Titolo

Valutazione della risposta di sistemi attivi e passivi a fronte di sequenze incidentali rilevanti ai fini della sicurezza

Descrittori

Tipologia del documento: **Rapporto Tecnico**

Collocazione contrattuale: Accordo di programma ENEA-MSE: Piano Annuale di Realizzazione 2011, Linea Progettuale 2: Studi di Sicurezza sugli impianti nucleari

Argomenti trattati:
Sicurezza nucleare
Analisi incidentale
Analisi di sicurezza probabilistica

Sommario

Il presente documento riporta le attività svolte nell'ambito della Linea Progettuale 2 (LP2), obiettivo B2 (Studi di Sicurezza sugli impianti nucleari) del PAR 2011, ADP ENEA-MSE.
Lo studio illustra il confronto della risposta dei sistemi di sicurezza attivi e passivi a fronte di sequenze incidentali gravi che possono portare ad incidenti severi.
In particolare sistemi di sicurezza attivi e passivi che svolgono la stessa funzione di smaltimento del calore residuo, vengono analizzati e comparati in termini di prestazioni ed affidabilità; viene inoltre effettuato il confronto tra le conseguenze provocate da uno stesso set di eventi iniziatori per un reattore basato su sistemi di sicurezza attivi ed uno basato su quelli passivi.

Note

Questo documento è stato preparato col contributo congiunto del seguente personale di ricerca ENEA e CIRTEN:

- L. Burgazzi, N. Davidovich, M. Sangiorgi, P. Turroni, N. Voukelatou (ENEA)
- F. Giannetti, L. Ferroni, T. Murgia, A. Naviglio (Università di Roma "La Sapienza")

Sigla doc. rif.: CIRTEN-Università di Roma "La Sapienza": *CERSE-UNIRM RL 1182/2011*

REV.	DESCRIZIONE	DATA		REDAZIONE	CONVALIDA	APPROVAZIONE
2			NOME			
			FIRMA			
1			NOME			
			FIRMA			
0	EMISSIONE	31/08/2012	NOME	L. Burgazzi	F. De Rosa	P. Meloni
			FIRMA			

Sommario

Obiettivo principale del presente studio è la valutazione comparativa della risposta dei sistemi di sicurezza attivi e passivi in condizioni di incidente estreme, come il transitorio di station blackout, come emerge dalla analisi dell'incidente di Fukushima-Daiichi. Particolare enfasi è posta sui sistemi passivi termoidraulici, che si basano sulla circolazione naturale per la funzione di rimozione del calore di decadimento, implementati nella progettazione delle centrali elettriche di Gen III + e mirate al miglioramento della sicurezza degli impianti.
L'attività è così ripartita: dopo una breve descrizione dei sistemi di sicurezza per la rimozione del calore residuo implementati nei reattori di ultima generazione, vengono riportate le principali caratteristiche dei sistemi attivi e passivi, quindi si illustrano le metodologie per la valutazione della relativa affidabilità con riferimento ad un caso tipo rappresentato dall'Isolation Condenser, i sistemi attivi e passivi che svolgono la medesima funzione vengono paragonati in termini di affidabilità, le sequenze incidentali che comportano la degradazione del nocciolo vengono analizzate ed infine vengono valutate le risposte e le prestazioni dei sistemi di sicurezza per far fronte alle suddette sequenze incidentali.
L'analisi rivela alcuni spunti importanti, i quali richiedono sforzi significativi da investire in nuovi progetti per soddisfare gli obiettivi di sicurezza ambiziosi.
Ad esempio, con riferimento ai sistemi passivi, si riconosce che la valutazione della relativa affidabilità è ancora un problema aperto, soprattutto a causa della quantità di incertezze in gioco, da risolversi all'interno della comunità dei ricercatori nella sicurezza nucleare. Inoltre un'analisi comparativa mostra che il relativo grado di sicurezza è comparabile o perfino inferiore a quello dei sistemi attivi, in quanto la auspicata maggiore affidabilità e disponibilità viene messa in discussione da alcuni importanti aspetti funzionali, compromettendo le loro prestazioni.
Lo studio probabilistico mostra lo stesso ordine di grandezza (intorno a 1.0E-7) relativo ai valori di CDF (Core Damage Frequency) per i due reattori EPR ed AP1000, caratterizzati rispettivamente dall'adozione di sistemi di emergenza attivi e passivi, a fronte dell'incidente di SBO (Station Black Out): pertanto i margini di sicurezza sono comparabili, sebbene sia da osservare che per il reattore EPR tale traguardo sia conseguito grazie alla elevata ridondanza dei sistemi di sicurezza per la rimozione del calore di decadimento. Un elevato livello di ridondanza oltre ad aumentare la complessità dell'impianto stesso, accresce anche il rischio di guasti comuni (come è avvenuto a Fukushima), che possono coinvolgere tutti i sistemi interessati, causandone il fallimento di tutti contemporaneamente.
Infine si può affermare che:
per i sistemi di sicurezza passivi:

- la supposta maggiore disponibilità ed affidabilità viene messa in discussione da alcuni importanti aspetti funzionali, tali da comprometterne la prestazione,

per i sistemi di sicurezza attivi:

- il livello di ridondanza provoca un maggiore livello di complessità dell'impianto, che é un fattore di rischio per sé, nonché la vulnerabilità dell'impianto ai guasti di causa comune.

