Chapter 2

Reliability of Passive Systems in Nuclear Power Plants

Luciano Burgazzi

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/47862

1. Introduction

In order to tackle the development of advanced nuclear technologies, the reliability of passive systems has become an important subject and area under discussion, for their extensive use in new and advanced nuclear power plants, (NEA, 2002), in combination with active safety or operational systems.

Following the IAEA definitions, [1], a passive component does not need any external input or energy to operate and it relies only upon natural physical laws (e.g. gravity, natural convection, conduction, etc.) and/or on inherent characteristics (properties of materials, internally stored energy, etc.) and/or 'intelligent' use of the energy that is inherently available in the system (e.g. decay heat, chemical reactions etc.).

The term "passive" identifies 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. That is why passive systems are expected to combine among others, the advantages of simplicity, a decrease in the need for human interaction and a reduction or avoidance of external electrical power or signals. These attractions may lead to increased safety and acceptability of nuclear power generation if the detractions can be reduced.

Besides the open feedback on economic competitiveness, special aspects like lack of data on some phenomena, missing operating experience over the wide range of conditions, and driving forces which are smaller - in most cases - than in active safety systems, must be taken into account: the less effective performance as compared to active safety systems has a strong impact on the reliability assessment of passive safety systems.

A categorisation has been developed by the IAEA in [1] distinguishing:

a. physical barriers and static structures (e.g. pipe wall, concrete building).

This category is characterized by:

- no signal inputs of "intelligence", no external power sources or forces,
- no moving mechanical parts,
- no moving working fluid.

Examples of safety features included in this category are physical barriers against the release of fission products, such as nuclear fuel cladding and pressure boundary systems; hardened building structures for the protection of a plant against seismic and or other external events; core cooling systems relying only on heat radiation and/or conduction from nuclear fuel to outer structural parts, with the reactor in hot shutdown; and static components of safety related passive systems (e.g., tubes, pressurizers, accumulators, surge tanks), as well as structural parts (e.g., supports, shields).

b. moving working fluids (e.g. cooling by free convection).

This category is characterized by:

- no signal inputs of "intelligence", no external power sources or forces,
- no moving mechanical parts, but
- moving working fluids.

Examples of safety features included in this category are reactor shutdown/emergency cooling systems based on injection of borated water produced by the disturbance of a hydrostatic equilibrium between the pressure boundary and an external water pool; reactor emergency cooling systems based on air or water natural circulation in heat exchangers immersed in water pools (inside containment) to which the decay heat is directly transferred; containment cooling systems based on natural circulation of air flowing around the containment walls, with intake and exhaust through a stack or in tubes covering the inner walls of silos of underground reactors; and fluidic gates between process systems, such as "surge lines" of Pressurized Water Reactors (PWRs).

c. moving mechanical parts (e.g. check valves).

This category is characterized by:

- no signal inputs of "intelligence", no external power sources or forces; but
- moving mechanical parts, whether or not moving working fluids are also present.

Examples of safety features included in this category are emergency injection systems consisting of accumulators or storage tanks and discharge lines equipped with check valves; overpressure protection and/or emergency cooling devices of pressure boundary systems based on fluid release through relief valves; filtered venting systems of containments activated by rupture disks; and mechanical actuators, such as check valves and spring-loaded relief valves, as well as some trip mechanisms (e.g., temperature, pressure and level actuators).

d. external signals and stored energy (passive execution/active actuation, e.g. scram systems).

This category addresses the intermediary zone between active and passive where the execution of the safety function is made through passive methods as described in the

previous categories except that internal intelligence is not available to initiate the process. In these cases an external signal is permitted to trigger the passive process. To recognize this departure, this category is referred to as "passive execution/active initiation".

Examples of safety features included in this category are emergency core cooling and injections systems based on gravity that initiate by battery-powered electric or electro-pneumatic valves; emergency reactor shutdown systems based on gravity or static pressure driven control rods.

According to this classification, safety systems are classified into the higher categories of passivity when all their components needed for safety are passive. Systems relying on no external power supply but using a dedicated, internal power source (e.g., a battery) to supply an active component are not subject to normal, externally caused failures and are included in the lowest category of passivity. This kind of system has active and passive characteristics at different times, for example, the active opening of a valve initiates subsequent passive operation by natural convection.

Inclusion of failure modes and reliability estimates of passive components for all systems is recommended in probabilistic safety assessment (PSA)1 studies. Consequently the reliability assessment of passive safety systems, defined as the probability to perform the requested mission to achieve the generic safety function, becomes an essential step.

Notwithstanding that passive systems are credited a higher reliability with respect to active ones, – because of the smaller unavailability due to hardware failure and human error -, there is always a nonzero likelihood of the occurrence of physical phenomena leading to pertinent failure modes, once the system comes into operation. In fact the deviations of the natural forces or physical principles, upon which they rely, from the expected conditions can impair the performance of the system itself. This remark is especially applicable to type B passive systems (i.e. implementing moving working fluids) named thermal-hydraulic passive systems, due to the small engaged driving forces and the thermal-hydraulic phenomena affecting the system performance.

Indeed, while in the case of passive A systems the development of the structural reliability analysis methodology can be carried out with the application of the principles of the probabilistic structural mechanics theory, and operating experience data can be inferred for the reliability assessment of passive C and D components, there is yet no agreed approach as far as passive B systems are concerned.

In fact, such passive safety systems in their designs rely on natural forces, such as gravity or natural convection, to perform their accident prevention and mitigation functions once actuated and started: these driving forces are not generated by external power sources (e.g., pumped systems), as is the case in operating reactor designs. Because the magnitude of the natural forces, which drive the operation of passive systems, is relatively small, counter-forces (e.g. friction) can be of comparable magnitude and cannot be ignored as it is generally

[1] In the following PSA (Probabilistic Safety Assessment) and PRA (Probabilistic Risk Assessment) are utilized indifferently

the case of systems including pumps. Moreover, there are considerable uncertainties associated with factors on which the magnitude of these forces and counter forces depends (e.g. values of heat transfer coefficients and pressure losses). In addition, the magnitude of such natural driving forces depends on specific plant conditions and configurations which could exist at the time a system is called upon to perform its safety function. All these aspects affect the thermal-hydraulic (T-H) performance of the passive system.

Consequently, a lot of efforts have been devoted mostly to the development of consistent approaches and methodologies aimed at the reliability assessment of the T-H passive systems, with reference to the evaluation of the implemented physical principles (gravity, conduction, etc.). For example, the system fault tree in case of passive systems would consist of basic events, representing failure of the physical phenomena and failure of activating devices: the use of thermal-hydraulic analysis related information for modeling the passive systems should be considered in the assessment process.

The efforts conducted so far to deal with the passive safety systems reliability, have raised an amount of open issues to be addressed in a consistent way, in order to endorse the proposed approaches and to add credit to the underlying models and the eventual reliability figures, resulting from their application. In fact the applications of the proposed methodologies are to a large extent dependent upon the assumptions underlying the methods themselves. At the international level, for instance, IAEA recently coordinated a research project, denoted as "*Natural Circulation Phenomena, Modelling and Reliability of Passive Systems*" (2004-2008), [2,3], while another coordinated research project on "*Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors*" (2008-2011) is currently underway: while focus of the former project has been the natural circulation and related phenomena, the objective of the latter program is to determine a common analysis-and-test method for reliability assessment of passive safety system performance. This chapter provides the insights resulting from the analysis on the technical issues associated with assessing the reliability of passive systems in the context of nuclear safety and probabilistic safety analysis, and a viable path towards the implementation of the research efforts in the related areas is delineated as well. Focus on these issues is very important since it is the major goal of the international research activities (e.g. IAEA) to strive to reach a common consensus about the different proposed approaches. The chapter is organized as follows: after an overview on passive safety systems being implemented in the design of innovative reactors and an introduction on the main components of Probabilistic Safety Assessment approach, at first the current available methodologies are illustrated and compared, the open issues coming out from their analysis are identified and for which one of them the state of the art and the outlook is presented; the relative importance of each of them within the evaluation process is presented as well.

2. Passive systems implementation in advanced reactor designs

Several advanced water cooled reactor designs incorporate passive safety systems based on natural circulation, as described in [2,3]: some of the most relevant design concepts for

natural circulation systems are described hereafter and namely as regards AP600/AP1000, ESBWR and ABWR designs.

It is important to note that the incorporation of systems based on natural circulation to achieve plant safety and economic goals is being extended also to Generation-IV reactor concepts: however due to the early stage of the design - many systems are not yet established - they are not explicitly addressed.

2.1. AP600/AP1000 Passive Residual Heat Removal systems (PRHR)

Figure 1 presents a schematic that describes the connections of the primary system passive safety systems.

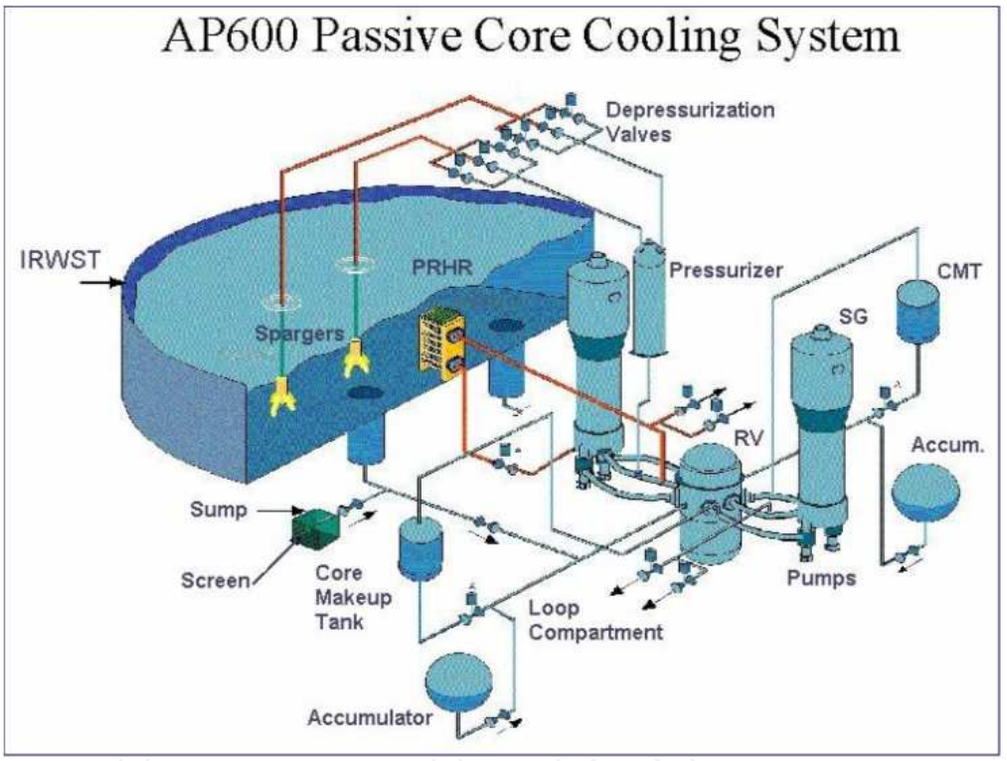

Figure 1. Passive Safety Systems used in the AP600/AP1000 Designs

The AP600/AP1000 passive safety systems consist of:

