the system's ability to perform, its intended safety function for the full duration of its mission time may be more complex.
- For some passive systems, to ensure sufficient driving forces, it may be necessary to intentionally open permanently the reactor coolant system (IAEA TECDOC-1624 [2] illustrates this aspect for several passive reactors). **Even if opening is not directly connected to containment atmosphere, fulfilment of confinement safety function may need a specific attention with these types of passive systems.**

The following chapters deal with the consideration of these aspects focusing on some general items of the safety demonstration:

- Performance demonstration, including the use of computer modelling codes;
- Consideration of hazards;
- Consideration of human action;
- Probabilistic safety assessment.

Performance demonstration

Phenomena and parameters that influence the performance of a passive system can be rather different than for an active system due to the specific range of operating conditions, hence the performance demonstration could be also different from active systems.

A list of phenomena should be established, e.g. by performing a specific failure mode analysis. Attention should also be given to the influence of active systems, also those not important to safety, whose actuation could challenge the performance of passive systems.

After concluding that all the above factors of influence are comprehensively identified, well-known and understood with a sufficient accuracy, a set of representative parameters, including their ranges to define the boundary conditions, should be established to demonstrate the performance of safety function. This includes the definition of tests to validate a new design.

In addition, the range of operating conditions for passive systems can differ from active systems and hence can be out of the domain of validation for the computer modelling code used within the performance demonstration. This may require specific experimental tests to validate the codes.

Taking into account that the range of conditions necessary to perform the safety function could be narrow for passive systems, it is emphasized that:

- **reciprocal influences[7] should be adequately considered, notably through integral effects tests;**
- **effects of test scaling may be challenging to characterize.**

[7] For example, temperature influences the volume of non-condensable gases, friction influences stratification…

The capability of putting the plant into a stable long term condition in a timely manner should also be considered. In particular, the definition of and the provisions to reach the final safe state need to be addressed.

The ability of a passive system to perform its safety function shall be ensured over the whole plant life time as for an active system.

Representative commissioning and periodic tests program during the operation phase may be unique compared to active systems as the representative test conditions to qualify the system or for periodic testing will be different. An appropriate commissioning and in-service test program should be defined and justified.

To guarantee the qualification over the whole plant life time, parameters necessary to justify the operability should be followed during day to day operation and integrated into the Operational Limits and Conditions (OLC). The means for condition monitoring (including adequate instrumentation) should be available and could be different than for an active system.

Internal and external hazards consideration for passive systems

According to WENRA Reference Level T5.3, *"the protection concept [for natural hazards] shall ensure that measures to cope with a design basis accident remain effective during and following a design basis event"*. More generally, attention should be given to hazards that could challenge the operation of systems important to safety as defined by the IAEA SSR-2/1 requirement: *"items important to safety shall be designed and located… to withstand the effects of hazards or to be protected… against hazards and against common cause failure mechanisms generated by hazards"*.

In general, a hazard modifies the environmental conditions that systems have to cope with. For active systems, they can be dealt with by technological choices to ensure that active components can withstand these changes. Yet, the efficiency of passive systems generally relies on a specific range of boundary conditions. Thus, some passive systems may be more sensitive to environmental changes induced by hazards and this potential sensitivity should be evaluated, e.g.:

- Environmental conditions that change air temperature, moisture and particles concentration in the air for a system that uses the atmosphere as heat sink,
- Fire that could modify the necessary temperature distribution in a system that uses buoyancy for fluid circulation,
- Pipe deformation in the case of seismic event or load drop for a system that uses natural fluid circulation.

Addressing these questions will probably be more complicated for DEC conditions. WENRA Reference Level T6.3 requires that, *"when assessing the effects of natural hazards included in the DEC analysis, and identifying reasonably practicable improvements related to such events, analysis shall, as far as practicable, include demonstration of sufficient margins to avoid 'cliff-edge effects' that would result in loss of a fundamental safety function"*. The demonstration of sufficient margins to cliff-edge effects might be more challenging due to a potential narrow range of conditions.

Use of passive systems does not lead to modifications with regard to the safety approach to establish the protection concept against hazards. Nevertheless specific attention should be

paid to conditions resulting from hazards to confirm that the necessary boundary conditions to have a successful operation of the passive systems are still met.

Consideration of human actions

Although the performance of passive systems does not rely on operator actions, human actions should be carefully considered when assessing passive systems.

Firstly, due to the often limited number of components for the system's actuation and the elimination of human action for the system's performance, RHWG recognizes the reduced potential for human error. Nevertheless, sensitivity to human errors has to be addressed. This could challenge achieving appropriate operating conditions. Sensitivity of passive systems to human errors should be carefully considered in the design phase, construction phase (e.g. foreign materials such as tools) and operation phase (e.g. maintenance activities).

Moreover, despite that the safety demonstration for passive systems does generally not rely on operator actions, the potential benefits or needs of human actions during accidental conditions should be anticipated. Relevant monitoring should be implemented with the objective to provide information on the status of the performance of passive systems. In this context, EOPs and SAMGs should be established with the same accuracy for designs with passive systems as for those with active ones.

Finally, the feasibility of necessary human actions and monitoring should be ensured and the safety of the on-site personnel should not be forgotten. Satisfying these needs usually requires a reliable source of continuous power (e.g. for monitoring, lighting, ventilation).