Table of contents

Summary

Main focus of the present study is the comparative assessment of NPP active and passive system response under extreme accident conditions, like the Station black out transient, as emerging from the Fukushima Dai-ichi events analysis. Special emphasis is placed on the thermal-hydraulic passive systems, resting on natural circulation and devoted to decay heat removal safety function in accident conditions, implemented in the design of Gen III+ power plants aiming at plant safety improvement.
The analysis reveals some important insights, calling significant efforts to be invested in new projects to fulfil the ambitious safety goals.
For instance, with reference to passive systems, it is recognized that their reliability assessment is still an open issue, mainly due to the amount of concerned uncertainties, to be resolved among the community of researchers in the nuclear safety. Moreover a comparative analysis shows that their safety achievement is comparable to or even less than the active systems' one, since the claimed higher reliability and availability are challenged by some important functional aspects, impairing their performance.
The results of the SBO's probabilistic safety assessment for EPR and AP1000 reactors, show that the safety levels reached by active safety systems reactors of GEN III+ (EPR) are comparable to those of passive safety system reactors (AP1000). However the EPR reactor is able to achieve these high safety levels by increasing the redundancy of the safety systems. In fact redundancy implementation increses the plant complexity and the susceptibility to common cause failures (as was flooding for Fukushima accident), able to affect all the devices, causing the contemporary failure of all of them.
Finally we can state:
for Passive Safety Systems Reactors that:

- their claimed higher reliability and availability are challenged by some important functional aspects, impairing their performance.

for Active Safety System Reactors that:

- the higher level of redundancy causes a higher level of complexity of the plant, that is a risk factor itself, and the plant vulnerability to common cause of failures.

1. Introduction

The earthquake and subsequent tsunami on March 2011 led to a station blackout and the loss of all control systems at the Fukushima Dai-ichi nuclear power plant. With the loss of the cooling capabilities, the decay heat and exothermal oxidation processes led to a core meltdown in the three boiling water reactors on line, accompanied by hydrogen explosions and mechanical energy release. Modern light water reactor designs with their advanced active and passive safety features should have survived the Fukushima event. Therefore the plant behaviour under relevant accident conditions, i.e., beyond design basis accidents, has to be assessed, especially in terms of performance assessment of innovative systems, like passive systems, implemented in the design of Gen III+ power plants aiming at plant safety improvement. Special emphasis is placed on the thermal-hydraulic passive systems, resting on natural circulation and devoted to decay heat removal safety function in accident conditions. Therefore the main objective of the present study is to analyse and compare the performance of active and passive systems under extreme accident conditions, as the Station Black Out transient.
The study is organized as follows: after a brief description of the safety systems for the removal of residual heat implemented in new reactor design, the main characteristics of active and passive systems are illustrated together with the methodologies for the assessment of the relative reliability with reference to a typical case represented by the Isolation Condenser, the active and passive systems that perform the same function are compared in terms of estimated reliability, the accident sequences that involve core degradation are analyzed, and finally we evaluate the response and performance of safety systems to cope with the above-mentioned accident sequences.

2. Gen III+ Decay Heat Removal systems descriptions

AP1000

Passive Core Cooling System (PXS)

The AP1000's PXS provides core residual heat removal, depressurization and safety injection without the necessity of operator action nor AC electric power supply. The PXS includes one passive residual heat removal heat exchanger (PRHR-HX) connected to the first loop of the RCS with an inlet and an outlet line. The PRHR-HX is located inside the IRWST (positioned above the RCS to guarantee natural circulation) that provides the heat sink for the heat exchanger.
When PXS operates in residual heat removal mode the primary cooling water circulates through the PRHR-HX by natural convection. The decay heat is transferred to the IRWST's water, cooling the primary water that is re-injected inside the RCS. IRWST's water reaches the saturated temperature in a few hours and begins to evaporate. The steam generated is condensed by the Passive Containment Cooling System and redirected inside the IRWST.

EPR

Decay heat generated in EPR's core is removed by SIS/RHRS system, operating in RHR mode. The system consist of four independent ad separated trains, each composed by an accumulator, a MHIS Pump, a LHIS Pump and a Heat Exchanger. Any single train is connected to the RCS through a suction line derived from the hot-leg and a injection line placed on the cold-leg.

When operating in RHR (Residual Heat Removal) mode, LHIS Pump draws the primary cooling water from the RCS's hot-leg. The primary cooling water is sent to the LHIS's Heat Exchanger (LHIS-HX) where the residual heat is removed by the CCWS (Component Cooling Water System) and the primary cooling water is cooled.
The cooled primary water is than re-injected inside the RCS through the junction located on the cold-leg.

ESBWR

Passive Decay Heat Removal System

ESBWR is equipped with passive decay heat removal system denominated Isolation Condenser System (ICS) that guarantee an adequate core cooling for at least 72 hours without any operator action nor AC current power supply. The ICS is a closed loop composed by an isolation condenser located inside a water pool outside the containment and an inlet and an outlet line that connect the ICS to the RCS. When the reactor is in shutdown state, the steam generated inside the vessel because of decay heat flows, by natural circulation, inside ICS's outlet line, reaching the isolation condenser. In the isolation condenser the steam condensate. Water in than re-injected in the RCS through the inlet line.
The water pool is vented to the atmosphere and located outside the primary containment. The water inventory of the pool, operating as heat sink for the ICS, is sufficient to guarantee an adequate reactor cooling for at least 72 hours.