- A Passive Residual Heat Removal (PRHR) System
- Two Core Make-up Tanks (CMTs)
- A Four Stage Automatic Depressurization System (ADS)
- Two Accumulator Tanks (ACC)
- An In-containment Refueling Water Storage Tank, (IRWST)
- A Lower Containment Sump (CS)
- Passive Containment Cooling System (PCS)

The PRHR implemented in the Westinghouse AP1000 design consists of a C-Tube type heat exchanger in the water-filled In-containment Refuelling Water Storage Tank (IRWST) as

shown in the schematic given in Figure 2. The PRHR provides primary coolant heat removal via a natural circulation loop. Hot water rises through the PRHR inlet line attached to one of the hot legs. The hot water enters the tube sheet in the top header of the PRHR heat exchanger at full system pressure and temperature. The IRWST is filled with cold borated water and is open to containment heat removal from the PRHR heat exchanger occurs by boiling on the outside surface of the tubes. The cold primary coolant returns to the primary loop via the PRHR outline line that is connected to the steam generator lower head.

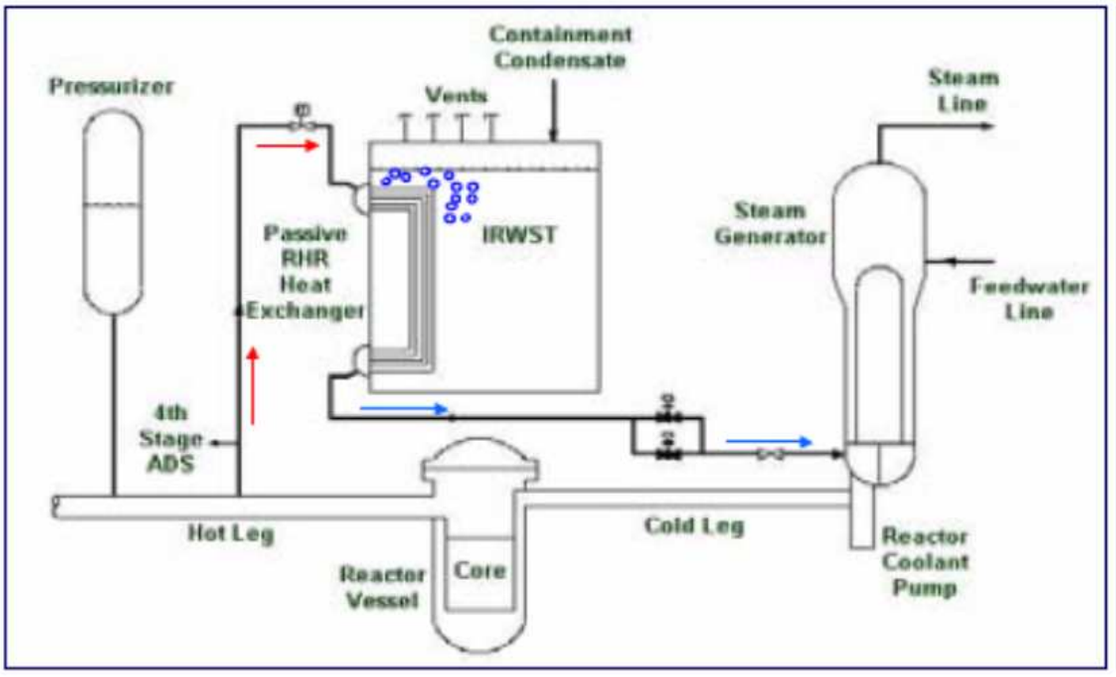

Figure 2. AP1000 passive residual heat removal systems (PRHR)

2.2. ESBWR (Economic Simplified Boiling Water Reactor) Isolation Condenser System (ICS)

During a Loss of Coolant Accident (LOCA), the reactor shuts down and the Reactor Pressure Vessel (RPV) is isolated by closing the main steam line isolation valves. The ICS removes decay heat after any reactor isolation. In other words, the ICS passively removes sensible and core decay heat from the reactor when the normal heat removal system is unavailable. Decay heat removal limits further increases in steam pressure and keeps the RPV pressure below the safety set point. The arrangement of the IC heat exchanger is shown in Figure 3.

The ICS consists of four independent loops, each containing two heat exchanger modules that condense steam inside the tube and transfers heat by heating/evaporating water in the IC pool, which is vented to the atmosphere. This transferring mechanism from IC tubes to the surrounding IC pool water is accomplished by natural convection, and no forced circulation equipment is required.

The ICS is initiated automatically by any of the following signals: high reactor pressure, main steam line isolation valve (MSIV) closure, or an RPV water level signal. To operate the

ICS, the IC condensate return valve is opened whereupon the standing condensate drains into the reactor and the steam water interface in the IC tube bundle moves downward below the lower headers.

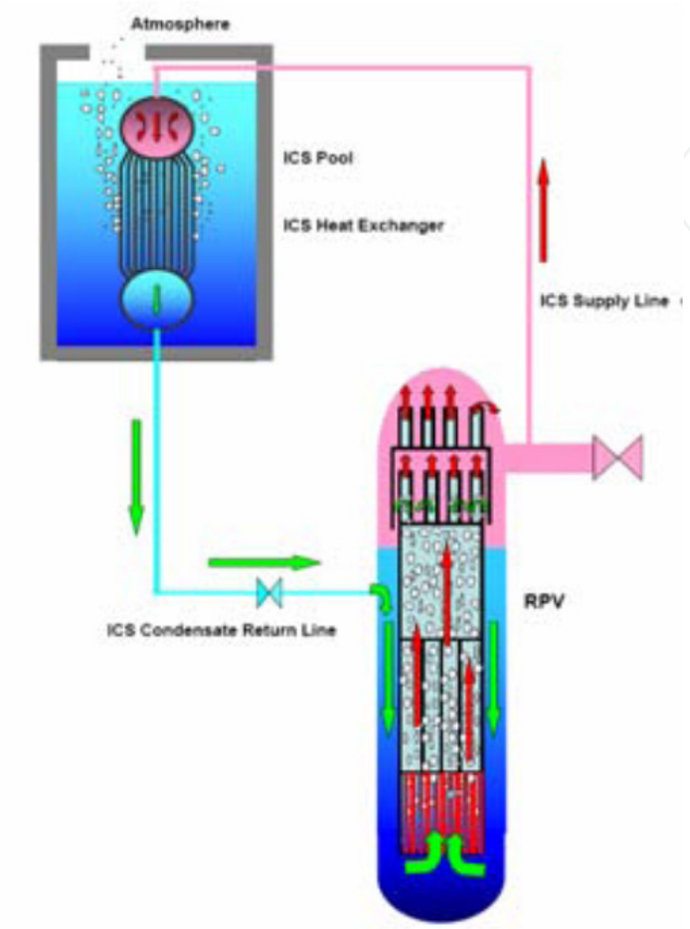

Figure 3. Isolation condenser arrangement

2.3. ESBWR Passive Containment Cooling System (PCCS)

The PCCS is a passive system which removes the decay heat released to the containment and maintains the containment within its pressure limits for design basis accidents such as a LOCA. The schematic of the PCCS is shown in Figure 4. The PCC heat exchangers receive a steam-gas mixture from the Dry Well (DW), condense the steam and return the condensate to the RPV via the Gravity Driven Cooling System GDCS pools. The non condensable gas is vented to the Wet Well (WW) gas space through a vent line submerged in the Suppression Pool (SP). The venting of the non condensable gas is driven by the differential pressure between the DW and WW. The PCCS condenser, which is open to the containment, receives a steam-gas mixture supply directly from the DW. Therefore, the PCCS operation requires no sensing, control, logic or power actuated devices for operation. The PCCS consists of six PCCS condensers. Each PCCS condenser is made of two identical modules and each entire PCCS condenser two-module assembly is designed for 11 MWt capacity. The condenser condenses steam on the tube side and transfers heat to the water in the IC/PCC pool. The evaporated

steam in the IC/PCC pool is vented to the atmosphere. PCCS condensers are located in the large open IC/PCC pool, which are designed to allow full use of the collective water inventory.