Probabilistic Safety Assessment

Within the PSA model, all accident sequences induced by the initiating events are systematically analyzed. The role of all SSCs and human actions involved in the accident development is identified and the corresponding reliability assessment is performed.

The reliability assessment of active systems mainly relies on failure probability of components. For passive systems, it should not be neglected that phenomena which are necessary to initiate and/or to maintain the passive system function may be ineffective and lead to a failure probability of passive function.

In general, this requires a functional analysis and the identification of a set of representative parameters, including their specific range of conditions. This can lead to an identification of the various root causes which may prevent from reaching or maintaining these parameters within the operating range. **In order to include consideration of failures due to phenomenological causes in addition to plant failures in PSA and to confirm the relevance of this consideration, the reliability model should consider the occurrence of these root causes.**

03.3 Operating experience feedback

According to SSR-2/1, *"items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested"*. This expectation does obviously not prevent a designer from developing innovative systems. Nevertheless, SSR-2/1 states that *"where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, per-*

formance tests with specific acceptance criteria or the examination of operating experience from other relevant applications". Examination of operating experience feedback is one of the well-recognized pillars of safety assessment and obtaining such operating experience feedback could be challenging for passive systems.

Even though some passive systems already exist for the current reactor fleet, most of the systems found in current NPPs are active ones. The deployment of new reactors with passive systems will obviously provide some operating experience feedback. Nevertheless, such systems are often complemented by active systems (see [2]) to control deviation from normal operation, which could limit passive systems operation. Hence there might only be limited feedback on proven passive systems operation. However, full scale commissioning tests and periodic tests could complement operating experience feedback.

References

-

[1] IAEA TECDOC-626, Safety related terms for advanced nuclear plants, Vienna, September 1991.

[2] IAEA TECDOC-1624, Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, Vienna, November 2009.

[3] Policy and technical issues associated with the regulatory treatment of non-safety systems in passive plant designs, NRC, SECY-94-084, March 1994.

[4] IAEA SSR-2/1 (Rev.1), Safety of Nuclear Power Plants: Design, Specific Safety Requirements, Vienna, 2016

Annex

-

According to IAEA Safety Glossary (2016), *"a system comprises several components, assembled in such a way as to perform a specific (active) function"*. Many types of systems are claimed as passive by designers, varying from systems composed only with structures and static barriers to more complex systems whose function relies on fluid movement and needs a component actuation to be initiated, eventually on the basis of an I&C signal. All of these systems comply with the quite flexible definition of passive system provided by IAEA TECDOC (see [1]): *"either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation"*. It should be noted that there have been attempts to categorize these types of systems (e.g. see [1]).

The European Utility requirements provide also a quite flexible, even if more accurate definition that is worthwhile to consider within this document: *"a system which is essentially self-contained or self-supported, which relies on natural forces, such as gravity or natural circulation, or stored energy, such as batteries, rotating inertia, and compressed fluids, or energy inherent to the system itself for its motive power, and check valves and non-cycling powered valves (which may change state to perform their intended functions but do not require a subsequent change of state nor continuous availability of power to maintain their intended functions)"*.

On the basis of these definitions and of the specific claims highlighted by designers to claim that systems are passive (see [2]), RHWG identifies in more detail below the main attributes of passive systems and their consequential technical characteristics.

Two main phases should be distinguished to identify relevant characteristics, actuation (if any) and performance of safety function:

- Actuation. This phase is not always relevant for a passive system while it could be in continuous operation or simply needs the achievement of some conditions to operate: in such cases, interesting characteristics are the same for both aforementioned phases. However, actuation of a passive system could also rely on actuation of components. In such cases, actuation is generally ensured by a limited use of components that need to change state, and these components:
    - Change state only once: when actuation of the function is necessary,
    - Only rely on stored energy or are self-actuated to change state,
    - Do not rely on continuous function on support features.
- Performance of safety function. Performance of safety function is the most specific phase with regards to active systems. Within the scope of this report, one characteristic is of particular importance: the driving force(s) involved in this performance are limited to "natural forces", thus without conversion of energy (such as from electrical power to fluid flow and pressure increase or steam-driven pumps) and without any external input. The driving forces belong to the following list:
    - gravity, including density difference,
    - pressure difference,

- thermal exchanges,
- internal heating phenomena (e.g. nuclear decay heat),
- internal chemical phenomena,
- phase changes (e.g. from steam to liquid water or from liquid water to steam),
- any combination of the above forces.

There are also some other characteristics linked to those above including the absence of the need for:

- component movement,
- support features, unless they could be considered as passive,
- human action,
- I&C.

The scope of the position paper includes all systems that fulfill at least one or some of these characteristics.

A system only composed with structures and static barriers are obviously credited as passive but is out of interest of the paper, while the particularities of these elements are well-codified and do not need further guidance.

Besides, international scientific literature generally mentions low driving forces as typical for passive systems with fluids, e.g. see foreword of [2] or [3].

Finally, this report particularly addresses some types of passive systems, mainly innovative passive heat removal systems implying low driving forces (i.e. systems as reactor scram or traditional hydro-accumulators are not of interest for this document). Whilst it is expected that the majority of the outputs will be applicable to all passive systems, this may not be the case for all systems.