3. Active and passive safety systems

As emphasized in the previous section, in the safety system design for Nuclear Power Plants (NPPs), the fluid dynamic systems to cope with accidents can be based on different functional principles:

-*Active design;* the function of the fluid dynamic system is directly related to the function of the active component, e.g. the active component 'pump' forces the medium through a heat exchanger.
-*Passive design;* the function of the fluid dynamic system is based on physical principles after actuation of the system, e.g. medium flow by gravity, heat transfer by natural convection.
A simplified summary of Gen III+ reactor designs is shown in the following table:

	Design	**Safety**
BWR	ABWR	Active
	ESBWR	Passive
PWR	EPR	Active
	AP1000	Passive

Table 3.1 Generation 3+ summary

Recently, development of passive safety reactors has been very prevalent, since passive designs seem to be favoured by the public, because of the claimed advantages of simplicity, reduction of the need for human interaction, reduction or avoidance of external electrical power.

These attractions may lead to increased safety and acceptability of nuclear power generation if the detractions can be reduced.
In fact, 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.
In the present discussion focus is placed mainly on passive systems and in order to achieve an objective decision, probabilistic methodology can be used for evaluation of the relative performance and comparison with active ones.
At first some considerations on active systems are recalled as drivers for introduction of passive safety features in Generation III+ Nuclear Power Plants.

3.1 Safety issues concerned with active systems

The conventional reactors or so called ‘‘traditional ones’’ have seen an extensive use of ‘‘active’’ engineering safety systems for reactor control and protection in the past. These systems have certain potential concerning termination of events or accidents that are effectively coped with by a protective system limited by the reliability of the active safety systems or prompt operator actions to prevent significant fuel failure and fission product release.
For example, with reference to the DHR safety function, the dissipation of decay heat is accomplished in Gen III+ water reactors, like EPR, via redundant emergency core cooling systems (ECCS), improving system design with more independence, separation and diversity, to cope with Common Cause Failures (CCF) that can challenge the system performance.
Since the reliability of active systems cannot be reduced below a threshold and that of the operator’s action is debatable, there is growing concern about the safety of such plants due to the large uncertainty involved in Probabilistic Safety Analysis (PSA), particularly in analyzing human faults.
In view of this, a desirable goal for the safety characteristics of an innovative reactor is that its primary defence against any serious accidents is achieved through its design features preventing the occurrence of such accidents without depending either on the operator’s action or the active systems.
That means that, in addition to the implementation of redundancy provisions for active systems, the plant can be designed with adequate passive and inherent safety features to provide protection for any event that may lead to a serious accident. Such robustness in design contributes to a significant reduction in the conditional probability of severe accident scenarios arising out of initiating events of internal and external origin. The function of confinement of any radioactivity released in the containment is also made more reliable by adopting robust, redundant, and passive design features.
That means such reactors are different from traditional ones, i.e. they are designed on the philosophy of ‘‘safety by design’’. Such reactors have the potential to restore the reactor to a stable state in any postulated accident condition and the risk to the public must be at least in the same level or even lower than the other industrial plants. The most important safety tasks of the future reactors are not only to prevent excessive radioactive release to the environment but also to avoid necessity of evacuation of the population. Minimum frequency of such events should not exceed an acceptable level, which is much lower than that of current reactors. Generally, this is very ambitious and, often, economically expensive task if the

future reactors are built with active engineering safety features. On the other hand, passive safety systems are claimed to have higher reliability compared with active safety systems and could help in meeting the above criteria without much economic penalty. Moreover, advanced reactor safety systems can be designed and built with more inherent and passive systems with multiple lines of defence-in-depth which would provide adequate protection against any release of radioactivity outside the plant containment.
As a result most of future plant designs are introducing passive safety features that do not depend upon external source of power for their successful performance and the need for human interaction and external signal is reduced: safety systems of a modern nuclear plant are implemented so that they combine both passive and active safety features.

3.2 Safety features of passive 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.
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, (ref. 3.1), in combination with active safety or operational systems.
A categorisation has been developed by the IAEA in ref. 3.2 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 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, over these last years a lot of efforts have been devoted among the international community mostly to the development of consistent approaches and methodologies aimed at the reliability assessment of the T-H passive systems, with reference to the modelling and evaluation of the implemented physical principles (gravity, conduction, etc.) upon which the system is relying. 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 modelling the passive systems should be considered in the assessment process.

Section 3 References

3.1 NEA CSNI/WGRISK, 2002. Workshop on Passive Systems Reliability—A Challenge to Reliability, Engineering and Licensing of Advanced Nuclear Power Plants.

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

Cadarache, (F), 4-6/03/'02, NEA/CSNI/R (2002)10

3.2 IAEA TEC-DOC-626, 1991. Safety Related Terms for Advanced Nuclear Power Plants. September 1991.

4. Performance assessment of passive systems

This chapter is conveniently subdivided in two sections presenting a) 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 b) the reliability study of a typical natural circulation, two-phase flow loop passive system having a configuration relevant to the technology of currently advanced Light Water Nuclear Reactors. Firstly, hereafter, an introduction on the main components of Probabilistic Safety Assessment approach is presented and the general passive system unavailability model is proposed.