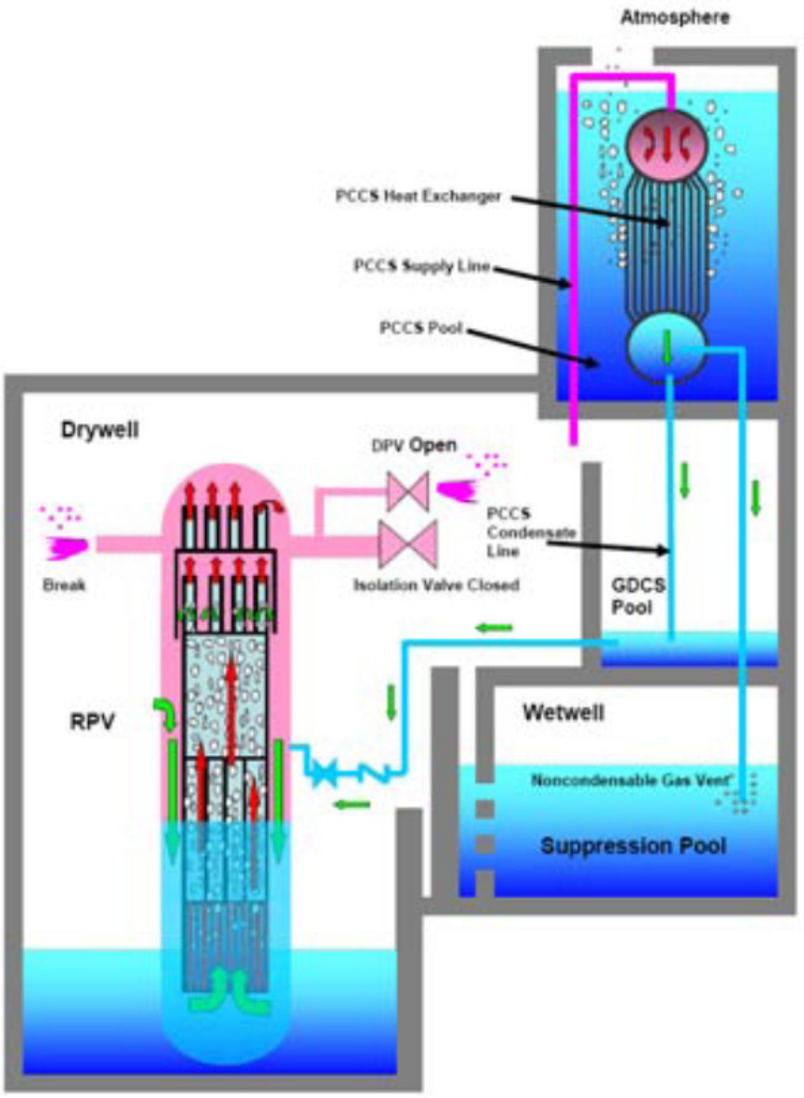

Figure 4. Passive containment cooling condenser arrangement

2.4. ABWR (Advanced Boiling Water Reactor) passive reactor cooling system and passive containment cooling system

The passive heat removal system (PHRS) consists of two dedicated systems (Figure 5, right) namely the passive reactor cooling system (PRCS: the same as Isolation condenser) and the passive containment cooling system (PCCS), that use a common heat sink pool above the containment allowing a one-day grace period, with a 4*50% redundancy (Figure 5, left). These passive systems not only cover beyond DBA condition, but also provide in-depth heat removal backup for the RHR.

In addition, they provide the overpressure protection safety function, practically excluding the necessity of containment venting before and after core damage. Figure 6 shows PCCS

functional schematic and an example of containment pressure transient following typical low pressure core melt scenario.

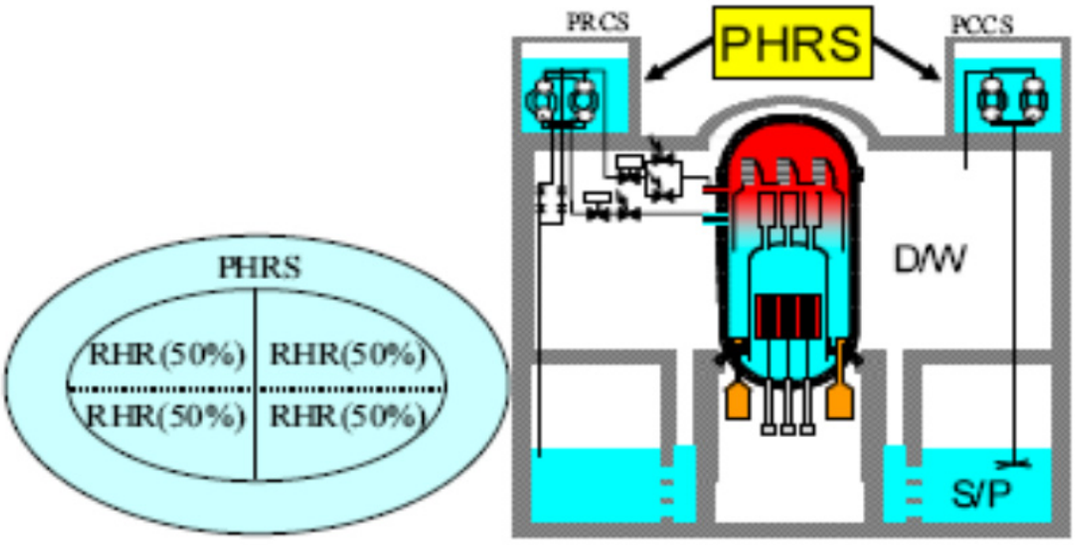

Figure 5. ABWR Passive heat removal system

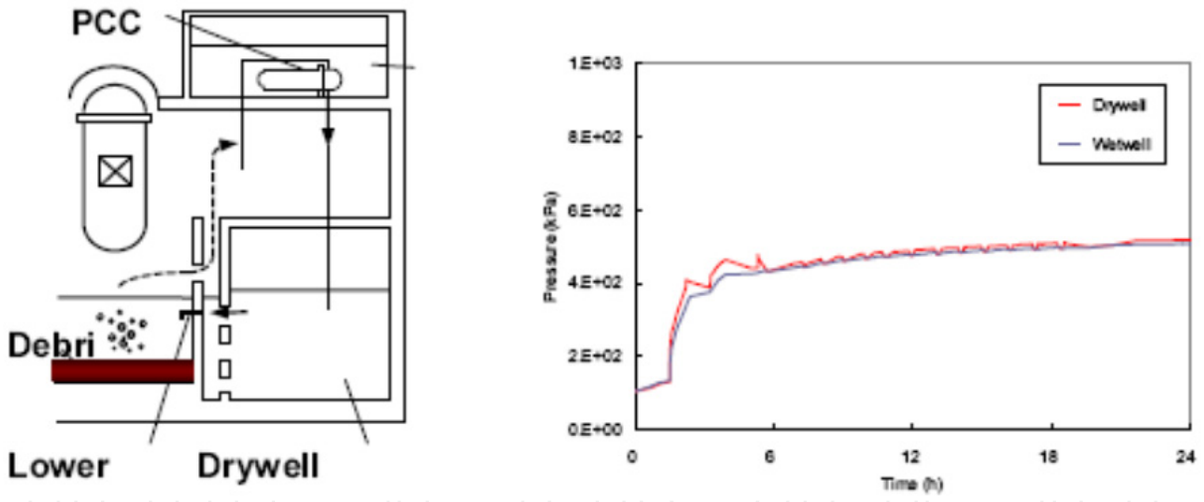

Figure 6. Example of containment pressure transient following typical low pressure core melt scenario.

3. Overview of PSA

PSA methodology widely used in the nuclear power industry is deemed helpful to the safety assessment of the facility and along the correspondent licensing process: probabilistic safety assessment can provide insights into safety and identify measures for informing designers of the safety of the plant.

The first comprehensive application of the PSA dates back to 1975, to the United States Nuclear Regulatory Commission's (U.S. NRC) Reactor Safety Study [4]. Since that pioneering study, there has been substantial methodological development, and PSA techniques have

become a standard tool in the safety evaluation of the nuclear power plants (NPPs) and industrial installations in general. Due to historical reasons, the PSA sometimes is called PRA.

As the most important area of PSA projects remains nuclear power plants, mainly due to the specific features of the nuclear installations, three levels of PSA have evolved:

Level 1:The assessment of plant failures leading to core damage and the estimation of core damage frequency. A Level 1 PSA provides insights into design weaknesses and ways of preventing core damage. In the case of other industrial assessments, Level 1 PSA provides estimates of the accidents frequency and the main contributors.

Level 2: As possible releases are additionally protected by containment in most NPPs, PSA at this response and severe accident management possibilities. The results obtained in Level 1 are the basis for Level 2 quantification. In the case of other industrial assessments, Level 2 PSA might be fully covered by Level 1, as containment function is rather unique feature and is not common in other industries.

Level 3: The assessment of off-site consequences leading to estimates of risks to the public. Level 3 incorporates results om both previous levels.

Level1 PSA is the most important level and creates the background for further risk assessment, therefore it will be presented in detail. The structure of the other levels is much more application specific, and will be discussed only in general.

The methodology is based on systematically: 1) postulating potential accident scenarios triggered by an initiating event (IE), 2) identifying the systems acting as "defences" against these scenarios, 3) decomposing the systems into components, associating the failure modes and relative probabilities, 4) assessing the frequency of the accident scenarios. Two elements of the PSA methodology typically stand out:

- The event tree (ET) which is used to model the accident scenarios: it represents the main sequences of functional success and failure of safety systems appointed to cope with the initiating events and the consequences of each sequence. These consequences, denoted also as end states, are identified either as a safe end state or an accident end state.
- The fault tree (FT) which documents the systematic, deductive analysis of all the possible causes for the failure of the required function within an accident scenario modelled by the ET. A FT analysis is performed for each of the safety systems, required in response to the IE.

Assigning the safe end state to a sequence means that the scenario has been successfully terminated and undesired consequences have not occurred. In contrast the accident end state means that the sequence has resulted in undesired consequences.

Synthetically, the methodology embraced for the analysis consists of the following major tasks:

- identification of initiating events or initiating event groups of accident sequences: each initiator is defined by a frequency of occurrence;
- systems analysis: identification of functions to be performed in response to each initiating events to successfully prevent plant damage or to mitigate the consequences

and identification of the correspondent plant systems that perform these functions (termed front-line systems): for each system the probability of failure is assessed, by fault tree model;

- accident sequences development by constructing event trees for each initiating event or initiating event groups;
- accident sequences analysis to assess the frequencies of all relevant accident sequences;
- identification of dominant sequences on a frequency-consequence base, i.e. the ones presenting the most severe consequences to the personnel, the plant, the public and the environment and definition of the reference accident scenarios to be further analysed through deterministic transient analysis (for instance by t-h code simulation), in order to verify the fulfilment of the safety criteria. Consequences in the case of Level 1 PSA of NPPs are usually defined as degrees of reactor core damage, including 'safe' state and 'severe' accident state.

One of the main issues encountered in probabilistic analysis concerns the availability of pertinent data for the quantification of the risk, which eventually raises a large uncertainty in the results achieved. Usually these data are accessible from consolidated data bases (e.g. IAEA), resulting from the operational experience of the plants.

They pertain, for instance, to component failure rates, component probability on demand, initiating event frequency: for this reason within a PSA study usually an uncertainty analysis, in addition to a sensitivity analysis, is required in order to add credit to the model and to assess if sequences have been correctly evaluated on the probabilistic standpoint.

