IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

January 2016

Considerations on the performance and reliability of passive safety systems for nuclear reactors

I. Background

Pressurized water reactors currently operating in France are equipped with safety systems which, for the most part, require a power source, such as an electrical power supply, in order to operate. They also include passive safety features, such as:

- nuclear fission reaction control and shutdown rods (which drop by gravity upon loss of electrical power) ;
- safety injection system accumulators (which inject water into the reactor coolant system when the pressure inside it drops below a preset value) ;
- thermosiphon cooling after voluntary or accidental shutdown of reactor coolant pumps (achieved by natural circulation flow due to density differences between reactor coolant system regions with different altimetry) ;
- hydrogen recombiners (which catalyze the recombination reaction of oxygen in the air with hydrogen released in the containment under accident conditions).

Certain nuclear reactor designs currently proposed by nuclear power plant designers make more extensive use of passive safety systems in order to bring the reactor to a safe shutdown state and maintain this state for a long period of time (72 hours for AP1000 reactors) without human intervention and with limited reliance on support functions.

Furthermore, since the accident at the Fukushima Dai-ichi NPP in Japan, there is a growing interest in passive safety systems, particularly to mitigate accident conditions involving long-term loss of electrical power or heat sink.

This report recalls the main characteristics of passive safety systems and outlines the main difficulties associated with assessing the performance and reliability of such systems, as well as priority research areas to be developed in order to overcome these difficulties.

II. Definition and main characteristics of passive safety systems

II.1 General

Passive safety systems are mainly characterised by:

- **reduced reliance on active components**[1] for proper actuation ;
- **reliance on natural phenomena** (gravity, differential pressure, etc.) for proper operation ;
- **not requiring support functions for proper operation ;**
- **not requiring human intervention for actuation and operation**.

II.2 Classification of passive safety systems

Given the diversity of passive safety systems available, IAEA proposes their classification into four categories, according to decreasing level of passiveness:

- systems requiring no moving mechanical parts or operating fluid, composed of static components or structures using no external power source (electrical or other) or I&C signals (e.g. static containment barriers, piping, tanks, seismic-proof structures, etc.) ; such systems are not covered in this report, as their implementation is well-known and poses no particular new difficulties ;
- systems comprising no moving mechanical parts and requiring no external power source or I&C signals for actuation or operation, but requiring operating fluid (e.g. condensers, thermosiphon cooling systems, containment sump filtration systems, etc.) ;
- systems requiring no external power source or I&C signals for actuation or operation, but comprising moving mechanical parts (e.g. accumulators, relief valves, passive pressure transmitters, containment venting and filtration systems using rupture discs, etc.) ;
- systems not requiring manual actuation, but nevertheless requiring I&C signals or an external power supply for startup (but not for subsequent operation) ; this external power can only be supplied by stored energy sources such as compressed fluid tanks, overhead tanks, or batteries (e.g. pump-driving steam turbines, pneumatic or electrically driven accumulators, etc.).

III. Operation and performance characteristics of passive safety systems

Proper operation of passive safety systems using operating fluids is ensured by physical phenomena generally involving low-intensity driving forces (such as natural convection). Such phenomena may be sensitive to various parameters.

[1] Active components require mechanical motion or external power for operation.

In order to evaluate the performance of a passive safety system, it is necessary to have a very good understanding of the physical phenomena used to actuate and operate the system, as well as those capable of preventing proper actuation or operation thereof. It is therefore necessary to first identify the main parameters associated with these phenomena for all functions[2] performed by the system, and then demonstrate that the computational software used is capable of producing reliable predictions for operating conditions where system actuation and operation are postulated.

This demonstration will generally be based on reduced-scale test results, which raises the issue of their representativity and transposition to the reactor scale.

Moreover, given the low intensity of the natural forces at play, a passive safety system's performance characteristics may be particularly sensitive to ambient conditions (e.g. containment temperature increase caused by initiating event) or external hazards (climatic, seismic, etc.).

A passive safety system's performance characteristics shall be demonstrated for the entire duration of the functions performed, and for the entire service life of the facility.

IV. Consideration on implementation of passive systems

IV.1 Safety approach

Defence-in-depth is the fundamental safety principle underlying the development of new reactor designs making more extensive use of passive systems.

It requires achieving a sufficient degree of independence between different defence-in-depth levels. However, it appears that in certain designs, a given natural physical phenomenon may impact the performance of passive systems operating at two different defence-in-depth levels. For example, the AP1000 passive containment cooling system (PCCS) uses the same physical phenomenon under accident conditions associated with defence-in-depth level 3, to remove residual heat from the reactor core so as to prevent core meltdown, and under accident conditions associated with defence-in-depth level 4, to remove heat from the containment in order to preserve its integrity under core meltdown conditions.

Using the same physical phenomenon to operate a passive system at defence-in-depth levels 3 and 4 requires a very high degree of confidence in the phenomenon's ability to ensure correct execution of the corresponding safety function under all conditions.

[2] For example, in the case of LWR containment sump filtration systems, the phenomena are different for the 'filtration' and 'recirculation' functions. Even in the case of such systems used in current reactor designs and implementing both passive and active safety features, additional justification shall be provided demonstrating compliance with expected performance criteria.