4.1 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] (ref. 4.1). 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 on 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 4.1. 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.

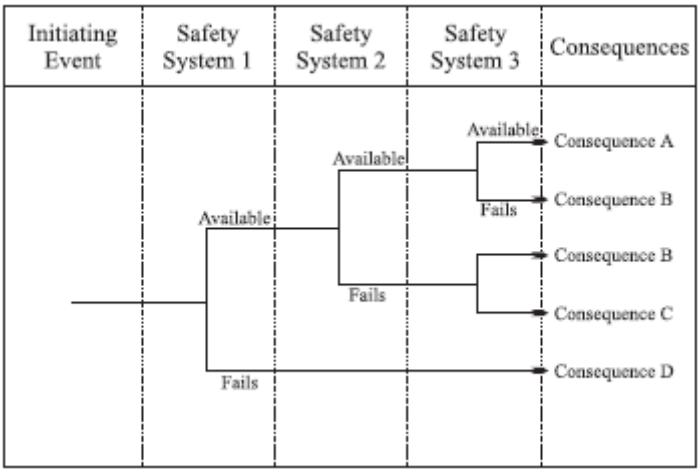


Figure 4.1. Example of an event tree

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 4.2. 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.

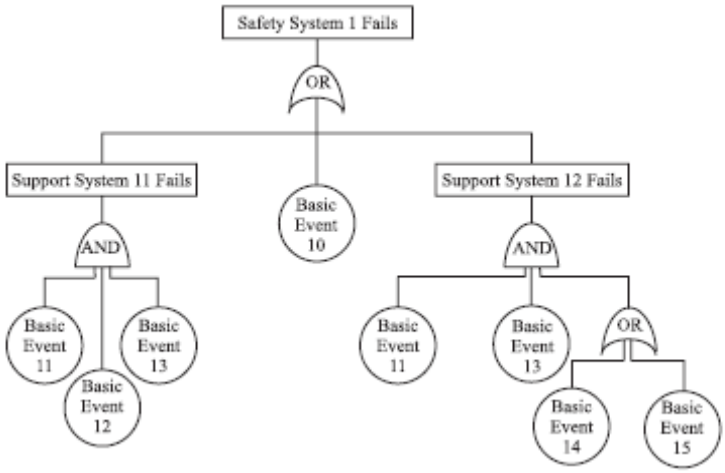


Figure 4.2 Example of a fault tree

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.

4.2 Generic Passive System Unavailability Model

Generally speaking, the reliability of passive systems depends upon:

- the environment that can interfere with the expected performance (e.g. internal, external or environmental attacks),
- the physical phenomena that can deviate from the expectation (e.g. exceeding the range of experience during severe accidents),

- passive components reliability reflecting that a passive component of the system may fail to meet the required passive function (e.g. leakage or blockage).

The principle of this mutual interaction is shown in figure 4.3.

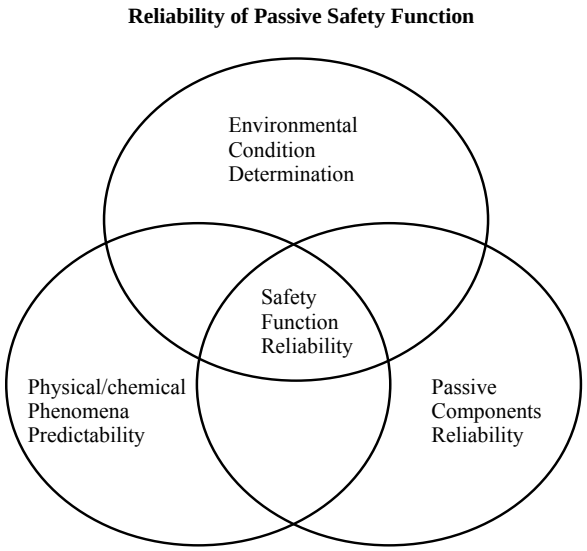


Figure 4.3 Parameters affecting the functional reliability

This is particularly relevant as far as the type B passive systems are concerned: their reliability 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.

According to this, these two kinds of system malfunction are to be expected, to be considered as ET headings and to be assessed by specific fault trees:

- Failure to start-up (e.g. valve failure to open), which addresses mainly the component malfunction rather than the initial conditions and mechanisms needed for starting the system operation
- Failure to continue operating (e.g. natural circulation stability)

These two kinds of system malfunction are to be considered as ET headings, to be assessed by specific FT components, as shown in figures 4.4 and 4.5.