Event trees are used for the graphical and logical presentation of the accident sequences. An example of an event tree is shown in Figure 7. The logical combinations of success/failure conditions of functions or systems (usually safety systems, also called front-line systems) in the event tree are modelled by the fault tree.

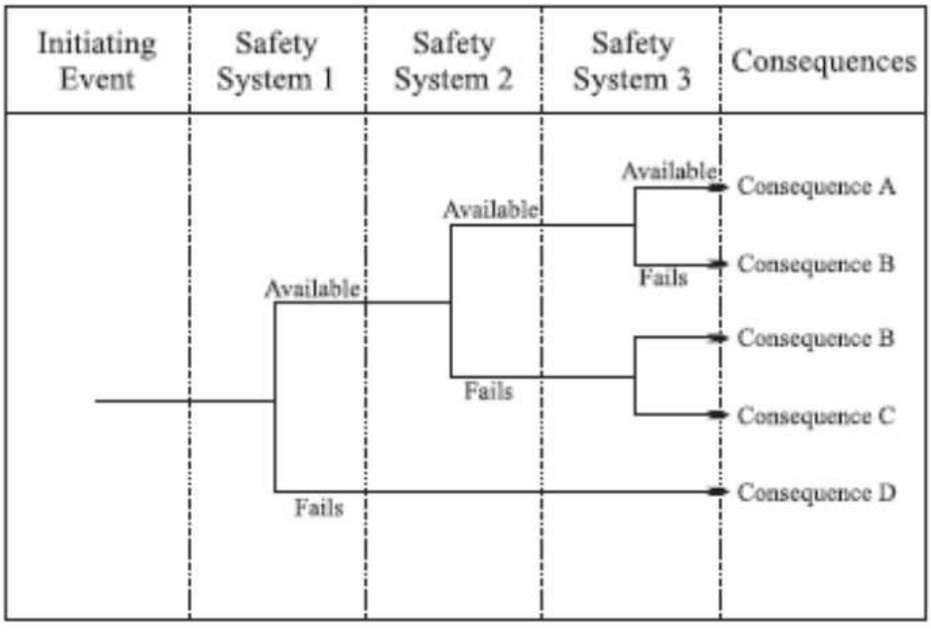

Figure 7. Example of an event tree

A fault tree logically combines the top event (e.g. complete failure of a support system) and the causes for that event (e.g. equipment failure, operator error etc.). An example of the fault tree is shown in Figure 8. The fault tree mainly consists of the basic events (all possible causes of the top event that are consistent with the level of detail of the study) and logical gates (OR, AND, M out of N and other logical operations). Other modelling tools, like common cause failures, house or area events are also used in the fault trees. All front-line and support systems are modelled by the fault trees and then combined in the event trees depending on the initiating event.

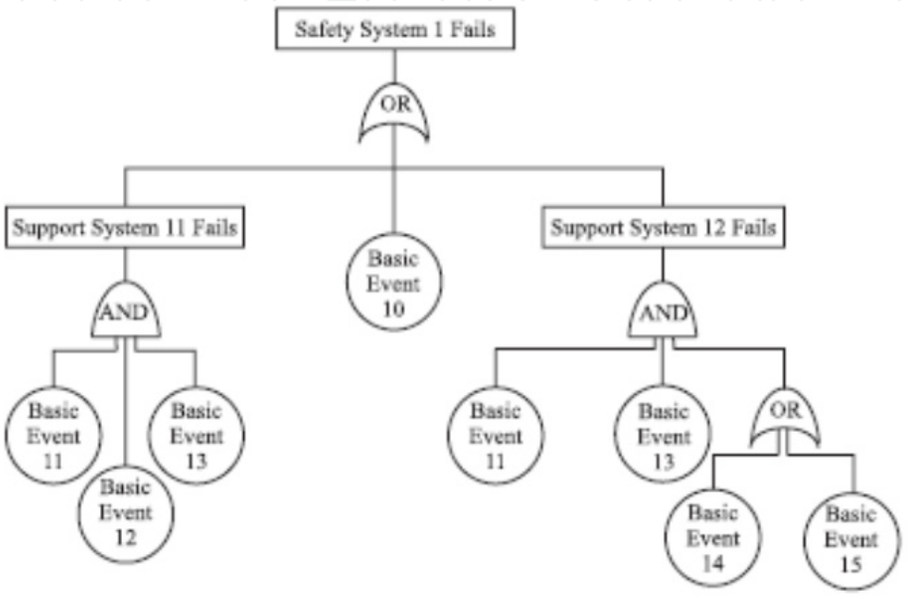

Figure 8. Example of a fault tree

A fault tree is capable to include rather special cases, usually identified in complex systems. These include system and components dependencies, called common cause failures (simultaneous failures of several components due to the same reason), area events (usually fire, flood etc., which damages groups of components in certain rooms), human actions (operator errors or mitigation actions).

The PSA is a powerful tool that can be used in many different ways to assess, understand and manage risk. Its primarily objectives are the following:

- estimate risk level of the facility,
- identify dominant event sequences affecting safety of the facility,
- identify systems, components and human actions important for safety,
- assess important dependencies (among systems or man-machine interactions),
- provide decision support in various application areas.

The growing area of PSA use is extensive support of probabilistic results in risk management and decision-making processes. The main areas of the PSA applications are assessment of design modifications and back-fitting, risk informed optimization of the Technical Specifications, accident management, emergency planning and others. Several

modern tools of risk management are also based on the PSA model, such as risk monitoring, precursor analysis and others.

Despite its popularity among the risk assessment tools, the PSA has a number of imitations and drawbacks. The main limitations of the PSA model are the following:

Binary representation of the component state. Only two states are analyzed: failed state or fully functioning state. However, this is not always realistic, as intermediate states are also possible. The same limitation exists for the redundant systems with certain success criteria - system is in failed state (success criteria is not satisfied) or in full power. The intermediate states for redundant systems are even more important.

Independence. In most cases, the components are assumed to be independent (except modelled by CCF), however there are many sources of dependencies, not treated by the model.

Aging effect. The aging effect is ignored because of the constant failure rate assumption. The only conservative possibility to treat the aging impact is to perform sensitivity study.

Time treatment. The FT/ET model is not capable to treat time explicitly during the accident progression. This is one of the major drawbacks of the methodology. In realistic systems, many parameters and functions depend on time and this is not encountered in the model and only approximate chronological order is assumed.

Uncertainty of the calculations. Uncertainties are inevitable in the PSA results and calculations and therefore direct treatment of the quantitative PSA estimates might be misleading. Due to the fact of uncertainties, the qualitative PSA results (identification of dominant accident sequences, comparison of different safety modifications) are of greater importance than quantitative.

4. Passive system unavailability model

The reliability of a passive system refers to the ability of the system to carry out a safety function under the prevailing conditions when required and addresses mainly the related performance stability.

In general the reliability of passive systems should be seen from two main aspects:

- systems/components reliability (e.g. piping, valves), as, for instance, the failure to start-up the system operation (e.g. drain valve failure to open)
- physical phenomena reliability, which addresses mainly the natural circulation stability, and the proneness of the system to the failure is dependent on the boundary conditions and the mechanisms needed for maintaining the intrinsic phenomena rather than on component malfunctions.

These two kinds of system malfunction are to to be considered as ET headings, to be assessed by specific FT components, as shown in figures 9 and 10.

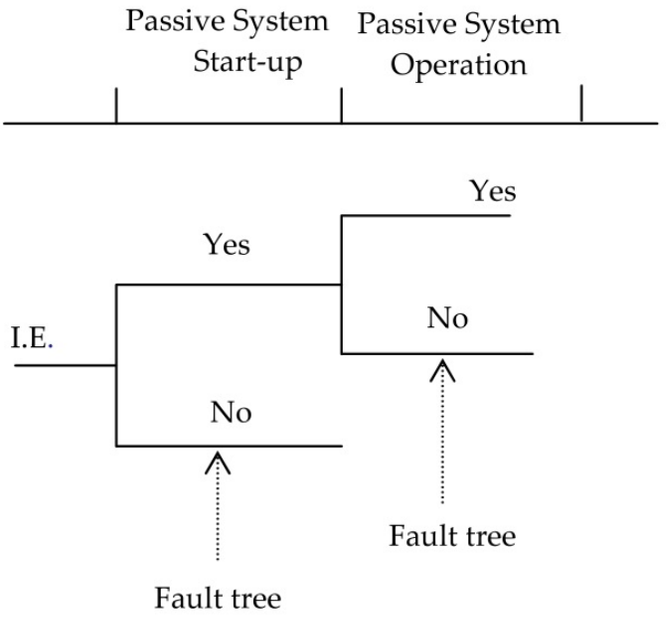

Figure 9. Event tree development

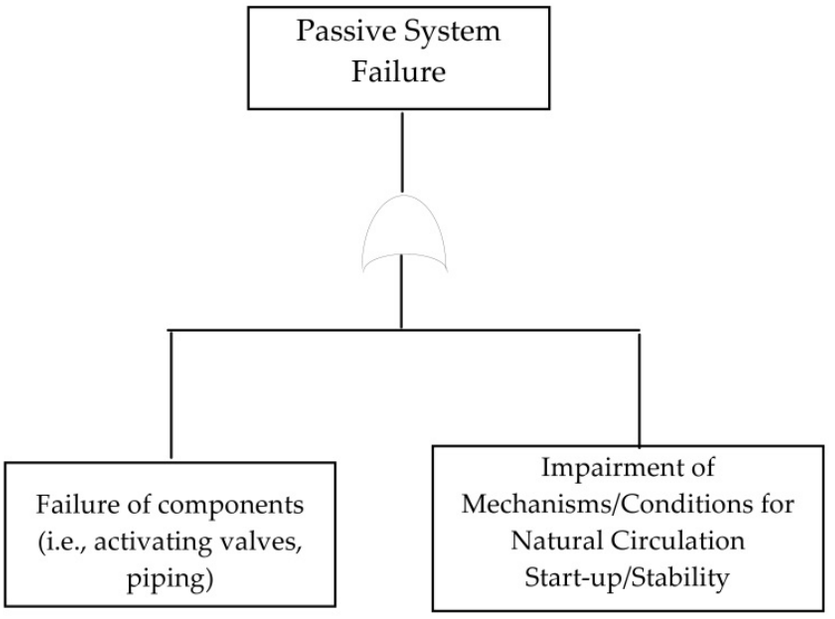

Figure 10. Fault tree model

The first facet calls for well-engineered safety components with at least the same level of reliability of the active ones.