Furthermore, as illustrated by the AP1000 design, the implementation of passive safety systems may lead designers to provide for active safety systems at the same defence-in-depth level so as to reduce occurrences of passive safety systems operation. These active safety systems are not subject to the same requirements as passive safety systems and are not taken into consideration in accident studies. However, since these active safety systems may operate, at least partially, under actual accident conditions, it is necessary to assess their impact on the operation of passive safety systems and their influence on the evolution of the accident (disruption of natural flow due to maintained pressure, different temperature changes, etc.).

The presence of active safety systems may complicate the demonstration of correct operation of passive safety systems under accident conditions where the latter are required.

IV.2 Performance verification

Due to the manner in which passive safety systems operate, verify**ing their performance characteristics and the stability of these characteristics over time is a complex process** relying on the feasibility of the following:

- detailed monitoring of influential parameters (for example, operating fluid circulation depends on slight density differences and is therefore potentially sensitive to frictional head losses) ;
- periodic testing under conditions representative of system actuation and operation (for example, containment heat removal via condensation or vaporisation can be difficult to test during normal operation of a reactor).

IV.3 Reliability assessment

Passive safety system designers generally view such systems as being more reliable than active safety systems (less equipment, less need for human intervention, less dependence on electrical power sources, etc.).

The failure probability analysis of a passive safety system, typically composed of static components, may seem less complicated than for an active safety system, which generally comprises a large number of components.

However, caution should be exercised as to the truly passive nature of safety systems which, according to their designers, rely solely on natural phenomena. Indeed, most of these systems rely on changes in mechanical equipment status (e.g. valve open), actuation signals and battery power.

Furthermore, **a passive safety system may not be capable of performing its assigned function, even in the absence of mechanical or electrical failure.** Indeed, as mentioned earlier, a passive safety system may rely on low-intensity phenomena (e.g. natural convection) which, under certain conditions, may be insufficient to perform its function. Such failure may occur when the phenomena at play are sensitive to system geometry (e.g. head loss sensitivity), ambient parameters and mismatches between design expectations and actual conditions. This type of failure, referred to as a functional failure, may lead to non-actuation or shutdown of a passive safety system, or unexpected operating conditions. If the same phenomenon is used to ensure proper operation of various passive safety system components, a functional failure could affect all components. This is referred to as a **common mode failure**.

When evaluating the reliability of passive safety systems, it is important to consider the difficulty in producing conclusive probabilistic safety assessments (PSAs), in particular due to the difficulty of assigning failure probabilities to passive safety systems under all conditions covered by PSAs, and the lack of operational feedback on the reliability of such systems under accident conditions.

Specific development approaches appear to be necessary in order to properly evaluate the reliability of passive safety systems, with particular emphasis on assessing the failure probabilities of thermal-hydraulic mechanisms used by these systems.

IV.4 Expected contributions from R&D

Careful considerations are needed to determine the R&D requirements associated with the implementation of passive safety systems. For IRSN, these considerations are aimed at developing the expertise and knowledge needed to assess future technological developments possibly implemented in nuclear reactor designs making use of such systems.

As described in the present document, initial considerations for assessing the performance and reliability of such systems (at all stages, from design to operation, including manufacture and maintenance) have already been identified as part of IRSN's scientific strategy.

These scientific considerations need to be addressed within the context of nuclear safety demonstration objectives so as to be identified as open questions requiring further knowledge. In parallel, a full assessment of current knowledge shall be prepared based on available information concerning reactor designs making more extensive use of passive safety systems.

This will allow for the establishment of well-defined research areas, with emphasis on the following:

- understanding of physical phenomena influencing the operation of passive safety systems,
- simulation capabilities for such phenomena,
- testing for validation of simulation software.

Technical exchanges with industry stakeholders are essential for successful implementation of such actions. IRSN has set up a working group with AREVA, EDF and CEA for this purpose.

These research areas need to be pursued within an international framework. In particular, IRSN is participating in the NUSMOR project (NUgenia Small Modular Reactor with passive safety features) to be proposed as part of the Horizon 2020 EU framework programme.

V. Conclusion

Certain nuclear reactor designs currently under construction or development make more extensive use of passive safety systems in order to bring the reactor to a safe shutdown state and maintain this state for a long period of time without need for human intervention and with limited reliance on support functions.

IRSN considerations to date on passive safety systems have led to the identification of a number of intrinsic difficulties, particularly concerning the following:

- **performance assessment**: assessing the performance of passive safety systems requires a very good understanding of the physical phenomena underlying their operation, as well as the necessary simulation capabilities for such phenomena ;
- **reliability assessment**: specific development approaches appear to be necessary in order to properly evaluate the reliability of passive safety systems, with particular emphasis on assessing the failure probabilities of thermal-hydraulic mechanisms used by these systems.

Further research is required in order to properly assess the performance and reliability of passive safety systems to be implemented in new reactor designs. Initial considerations have already been identified as part of IRSN's scientific strategy.

IRSN pursues this research within the framework of joint actions with foreign organisations so as to ensure fruitful exchanges and benefit from available knowledge. In particular, IRSN coordinates a working group devoted to discussing new safety approaches applicable to these systems on the behalf of WENRA Reactor Harmonization Working Group. IRSN also participates in the NUSMOR project to be proposed as part of the Horizon 2020 EU framework programme for knowledge development on passive safety system performance, and coordinates a working group with French industry stakeholders in order to identify priority research areas to be developed.