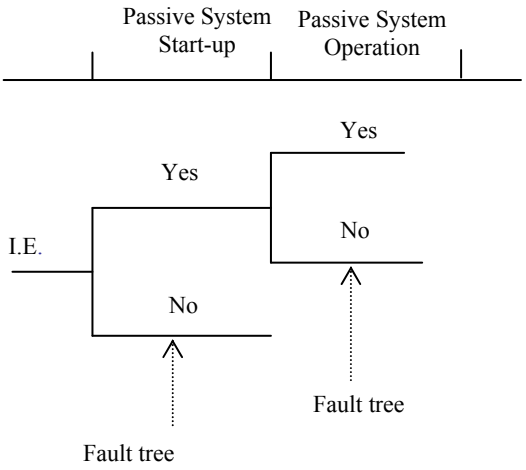


Figure 4.4 Event tree development

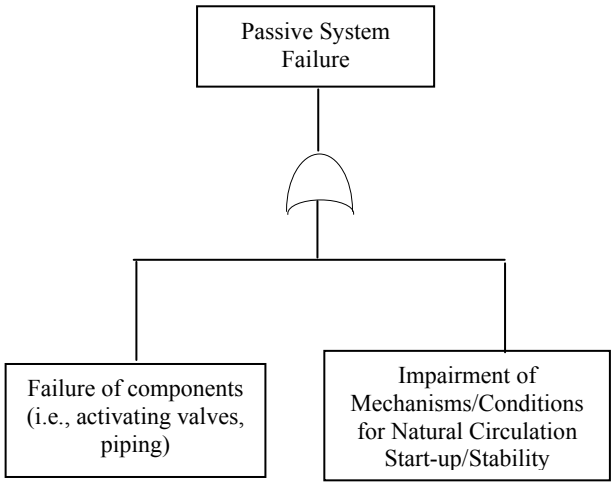


Figure 4.5 Fault tree model

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.
These two concurrent aspects should be conveniently worked out in order to achieve a consistent approach. In the forthcoming sections all these concepts will be comprehensively expanded to properly address the passive system assessment topic.

4.3 State of the art on the methodologies

This section is organized as follows: at first the current available methodologies are illustrated and compared, the open issues coming out from their analysis are identified and discussed.
A very good description of the various methodologies proposed so far and currently available in the open literature is given in ref. 4.2.
The earliest significant effort to quantify the reliability of such systems is represented by a methodology known as REPAS (Reliability Evaluation of Passive Systems), (ref. 4.3), 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 ref. 4.4, 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 4.5. 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 ref. 4.4. 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 ref. 4.6 and 4.7. 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 (ref. 4.8), 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, (ref. 4.9), 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 (ref. 4.10). 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 ref. 4.11. 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 taken from ref. 4.12 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 4.1 Main features of the various approaches

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 they will be treated separately.

- The comparison between active and passive systems, mainly on a functional viewpoint (this point is being dealt with in section 5).

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.

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 ref. 4.6 and 4.9.

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, 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 are recognized as epistemic uncertainties (ref. 4.9).

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, 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 4.2 (ref. 4.2).

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 4.2 Categories of uncertainties associated with T-H passive systems reliability assessment

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 ref. 4.13, which outlines the main aspects of the REPAS procedure.
In ref. 4.13, 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.

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 ref. 4.11, 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 ref. 4.10, 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, (ref. 4.14): 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 paragraph, 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, (ref. 4.15), 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, (ref. 4.16).

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 (ref. 4.17, 4.18). 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. 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. 4.19 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 ref. 4.4 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.
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.
The goal of dynamic PRA is to account for the interaction of the process dynamics and the stochastic nature/behaviour 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 ref. 4.20, which introduces the T-H passive system as a non-stationary stochastic process, where the natural circulation is modelled 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.

4.4 Study of the Reliability of a Passive System for DHR (i.e. Isolation Condenser)

As outlined above, a passive system has a reliability and availability determined mainly by two factors: the integrity (and functionality, if a component is used in a very limited way to initiate subsequent passive operation) of its components and by the confidence with which it will perform under all required conditions, that is the thermal-hydraulic performance.
The present study is concerning a relevant thermal-hydraulic passive system designed for decay heat removal of advanced boiling water reactors, relying on natural circulation and provided with a heat exchanger immersed in a cooling pool, acting as heat sink, and connected to the pressure vessel via steam and condensate lines, that is the Isolation Condenser (IC), whose features are here briefly recalled.
The IC system is designed to remove excess sensible and core decay heat from the BWR reactor by natural circulation, when the normal heat removal system is unavailable, after any of the following events:

- Sudden reactor isolation from power operating conditions;
- Reactor hot standby mode;
- Safe shutdown conditions.

Its main purpose is to limit the overpressure in the reactor system at a value below the set point of the Safety Relief Valves (SRV), preventing unnecessary reactor depressurization.
The IC system (outlined in fig.1) basically consists of a number of totally independent loops, taking into consideration a redundancy degree (for example the IC foreseen for the Simplified Boiling Water Reactor consists of three redundant units, each unit made of two identical modules which act as heat exchangers), each loop contains a heat exchanger (straight tube bundle), that condenses steam on the inner tube side and transfers heat to the water in a large pool, located in the reactor building and above the reactor containment, which is vented to the atmosphere.
The IC is connected by piping to the reactor pressure vessel, and is placed at an elevation above the source of the steam in the Reactor Pressure Vessel (RPV). The steam connection between the vessel and the IC system condenser is normally open and the condensate line is normally closed. This allows the IC and drain piping to fill with condensate, which is maintained at a sub-cooled temperature by the pool water during normal power operation of the plant. The condensate line is provided with a main and a bypass valves which open when operation of the IC system is required thus allowing steam flow directly from the reactor into the condenser, and once condensed the liquid drains into the reactor vessel by gravity via the return line. The flow rate is determined by natural circulation. The primary side of the condenser is also provided with vent lines to remove non-condensable gases, which may reduce heat transfer rates during extended periods of operation. These lines are provided with two main and two bypass located in series valves which are required to open upon high reactor pressure values, during IC operation.
It has to be underlined that, actually, due to the opening of the valve on the condensate line in order to trigger its operation, the IC system should comply with the IAEA category D, which addresses the intermediary zone between active and passive, where the passive execution of the safety function is accomplished through passive means (that is natural circulation) but the process is initiated by active components (in the present case the valve actuation).