The second aspect is concerned with the way the physical principle (gravity and density difference) operate and depends on the surrounding conditions related to accident development in terms of thermal hydraulic parameters evolution (i.e. characteristic parameters as flow rate and exchanged heat flux). This could require not a unique

unreliability figure, but the unreliability to be re evaluated for each sequence following an accident initiator, or at least for a small group of bounding accident sequences, enveloping the ones chosen upon similarity of accident progress and expected consequences: with this respect thermal hydraulic analysis of the accident is helpful to estimate the evolution of the parameters during the accident progress.

First step of the analysis is the identification of the failure modes affecting the natural circulation: for this scope two well structured commonly used qualitative hazard analysis, as Failure Mode and Effect Analysis (FMEA) and HAZard and OPerability analysis (HAZOP), specifically tailored on the topic, by considering the phenomenology typical of natural circulation, are adopted.

This analysis concerns both mechanical components (e.g. valve, piping, heat exchanger) of the system and the natural circulation itself, as "virtual" component and the system under investigation is the aforementioned Isolation Condenser.

FMEA is a bottom-up procedure conducted at component level by which each failure mode in a system is investigated in terms of failure causes, preventive actions on causes, consequences on the system, corrective/preventive actions to mitigate the effects on the system, while the HAZOP procedure considers any parameters characteristic of the system (among pressure, temperature, flow rate, heat exchanged through the HX, opening of the drain valve) and by applying a set of "guide" words, which imply a deviation from the nominal conditions as for instance undesired decrease or increase, determines the consequences of operating conditions outside the design intentions. FMEA and HAZOP analysis are shown in Table 1 and 2 respectively.

The analysis points out several factors leading to disturbances in the Isolation Condenser system; the list of these includes:

- Unexpected mechanical and thermal loads, challenging the primary boundary integrity
- HX plugging
- Mechanical component malfunction, i.e. drain valve
- Non-condensable gas build-up
- Heat exchange process reduction: surface oxidation, thermal stratification, piping layout, etc.

Finally a set of critical parameters direct indicators of the failure of the system is identified; these include:

- Non-condensable fraction
- Undetected leakage
- Valve closure area in the discharge line
- Heat loss
- Piping layout
- HX plugged pipes

Component	Failure Mode	Causes	Prev. Actions on Causes	Consequences	Corrective/Preventive Action on Consequences	Comment
System piping	Rupture	Material defects and aging; Corrosion; Abnormal operation conditions; Vibrations; Local. Stresses; Impact of heavy loads (missile)	Adequate welding process quality; Water chemistry control; In Service inspect; Design against missile generation	LOCA in the Drywell; Instantaneous loss of natural circulation; Emptying of the circuit; Loss of heat removal capability; Loss of reactor coolant inventory	Isolate the breached loop; Safety relief valves actuation; Automatic reactor depressurisation; Gravity Driven Cooling System actuation;	Includes both steam line and drain line Critical Parameter: Undetected Leakage
	Leak	Material defects and aging; Corrosion; Abnormal operation conditions; Vibrations; Local. stresses	Adequate welding process quality; Water chemistry control; In Service inspect.	Small LOCA in the Drywell; Slow emptying of the circuit and natural circulation arrest for long periods of operation; Reduced heat removal capability	Leak monitoring; Isolate the breached loop; Safety relief valves actuation	Critical Parameter: Undetected Leakage
Tube Bundle of the heat exchangers of the IC	Single pipe rupture	Wearing due to vibration and corrosion	Preventive maintenance; Water chemistry control; Leak monitoring	Release of primary water to the pool; Slow emptying of the circuit and natural circulation arrest for long periods of operation; Reduced heat removal capability	Flow monitoring; Isolate the breached loop; Safety relief valves actuation	Critical Parameter: Undetected Leakage
	Multiple pipe rupture	Wearing due to corrosion, vibration and pressure transient	Preventive maintenance; Water chemistry control; Leak monitoring	Release of primary water to the pool; Natural circulation stop; Emptying of the circuit; Loss of reactor coolant inventory; Loss of heat removal capability	Isolate the breached loop; Safety relief valves actuation; Automatic reactor depressurisation; Gravity Driven Cooling System actuation	Critical Parameter: Undetected Leakage
	Single pipe plugging	Crud in the cooling loop; Foreign object in the cooling loop	Water chemistry control; Yearly test of pipes flow; Preventive maintenance	No consequences		Critical Parameter: HX Plugged Pipes
Tube Bundle of the heat exchangers of the IC	Multiple pipe plugging	Violent pressure and vibration transient detaching large amount of crud from pipes walls.	Water chemistry control; Use of suitable materials for cooling loop pipes; Preventive maintenance	Natural circulation stop; Loss of heat removal capability; Reactor pressure and temperature increase	Safety relief valves actuation	Critical Parameter: HX Plugged Pipes

Component	Failure Mode	Causes	Prev. Actions on Causes	Consequences	Corrective/Preventive Action on Consequences	Comment
Drain valve on the return condensate line	Valve fails to open	Control circuit failure; Loss of electric power to motor; Electric motor failure	Redundancy of control devices; Signal to the operator; In Service inspect.	Non triggering of Isolation Condenser if bypass valve does not operate; Loss of heat removal capability; Reactor pressure and temperature increase	Reactor pressure and temperature control; Safety relief valves actuation; Realignment by the operator; Corrective maintenance	Critical Parameter: Partially Open Valve
	Inadvertent valve closing	Spurious signal; Control circuit failure; Human error	Redundancy of control devices; Signal to the operator; Procedured actions	Natural circulation stop in case bypass valve does not operate; Loss of heat removal capability; Reactor pressure and temperature increase	Reactor pressure and temperature control; Safety relief valves actuation; Realignment by the operator; Corrective maintenance	Critical Parameter: Partially Open Valve
Natural Circulation	Envelope failure	Material defects and aging; Corrosion; Abnormal operation conditions; Vibrations; Local. Stresses; Impact of heavy loads (missile)	Adequate welding process quality; Water chemistry control; In Service inspect; Design against missile generation	LOCA in the Drywell; Instantaneous loss of natural circulation; Emptying of the circuit; Loss of heat removal capability; Loss of reactor coolant inventory	Isolate the breached loop; Safety relief valves actuation; Automatic reactor depressurisation; Gravity Driven Cooling System actuation	Includes both steam line and drain line Critical Parameter: Undetected Leakage
	Cracking	Material defects and aging; Corrosion; Abnormal operation conditions; Vibrations; Local. stresses	Adequate welding process quality; Water chemistry control; In Service inspect.	Small LOCA in the Drywell; Slow emptying of the circuit and natural circulation arrest for long periods of operation; Reduced heat removal capability	Leak monitoring; Isolate the breached loop; Safety relief valves actuation	Critical Parameter: Undetected Leakage
	Modification of surface characteristics	Oxidation; Aerosol deposits	Water chemistry control	Reduction in heat exchange efficiency; Reduced heat removal capability	Flow monitoring	Critical Parameter: Oxide Layer
Natural Circulation	Thermal stratification	Temperature dishomogeneity; Density variations; Onset of local thermal hydraulic phenomena	Process control (pressure, flow, temperature)	Reduction of heat convection; Natural circulation blockage; Loss of heat removal capability; Reactor pressure and temperature increase	Flow monitoring; Reactor pressure and temperature control; Safety relief valves actuation	Critical Parameter: Piping Layout, Heat Loss

Component	Failure Mode	Causes	Prev. Actions on Causes	Consequences	Corrective/Preventive Action on Consequences	Comment
	Non condensable build-up	Onset of chemical phenomena; Radiolysis products; Impurities	Water chemistry control (PH, O2, H2)	Reduction in heat exchange efficiency; Reduction of heat convection; Natural circulation blockage; Loss of heat removal capability; Reactor pressure and temperature increase	Flow monitoring; Reactor pressure and temperature control; Purging through vent lines Safety relief valves actuation	Critical Parameter: Non-Condensable Fraction
	Heat dissipation	Thermal insulation degradation; Inaccurate material assembly	In Service inspect.	Reduction of heat convection; Natural circulation impairment	Flow monitoring;	Critical Parameter: Heat Loss

Table 1. FMEA Table for the Isolation Condenser System

PARAMETER: Flow rate					
Guide Word	Deviation	Possible Causes	Consequences	Safeguards/Interlocks	Actions Required
More of[1]	High Flow	N/A			
Less of	Low Flow	Modifications of surface characteristics (crud deposition, oxidation); Non-condensable build-up; Thermal stratification; Pipe partial plugging; Pipe leak; HX single pipe plugging; HX single pipe rupture Drain valve partial opening	Natural circulation degradation and reduced heat transfer capability; T and P increase	Safety relief valve actuation; Vent line valve actuation	Corrective maintenance; Operator action
No/None	No Flow	Non-condensable build-up; Thermal stratification; Pipe plugging; Pipe rupture; HX Multiple pipe plugging; HX Multiple pipe rupture; Drain valve closed	Natural circulation stop and loss of heat transfer capability; T and P increase	Safety relief valve actuation; Vent line valve actuation; Automatic Depressurisation System actuation; Gravity Driven Cooling System actuation	Corrective maintenance; Operator action
PARAMETER: Pressure					
Guide Word	Deviation	Possible Causes	Consequences	Safeguards/Interlocks	Actions Required
More of	High Pressure	Non-condensable build-up; Surface modifications (crud, oxidation); HX tube plugging; HX tube rupture Partial valve opening	Natural circulation degradation and reduced heat transfer capability; T increase	Safety relief valve actuation; Vent line valve actuation	Corrective maintenance; Operator action
Less of[1]	Low Pressure	N/A			
No/None	No Pressure	N/A			

PARAMETER: Drain valve opening					
Guide Word	Deviation	Possible Causes	Consequences	Safeguards/Interlocks	Actions Required
More of	N/A				
Less of	Reduced Opening	Partial blockage	Natural circulation degradation and reduced heat transfer capability; T and P increase	Safety relief valve actuation;	Corrective maintenance; Operator action
No/None	No Opening	Loss of electrical power; Circuit control failure; Electrical motor failure; Valve stuck	Natural circulation stop and loss of heat transfer capability; T and P increase	Safety relief valve actuation; Vent line valve actuation; Automatic Depressurisation System actuation; Gravity Driven Cooling System actuation	Corrective maintenance; Operator action
PARAMETER: Exchanged heat flux					
Guide Word	Deviation	Possible Causes	Consequences	Safeguards/Interlocks	Actions Required
More of[1]	High flux	N/A			
Less of	Low Flux	Non-condensable build-up; Surface modifications (crud, oxidation); HX single tube plugging; HX single tube rupture	Natural circulation degradation and reduced heat transfer capability; T and P increase	Safety relief valve actuation; Vent line valve actuation	Corrective maintenance; Operator action
No/None	No Flux	Non-condensable build-up; HX multiple tube plugging; HX multiple tube rupture	Natural circulation stop and loss of heat transfer capability; T and P increase	Safety relief valve actuation; Vent line valve actuation; Automatic Depressurisation System actuation; Gravity Driven Cooling System actuation	Corrective maintenance; Operator action

[1] This deviation is not evaluated, even if it implies an overcooling of the system that could potentially induce to thermal stresses on core structures and reactor components, like the heat exchanger.

Table 2. HAZOP Table for the Isolation Condenser System

Each of these failure mode driving parameters is examined to determine the expected failure probability by defining the range and the probability distribution function pertaining to the parameter. These failure characteristics are then used to develop a probabilistic model to predict the natural circulation failure.

As stated before FT technique seems to be the most suitable mean to quantify the passive system unavailability, once introduced the failure modes in the form of critical parameters elementary basic events, linked following the Boolean algebra rules (AND et OR), or in the form of sub-fault trees. However 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 fact, since the failure of the physical process is addressed, the conventional failure model associated with the basic events (i.e. exponential, $e^{-\lambda t}$, λ failure rate, t mission time), commonly used for component failure model, is not applicable: each pertinent basic event will be characterized by defined parameters driving the failure mechanisms - e.g. non-

condensable fraction, leak rate, partial opening of the isolation valve, heat exchanger plugged pipes, etc. - and the associated failure criterion. Thus each basic event model pertaining to the relevant failure mode requires the assignment of both the probability distribution and range of the correspondent parameter and the definition of the critical interval defining the failure (for example failure for non-condensable fraction >x%, leak rate > x gr./sec or crack size > x cm^2 and so on).In order to evaluate the overall probability of failure of the system, the single failure probabilities are combined according to:

$$Pe_t = 1.0 - ((1.0 - Pe_1)*(1.0 - Pe_2)*...*(1.0 - Pe_n)) \quad (1)$$

where:
Pe_t overall probability of failure
Pe_1 through Pe_n individual probabilities of failure pertaining to each failure mode, assuming mutually non-exclusive independent events
The failure model relative to each single basic event is given by:

$$Pe_i = \int p_i(x)\, dx \quad x>x_o \quad (2)$$

$p_i(x)$probability distribution function of the parameter x
$x_o$threshold value according to the failure criterion

It's worth noting that the assumed failure criterion, based on the failure threshold for each path, implies the neglecting of the "intermediate" modes of operation of the system or equivalently the degraded performance of the system (up to the failure point): this gives credit for a passive system that "partially works" and has failed for its intended function but provides some operation. This operation could be sufficient to prolong the window for opportunity to recover a failed system, for instance through redundancy configuration, and ultimately prevent or arrest core degradation.

Once the probabilistic distributions of the parameters are assigned, the reliability of the system can be directly obtained from (1) once a failure criterion is assigned and the single failure probabilities are evaluated through (2): this point is being satisfied by assigning both the range and the probability distributions, basing on expert judgment and engineering assessment. In fact, as further illustrated, difficulties arise in assigning both the range and the probability density functions relative to the critical parameters defining the failure modes, in addition to the definition of a proper failure criterion, because of the lack of operational experience and data.

5. Methodologies characterization and comparative assessment

A very good description of the various methodologies proposed so far and currently available in the open literature is given in [5].

The earliest significant effort to quantify the reliability of such systems is represented by a methodology known as REPAS (Reliability Evaluation of Passive Systems), [6], which has been developed in late 1990s, cooperatively by ENEA, the University of Pisa, the Polytechnic

of Milan and the University of Rome, that was later incorporated in the EU (European Union) RMPS (Reliability Methods for Passive Systems) project. 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.

The RMPS methodology, described in [7], was developed to address the following problems: 1) Identification and quantification of the sources of uncertainties and determination of the important variables, 2) Propagation of the uncertainties through thermal-hydraulic (T-H) models and assessment of passive system unreliability and 3) Introduction of passive system unreliability in accident sequence analyses. In this approach, the passive system is modelled by a qualified T-H code (e.g. CATHARE, RELAP) and the reliability evaluation is based on results of code runs, whose inputs are sampled by Monte-Carlo (M-C) simulation. This approach provides realistic assessment of the passive system reliability, thanks to the flexibility of the M-C simulation, which adapts to T-H model complexity without resort to simplifying approximation. In order to limit the number of T-H code runs required by M-C simulation, alternative methods have been proposed such as variance reduction techniques, first and second order reliability methods and response surface methods. The RMPS methodology has been successfully applied to passive systems utilizing natural circulation in different types of reactors (BWR, PWR, and VVER). A complete example of application concerning the passive residual heat removal system of a CAREM reactor is presented in [8]. The RMPS methodology tackles also an important problem, which is the integration of passive system reliability in a PSA study. So far, in existing innovative nuclear reactor projects PSA's, only passive system components failure probabilities are taken into account, disregarding the physical phenomena on which the system is based, such as the natural circulation. The first attempts performed within the framework of RMPS have taken into account the failures of the components of the passive system as well as the impairment of the physical process involved like basic events in static event tree as exposed in [7]. Two other steps have been identified after the development of the RMPS methodology where an improvement was desirable: the inclusion of a formal expert judgment (EJ) protocol to estimate distributions for parameters whose values are either sparse on not available, and the use of efficient sensitivity analysis techniques to estimate the impact of changes in the input parameter distributions on the reliability estimates.

R&D in the United States on the reliability of passive safety systems has not been as active at least until mid 2000. A few published papers from the Massachusetts Institute of Technology (MIT) have demonstrated their development of approaches to the issue. Their technique has examined TH uncertainties in passive cooling systems for Generation IV-type gas-cooled reactors. The MIT research on the reliability of passive safety systems has taken a similar approach but has focused on a different set of reactor technologies. Their research has examined thermal hydraulic uncertainties in passive cooling systems for Generation IV gas-cooled reactors, as described in [9,10]. Instead of post-design probabilistic risk analysis

for regulatory purposes, the MIT research seeks to leverage the capabilities of probabilistic risk assessment (PRA) to improve the design of the reactor systems early in their development life cycle.

In addition to the RMPS approach, a number of alternative methodologies have been investigated for the reliability assessment of T-H passive systems.

Three different methodologies have been proposed by ENEA (Italian National Agency for New Technologies, Energy and Sustainable Economic Development). In the first methodology [11], the failure probability is evaluated as the probability of occurrence of different independent failure modes, a priori identified as leading to the violation of the boundary conditions or physical mechanisms needed for successful passive system operation.

This approach based on independent failure modes introduces a high level of conservatism as it appears that the probability of failure of the system is relevantly high, because of the combination of various modes of failure as in a series system, where a single fault is sufficient to challenge the system performance. The correspondent value of probability of failure can be conservatively assumed as the upper bound for the unavailability of the system, within a sort of "parts-count" reliability estimation.

In the second, [12], modelling of the passive system is simplified by linking to the modelling of the unreliability of the hardware components of the system: this is achieved by identifying the hardware failures that degrade the natural mechanisms upon which the passive system relies and associating the unreliability of the components designed to assure the best conditions for passive function performance.

Thus, the probabilities of degraded physical mechanisms are reduced to unreliability figures of the components whose failures challenge the successful passive system operation. If, on the one hand, this approach may in theory represent a viable way to address the matter, on the other hand, some critical issues arise with respect to the effectiveness and completeness of the performance assessment over the entire range of possible failure modes that the system may potentially undergo and their association to corresponding hardware failures. In this simplified methodology, degradation of the natural circulation process is always related to failures of active and passive components, not acknowledging, for instance, any possibility of failure just because of unfavourable initial or boundary conditions. In addition, the fault tree model adopted to represent the physical process decomposition is used as a surrogate model to replace the complex T-H code that models the system behaviour. This decomposition is not appropriate to predict interactions among physical phenomena and makes it extremely difficult to realistically assess the impact of parametric uncertainty on the performance of the system.

The third approach is based on the concept of functional failure, within the reliability physics framework of load-capacity exceedance [7,13,14]. 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 pdfs according to defined safety criteria. The main drawback in the last method devised by ENEA lies in the selection and definition of the probability distributions that describe the characteristic parameters, based mainly on subjective/engineering judgment.

Every one of three methods devised by ENEA shares with the main RMPS approach the issue related to the uncertainties affecting the system performance assessment process. With respect to the RMPS a greater simplicity is introduced, although detrimental to the relevance of the approaches themselves: this is particularly relevant as far as the approach based on hardware components failure is concerned.

Finally a different approach is followed in the APSRA (Assessment of Passive System ReliAbility) methodology developed by BARC (Bhabha Atomic Research Centre, India), see [15]. In this approach, a failure surface is generated by considering the deviation of all those critical parameters, which influence the system performance. Then, the causes of deviation of these parameters are found through root diagnosis. It is attributed that the deviation of such physical parameters occurs only due to a failure of mechanical components such as valves, control systems, etc. Then, the probability of failure of a system is evaluated from the failure probability of these mechanical components through classical PSA treatment. Moreover, to reduce the uncertainty in code predictions, BARC foresee to use in-house experimental data from integral facilities as well as separate.

With reference to the two most relevant methodologies (i.e. RMPS and APSRA), the RMPS consists mainly in the identification and quantification of parameter uncertainties in the form of probability distributions, to be propagated directly into a T-H code or indirectly in using a response surface; the APSRA methodology strives to assess not the uncertainty of parameters but the causes of deviation from nominal conditions, which can be in the failure of active or passive components or systems.