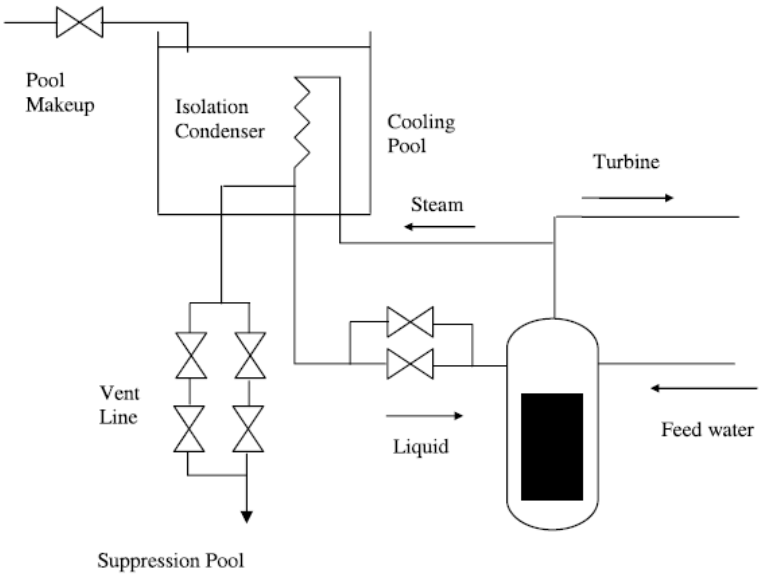


Fig.4.6 Isolation Condenser of a BWR

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 4.3 and 4.4 respectively.

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

Component	Failure Mode	Causes	Prev. Actions on Causes	Consequences	Corrective/Preventive Action on Consequences	Comment
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
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

Component	Failure Mode	Causes	Prev. Actions on Causes	Consequences	Corrective/Preventive Action on Consequences	Comment
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
	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 4.3 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 4.4 HAZOP Table for the Isolation Condenser system

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

Each of these failure mode drivers could be examined to determine the expected failure probability by defining the range and the probability distribution function pertaining to the parameter. These failure characteristics would 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:

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

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:

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

$p_i(x)$ 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, as illustrated in ref.. In fact, as previously 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.

Conversely in the present treatment we'll apply the approach set forth by ENEA as presented above and specifically the method based on failure mode of hardware components.

According to the general procedure the unavailability of a passive system is the sum of two contributions:

1. failures of actuation devices, that is, failures of the components that must change state in order to start the passive operation; an example is the condensate return line valve of the IC.
2. failures that defeat or degrade the natural mechanisms that are the principles for the operation of the passive systems.

The first contribution is treated in the classical way, that is, as a failure of a component that must change its state or a failure of the supporting systems, such as the electrical power supply. The second contribution requires the identification of the mechanisms and the boundary conditions needed for starting and maintaining the intrinsic phenomena. The failure probability is evaluated in the classical way as an unavailability of components or as the probability of occurrence of a failure mode that would violate the needed boundary conditions or mechanisms.

The component reliability data are based on fission reactor experience: they are generally taken from available data bases, and when no references are available, data are determined on the basis of engineering judgment. The analysis does not focus on one defined advanced BWR; nevertheless, the functions and the general requirements for the system and its arrangement are drawn from the available literature although the general validity of the present study is not affected by the particular IC considered.

The major components of the system are (see Fig. 4.6):

1. heat exchanger (straight tube bundle)

2. one main valve and a bypass valve in parallel with the main valve located on the drain line
3. piping.

The most critical components of the system are the motor operated valves on the condensate line that are required to actuate during transients, for instance, upon high reactor pressure or low reactor water level.
In Table 4.5 the system component reliability data are reported, while in Fig. 4.7 the related fault tree is shown.

IC Component Reliability Data

Component	Failure Mode	Failure Rate	Reference
Valve	Fails to open	3.0E−3/d[a]	IREP[b]
Valve	Fails to remain open	1.0E−7/h[c]	IREP
Valve	Fails to open countercurrent flow	3.0E−4/d	Expert judgment
Valve	Fails to remain open CCF	1.0E−8/h	Expert judgment
Heat exchanger	Single pipe rupture	3.0E−10/h	IREP
Heat exchanger	Multiple pipe rupture	3.0E−11/h	IREP
Heat exchanger	Single pipe plugging	3.0E−10/h	IREP
Heat exchanger	Multiple pipe plugging	3.0E−11/h	IREP
Piping	Rupture	2.4E−8/h (1.2E−9/hm × 20 m)	Expert judgment

[a]Read as 3.0×10^{-3}/demand.
[b]Interim Reliability Evaluation Program.
[c]Read as 1.0×10^{-7}/hour.

Table 4.5 Component reliability data

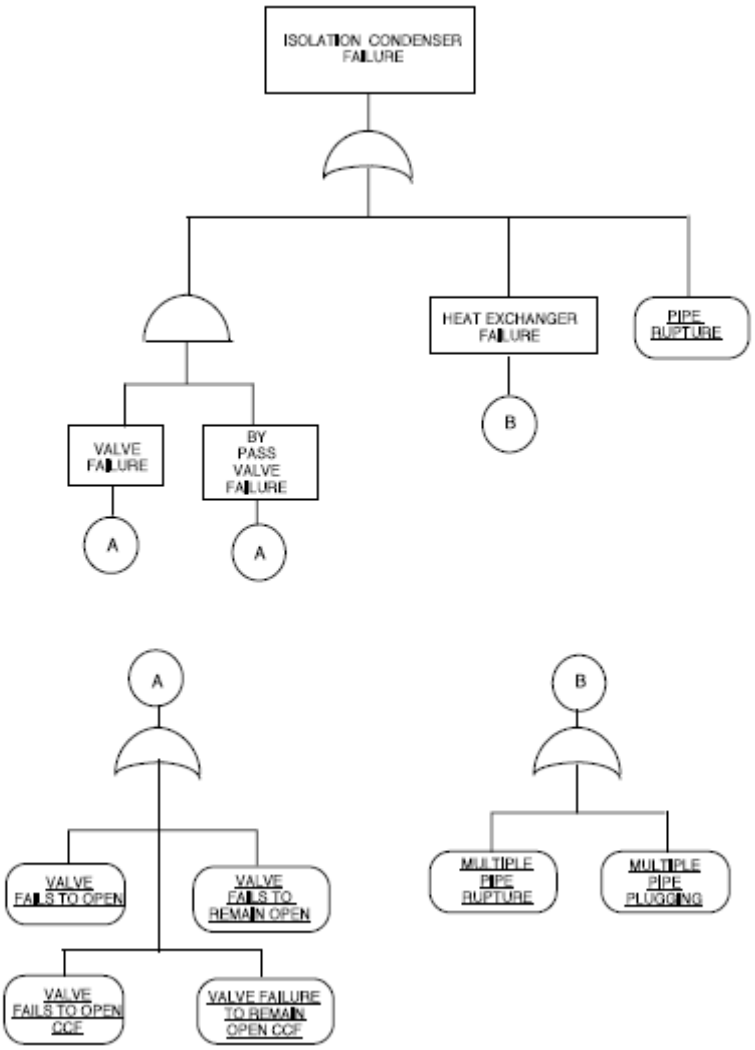
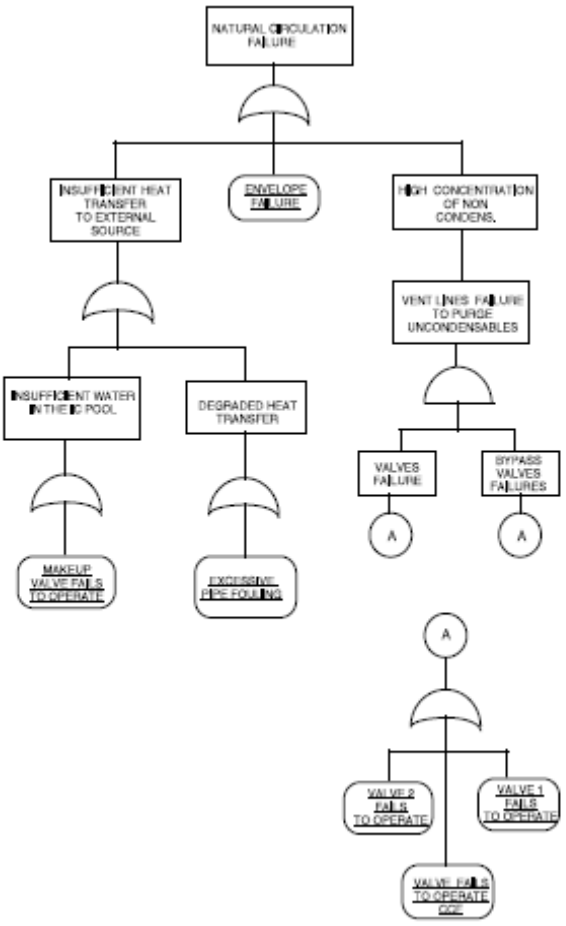


Fig 4.7 The IC fault tree.

The probability of natural circulation loss is stated as the probability of occurrence of different failure modes that impair the needed conditions or mechanisms for passive function performance.
As stated above, in order to overcome the difficulties related to the probabilistic characterization of the relevant parameters, the present effort aimed at the natural circulation assessment is developed through an approach that implies the evaluation of components designed to assure the best conditions for passive function performance.
Therefore, the natural circulation failure probability is assessed by the development of the fault tree reported in Fig. 4.8, which examines three main failure modes, that is, loss of heat transfer, presence of non condensable gases, and loss of primary boundary, while the overall fault tree relative to the IC system is reported in Fig. 4.9, which includes the natural circulation loss.