As a result, different approaches are used in the RMPS and APSRA methodologies. RMPS proposes to take into account, in the PSA model, the failure of a physical process. This problem is treated in using a best estimate T-H code plus uncertainty approach. APSRA includes in the PSA model the failure of those components which cause a deviation of the key parameters resulting in a system failure, but does not take into account possible uncertainties on these key parameters. As the consequence, the T-H code is used in RMPS to propagate the uncertainties and in APSRA to build a failure surface. APSRA incorporates an important effort on qualification of the model and use of the available experimental data. These aspects have not been studied in the RMPS, given the context of the RMPS project.

The following Table attempts to identify the main characteristics of the methodologies proposed so far, with respect to some aspects, such as the development of deterministic and probabilistic approaches, the use of deterministic models to evaluate the system performance, the identification of the sources of uncertainties and the application of expert judgment.

Methodology	Probabilistic vs. deterministic	Deterministic Analysis	Uncertainties	Expert Judgment/Experimental data
REPAS/RMPS	Merge of probabilistic and thermal hydraulic aspects	T-H code adopted for uncertainty propagation	Uncertainties in parameters modelled by probability density functions	EJ adopted to a large extent; Statistical analysis when experimental data exist
APSRA	Merge of probabilistic and thermal hydraulic aspects	T-H code adopted to build the failure surface	parameters' deviations from nominal conditions caused by failure of active or passive components (root diagnosis)	Experimental data usage; EJ for root diagnosis
ENEA approaches	Only probabilistic aspects		Uncertainties in parameters	EJ adopted to a large extent (except the approach based on hardware failure)

Table 3. Main features of the various approaches

6. Open issues

From the exam of the various methodologies, which have been developed over these most recent years within the community of the safety research, and are currently available in the open literature, the following open questions are highlighted and consequently needs for research in all related areas are pointed out :

- The aspects relative to the assessment of the uncertainties related to passive system performance: they regard both the best estimate T-H codes used for their evaluation and system reliability assessment itself;
- The dependencies among the parameters, mostly T-H parameters, playing a key role in the whole process assessment.
- The integration of the passive systems within an accident sequence in combination with active systems and human actions.
- The consideration for the physical process and involved physical quantities dependence upon time, implying, for instance, the development of dynamic event tree to incorporate the interactions between the physical parameter evolution and the state of the system and/or the transition of the system from one state to another.

It's worth noticing that these two last aspects are correlated, but hey will be treated separately.

- The comparison between active and passive systems, mainly on a functional viewpoint.

All of these points are elaborated in the following, in an attempt to cover the entire spectrum of issues related to the topic, and capture all the relevant aspects to concentrate on and devote resources towards for fulfilling a significant advance.

6.1. Uncertainties

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, as recognized in [7].

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 modelled 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 modelled. 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.

For instance, as initial step, the approach described in [16]. allows identifying the uncertainties pertaining to passive system operation in terms of critical parameters driving the modes of failure, as, for instance, the presence of non-condensable gas, thermal stratification and so on. In this context the critical parameters are recognized as epistemic uncertainties.

The same reference points 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.

A further step of the matter can be found in[11], which attempts to assign sound distributions to the critical parameters, to further develop a probabilistic model. 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. 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 on failure locations and modes and finally the selection of the parameters affecting the system performance.

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.

A clear prospect of the uncertainties as shown in Table 4 [5].

As emphasized 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, as reported in [17], which outlines the main aspects of the REPAS procedure.

Aleatory
Geometrical properties
Material properties
Initial/boundary conditions (design parameters)
Epistemic
T-H analysis
Model (correlations)
Parameters
System failure analysis
Failure criteria
Failure modes (critical parameters)

Table 4. Categories of uncertainties associated with T-H passive systems reliability assessment

In ref. [17], in order to simplify both the identification of the ranges and their corresponding probabilities, initially discrete values have been selected. As a general rule, a central pivot has been identified, and then the range has been extended to higher and lower values, if applicable. The pivot value represents the nominal condition for the parameter. The limits have been chosen in order to exclude unrealistic values or those values representing a limit zone for the operation demand of the passive system. Once the discrete ranges have been set up, discrete probability distributions have been associated, to represent the probabilities of occurrence of the values. As in the previous step, the general rule adopted is that the higher probability of occurrence corresponds to the nominal value for the parameter. Then lower probabilities have been assigned to the other values, as much low the probability as much wide the distance from the nominal value, as in a sort of Gaussian distribution.

Ultimately, as underlined in the previous section, the methodologies proposed in RMPS and within the studies conducted by MIT address the question by propagating the parameter and model uncertainties, by performing Monte Carlo simulations on the detailed T-H model based on a mechanistic code, and calculating the distribution of the safety variable and thus the probability of observing a value above the defined limit, according to the safety criterion.

6.2. Dependencies

Alike some other types of analyses for nuclear power plants, the documented experience with PSS reliability seems to focus on the analysis of one passive attribute at a time. In many

cases, this may be sufficient, but for some advanced designs with multiple passive features, modelling of the synergistic effects among them is important. For example, modelling of a passive core cooling system may require simultaneous modelling of the amount of non condensable gases which build up along the circuit during extended periods of operation, the potential for stratification in the cooling pool, and interactions between the passive core cooling system and the core. Analysis of each of these aspects independently may not fully capture the important boundary conditions of each system. For instance, with regard to the aforementioned methodologies, the basic simplifying assumption of independence among system performance relevant parameters, as the degradation measures, means that the correlation among the critical parameter distributions is zero or is very low to be judged significant, so that the assessment of the failure probability is quite straightforward. If parameters have contributors to their uncertainty in common, the respective states of knowledge are dependent. As a consequence of this dependence, parameter values cannot be combined freely and independently. Instances of such limitations need to be identified and the dependencies need to be quantified. If the analyst knows of dependencies between parameters explicitly, multivariate distributions or conditional subjective pdfs (probability density functions) may be used. The dependence between the parameters can be also introduced by covariance matrices or by functional relations between the parameters.

As observed in [15], both REPAS and RMPS approaches adopt a probability density function (pdf) to treat variations of the critical parameters considered in the predictions of codes. To apply the methodology, one needs to have the pdf values of these parameters. However, it is difficult to assign accurate pdf treatment of these parameters, which ultimately define the functional failure, due to the scarcity of available data, both on an experimental and operational ground. Moreover, these parameters are not really independent ones to have deviation of their own. Rather deviations of them from their nominal conditions occur due to failure/malfunctioning of other components or as a result of the combination with different concomitant mechanisms. Thus the hypothesis of independence among the failure driving parameters appears non proper.

With reference to the functional reliability approach set forth in [13], the selected representative parameters defining the system performance, for instance coolant flow or exchanged thermal power, are properly modelled through the construction of joint probability functions in order to assess the correspondent functional reliability. A recent study shows how the assumption of independence between the marginal distributions to construct the joint probability distributions to evaluate system reliability adds conservatism to the analysis, [18]: for this reason the model is implemented to incorporate the correlations between the parameters, in the form of bivariate normal probability distributions. That study has the merit to highlight the dependence among the parameters underlying the system performance: further studies are underway, with regard, for instance to the approach based on independent failure modes. As described in the previous section 2, this approach begins by identifying critical parameters, properly modelled through probability functions, as input to basic events, corresponding to the failure modes, arranged in a series system configuration, assuming non-mutually exclusive independent events. It introduces a

high level of conservatism as it appears that the probability of failure of the system is relevantly high to be considered acceptable, because of the combination of various modes of failure, where a single fault is sufficient to challenge the system performance. Initial evaluations, [19], reveal that the critical parameters are not suitable to be chosen independently of each other, mainly because of the expected synergism between the different phenomena under investigation, with the potential to jeopardize the system performance. This conclusion allows the implementation of the proposed methodology, by properly capturing the interaction between various failure modes, through modelling system performance under multiple degradation measures. It was verified that when the multiple degradation measures in a system are correlated, an incorrect independence assumption may overestimate the system reliability, according to a recent study, [20].

6.3. Incorporation of passive system within probabilistic safety assessment

PSA has been introduced for the evaluation of design and safety in the development of those reactors. A technology-neutral framework, that adopts PSA information as a major evaluation tool, has been proposed as the framework for the evaluation of safety or regulation for those reactors [21,22]. To utilize this framework, the evaluation of the reliability of Passive Systems has been recognized as an essential part of PSA.

In PSA, the status of individual systems such as a passive system is assessed by an accident sequence analysis to identify the integrated behaviour 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. This gives credit for a passive system that “partially works” and has failed for its intended function but provides some operation: this operation could be sufficient to prolong the window for opportunity to recover a failed system, for instance through redundancy configuration, and ultimately prevent or arrest core degradation [19]. This means that the status of a passive system can be divided into several states, and each status is affected by the integrated behaviour of the reactor, because its individual performance is closely related with the accident evolution and whole plant behaviour.

Ref. [23] lays the foundations to outline a general approach for the integration of a passive system, in the form of a front line system and in combination with active ones and/or human actions, within a PSA framework.

In [7] a consistent approach, based on an event tree representation, has been developed to incorporate in a PSA study the results of reliability analyses of passive systems obtained on specific accident sequences. In this approach, the accident sequences are analyzed by taking into account the success or the failure of the components and of the physical process involved in the passive systems. This methodology allows the probabilistic evaluation of the

influence of a passive system on a definite accident scenario and could be used to test the advantage of replacing an active system by a passive system in specific situations.

However in order to generalize the methodology, it is important to take into account the dynamic aspects differently than by their alone modelling into the T-H code. Indeed in complex situations where several safety systems are competing and where the human operation cannot be completely eliminated, this modelling should prove to be impossible or too expensive in computing times. It is thus interesting to explore other solutions already used in the dynamic PSA, like the method of the dynamic event trees, in order to capture the interaction between the process parameters and the system state within the dynamical evolution of the accident.

In the PSA of nuclear power plants (NPPs), accident scenarios, which are dynamic in nature, are usually analyzed with event trees and fault trees.

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 modelling the interactions between the physical evolution of the process variables (temperatures, pressures, mass flows, etc.,) and the behaviour 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 [24].

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. On the contrary, 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 onerous and complex.

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.

Merging probabilistic models with T-H models, i.e. dynamic reliability, is required to accomplish the evaluation process of T-H passive systems in a consistent manner: this is

particularly relevant with regard to the introduction of a passive system in an accident sequence, since the required mission could be longer than 24 h as usual level 1 PSA mission time. In fact for design basis accidents, the passive systems are required to establish and maintain core cooling and containment integrity, with no operator intervention or requirement for a.c. power for 72 h, as a grace time [25].

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.

A preliminary attempt in addressing the dynamic aspect of the system performance in the frame of passive system reliability is shown in [26], which introduces the T-H passive system as a non-stationary stochastic process, where the natural circulation is modeled in terms of time-variant performance parameters, (as for instance mass flow-rate and thermal power, to cite any) assumed as stochastic variables. In that work, the statistics associated with the stochastic variables change in time (in terms of associated mean values and standard deviations increase or decrease, for instance), so that the random variables have different values in every realization, and hence every realization is different.

6.4. Comparative assessment between active and passive systems

The design and development of future water-cooled reactors address the use of passive safety systems, i.e. those characterized by no or very limited reliance on external input (forces, power or signal, or human action) and whose operation takes advantage of natural forces, such as free convection and gravity, to fulfil the required safety function and to provide confidence in the plant's ability to handle transients and accidents. Therefore, they are required to accomplish their mission with a sufficient reliability margin that makes them attractive as an important means of achieving both simplification and cost reduction for future plants while assuring safety requirements with lesser dependence of the safety function on active components like pumps and diesel generators.

On the other hand, since the magnitude of the natural forces, which drive the operation of passive systems, is relatively small, counter-forces (e.g. friction) can be of comparable magnitude and cannot be ignored as is generally the case with pumped systems. This concern leads to the consideration that, despite the fact that passive systems "should be" or, at least, are considered, more reliable than active ones - because of the smaller unavailability due to hardware failure and human error - there is always a nonzero likelihood of the occurrence of physical phenomena leading to pertinent failure modes, once the system enters into operation.

These characteristics of a 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 [27].

Here are some of the benefits and disadvantages of the passive systems that should be evaluated vs. the correspondent active system.

- Advantages
- No external power supply: no loss of power accident has to be considered.
- No human factor, implying no inclusion of the operator error in the analysis.
- Better impact on public acceptance, due to the presence of "natural forces".
- Less complex system than active and therefore economic competitiveness.
- Passive systems must be designed with consideration for ease of ISI, testing and maintenance so that the dose to the worker is much less.
- Drawbacks
- Reliance on "low driving forces", as a source of uncertainty, and therefore need for T-H uncertainties modeling.
- 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.
- Need for operational tests, so that dependence upon human factor can not be 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
- Reliability and performance assessment in any case. 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 make nuclear power more competitive, from potential annual maintenance cost reductions to safety system response.

7. Final remarks

Based on the analysis of the critical aspects related to the open points discussed in the previous section a qualitative analysis, on the basis of the author's opinion, reported in

Table 5 below aims at identifying for each of the above items both the criticality with respect to the passive system reliability assessment process, in terms of the relative importance and the existing advancement, according to Table 6 which ranks the relative level of both the importance and progress.

Item	Importance	Advance
Uncertainties	H	L
Dependencies	M	L
Integration within PSA	M	L
Passive vs. Active	H	L

Table 5. Importance analysis

	Grade	Definition
Importance	H	The item is expected to have a significant impact on the system failure
	M	The item is expected to have a moderate impact on the system failure
	L	The item is expected to have only a small impact on the system failure
Advance	H	The issue is modelled in a detailed way with adequate validation
	M	The issue is represented by simple modelling based on experimental observations or results.
	L	The issue is not represented in the analysis or the models are too complex or inappropriate which indicates that the calculation results will have a high degree of ambiguity

Table 6. Grade rank for importance and advancement analysis

It is clear that he worst case is characterized by "high "and "low" rankings relative respectively to the importance and the advancement aspects, thus making the correspondent item development a critical challenge.

Based on this, the results of this qualitative analysis show the relevance relative to the uncertainties and the comparison between active and passive, as most critical points to be addressed in the application of the PRA to the evaluation of the passive system performance assessment. This allows the analyst to track a viable R&D program to deal with these issues and limitations and to steer the relative efforts towards their implementation.

8. Conclusions

Due to the specificities of passive systems that utilize natural circulation (small driving force, large uncertainties in their performance, lack of data…), there is a strong need for the development and demonstration of consistent methodologies and approaches for evaluating

their reliability. This is a crucial issue to be resolved for their extensive use in future nuclear power plants. Recently, the development of procedures suitable for establishing the performance of a passive system has been proposed: the unavailability of reference data makes troublesome the qualification of the achieved results. These procedures can be applied for evaluating the acceptability of a passive system, specifically when nuclear reactor safety considerations are important for comparing two different systems having the same mission and, with additional investigation, for evaluating the performance of an active and passive system on a common basis. The study while identifying limitations of the achieved results or specific significant aspects that have been overlooked has suggested areas for further development or improvements of the procedures:

- In order to get confidence in the achieved results, the reduction of the so identified level of uncertainty pertaining to the passive system behaviour, and regarding in particular the phenomenological uncertainty. In fact, it's worth noting that these uncertainties are mainly related to the state of knowledge about the studied object/phenomenon, i.e., they fall within the class of epistemic uncertainties, thus suitable for reduction by gathering and analyzing a relevant quantity of information and data.
- The determination of the dependencies among the relevant parameters adopted to analyze the system reliability.
- The study of the dynamical aspects of the system performance, because the inherent dynamic behaviour of the system to be characterized: this translates into the development of the dynamic event tree.
- The comparison against the active system, also to evaluate the economical competitiveness, while assuring the same level of safety.

Future research in nuclear safety addressing this specific topic relevant to advanced reactors should be steered towards all these points in order to foster and add credit to any proposed approach to address the issue and to facilitate the proposed methods endorsement by the scientific and technical community.

Author details

Luciano Burgazzi
Reactor Safety and Fuel Cycle Methods Technical Unit, ENEA, Italian National Agency for New Technologies, Energy and Sustainable Economic Development, Bologna, Italy

9. References

[1] IAEA TEC-DOC-626, 1991. Safety Related Terms for Advanced Nuclear Power Plants. September 1991.
[2] IAEA TEC DOC-1474, 2005. Natural Circulation in Water Cooled Nuclear power Plants. *Phenomena, models, and methodology for system reliability assessments*, November 2005.
[3] IAEA TECDOC-1624, 2009. Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants. November 2009

[4] United States Nuclear Regulatory Commission's (U.S. NRC) Reactor Safety Study (WASH-1400, 1975).
[5] Zio, E., Pedroni, N., 2009. Building Confidence in the Reliability Assessment of Thermal hydraulic Passive Systems. Reliability Engineering and System Safety, 94, 268-281.
[6] Jafari, J., D'Auria F., et al., 2003. Reliability Evaluation of a Natural Circulation System. Nuclear Engineering and Design 224, 79–104.
[7] Marques, M., 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.
[8] Lorenzo G., et al., Assessment of an Isolation Condenser of an Integral Reactor in View of Uncertainties in Engineering Parameters, Science and technology of Nuclear Installations, Volume 2011, Article ID 827354, 9 pages
[9] Apostolakis G., Pagani L. and Hejzlar, P., 2005. The Impact of Uncertainties on the Performance of Passive Systems. Nuclear Technology 149, 129–140
[10] Apostolakis G., Mackay F., and. Hejzlar P, 2008. Incorporating Reliability Analysis into the Design of Passive Cooling System with an Application to a Gas-Cooled Reactor. Nuclear Engineering & Design 238, 217-228
[11] Burgazzi, L., 2007a. Addressing the Uncertainties related to Passive System Reliability. Progress in Nuclear Energy 49, 93-102.
[12] Burgazzi, L., 2002. Passive System Reliability Analysis: a Study on the Isolation Condenser, Nuclear Technology 139, 3-9.
[13] Burgazzi, L., 2003. Reliability Evaluation of Passive Systems through Functional Reliability Assessment, Nuclear Technology 144, 145-151.
[14] Burgazzi, L. 2007b. Thermal-hydraulic Passive System reliability-based design approach, Reliability Engineering and System Safety 92 (9), 1250-1257.
[15] Nayak, A.K., et al., 2008. Passive System Reliability Analysis using the APSRA Methodology. Nuclear Engineering and Design 238, 1430-1440.
[16] Burgazzi, L., 2004. Evaluation of Uncertainties related to Passive Systems Performance. Nuclear Engineering and Design 230, 93-106.
[17] Ricotti M.E., Zio E., D'Auria F., Caruso G., 2002. Reliability Methods for Passive Systems (RMPS) Study – Strategy and Results, in proceedings of the NEA CSNI/WGRISK Workshop on Passive System Reliability. A Challenge to Reliability Engineering and Licensing of Advanced Nuclear Power Plants, 146-163
[18] Burgazzi, L., 2008a. Reliability Prediction of Passive Systems based on Bivariate Probability Distributions, Nuclear Technology 161, 1-7.
[19] Burgazzi, L., 2009. Evaluation of the Dependencies related to Passive System Failure. Nuclear Engineering and Design 239, 3048-3053
[20] Burgazzi, L., 2011. Reliability Prediction of Passive Systems with Multiple Degradation Measures, Nuclear Technology 173, 153-161.
[21] USNRC, 2007. Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing. US Nuclear Regulatory Commission, NUREG-1860.
[22] IAEA, 2007. Proposal for a technology-neutral safety approach for new designs. International Atomic Energy Agency, TECDOC-1570, Vienna.

[23] Burgazzi, L., 2008b. Incorporation of Passive Systems within a PRA Framework. Proceedings of PSAM9, 9th International Probabilistic, Safety Assessment and Management Conference, Hong Kong, 18-23 May 2008.
[24] 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
[25] Matzie, R. A. and Worrally, A., The AP1000 reactor—the Nuclear Renaissance Option. Nuclear Energy, 2004, 43, No. 1, Feb., 33–45
[26] Burgazzi, L., 2008c. About Time-variant Reliability Analysis with Reference to Passive Systems Assessment. Reliability Engineering and System Safety 93, 1682-1688.
[27] JiYong Oh and Golay, M., 2008. 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.