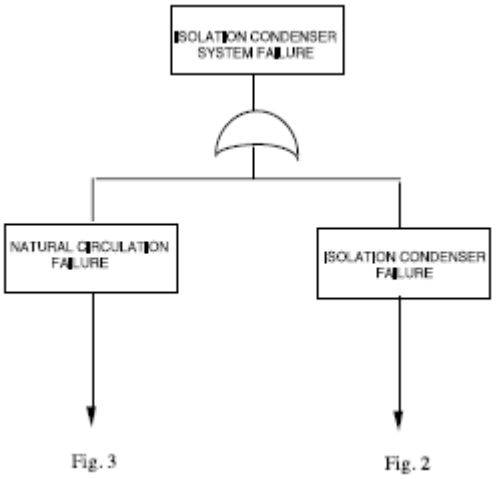


Fig. 4.9 The IC system fault tree.

Fig. 4.8. The natural circulation fault tree.

Loss of heat transfer addresses the failure of the IC heat transfer to an external source (IC pool water), which is assessed through two possible failures:

1. insufficient water in the IC pool (makeup valve)
2. degraded heat transfer conditions due to heat exchanger pipe excessive fouling.

The envelope failure, i.e., loss of primary boundary failure mode is given as the failure rate relative to piping rupture (1.2×10^{-9}/hm) and has already been taken into account in the IC fault tree; excessive pipe fouling failure mode is assigned the failure rate relative to multiple pipe plugging for the heat exchanger.
The reliability values for the natural circulation failure are reported in Table 4.4.

Reliability Data for Natural Circulation

Component	Failure Mode	Failure Rate	Reference
Valve	Fails to operate	3.0E−3/d[a]	IREP[b]
Valve	Fails to open CCF	3.0E−4/d	Expert judgment
Heat exchanger	Excessive pipe fouling	3.0E−11/h[c]	IREP[b]
Primary boundary	Rupture	1.2E−9/hm × 20 m	Expert judgment

[a]Read as 3.0×10^{-3}/demand.
[b]Interim Reliability Evaluation Program.
[c]Read as 3.0×10^{-11}/hour.

Table 4.4 Reliability Data for Natural Circulation

The reliability assessment of the IC system is performed at component level by means of the RISK SPECTRUM code, a personal computer software package for system risk and reliability analysis based on the fault tree technique. In the RISK SPECTRUM code, fault trees are built with the component reliability model, the component reliability data are assigned, and the final system reliability is assessed through the quantification of the fault tree.
The results obtained from both systems' reliability evaluation are shown in Table 4.5.

Failure Probabilities for IC

System	Failure Probability	Contributor (%)
IC	3.1E−4[a]	8
Natural circulation	3.3E−3	92
IC system	3.6E−3	

[a]Read as 3.1×10^{-4}.

Table 4.5 Failure Probabilities for IC

From Table 4.5 one infers that the natural circulation failure probability, which is evaluated with regard to the failure of specific system components, is the main contributor to the total system unavailability.
Moreover, it has to be pointed out that the aforementioned degree of redundancy of the units (for example, the IC foreseen for the SBWR consists of three redundant units, each unit made of two identical modules that act as heat exchangers) leads to a reduction in failure probability values, with the exception of CCFs evaluations.
The minimal-cut-set analysis identifies the failure of heat transfer to the external source due to insufficient water in the IC pool (in the study this failure is represented by the basic event consisting of the makeup valve fault) as the most important contribution to the final reliability value of the system. Other important contributions are given by the common-mode failures relative to either the valves on the drain line or the vent valves for un condensable gases purging.

Section 4 References

4.1 United States Nuclear Regulatory Commission's (U.S. NRC) Reactor Safety Study (WASH-1400, 1975)

4.2 Zio, E., Pedroni, N., 2009. Building Confidence in the Reliability Assessment of Thermal hydraulic Passive Systems. Reliability Engineering and System Safety, 94, 268-281

4.3 Jafari, J., D'Auria F., et al., 2003. Reliability Evaluation of a Natural Circulation System. Nuclear Engineering and Design 224, 79–104.

4.4 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

4.5 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

4.6 Apostolakis G., Pagani L. and Hejzlar, P., 2005. The Impact of Uncertainties on the Performance of Passive Systems. Nuclear Technology 149, 129–140

4.7 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

4.8 Burgazzi, L., 2002. Passive System Reliability Analysis: a Study on the Isolation Condenser, Nuclear Technology 139, 3-9.

4.9 Burgazzi, L., 2007a. Addressing the Uncertainties related to Passive System Reliability. Progress in Nuclear Energy 49, 93-102.

4.10 Burgazzi, L., 2003. Reliability Evaluation of Passive Systems through Functional Reliability Assessment, Nuclear Technology 144, 145-151.

4.11 Nayak, A.K., et al., 2008. Passive System Reliability Analysis using the APSRA Methodology. Nuclear Engineering and Design 238, 1430-1440.

4.12 Burgazzi, L., 2011.Addressing the Challenges posed by Advanced by Reactor Passive Safety System Performance Assessment, Nuclear Engineering and Design 241, 1834-1841

4.13 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

4.14 Burgazzi, L., 2008a. Reliability Prediction of Passive Systems based on Bivariate Probability Distributions, Nuclear Technology 161, 1-7.

4.15 Burgazzi, L., 2009. Evaluation of the Dependencies related to Passive System Failure. Nuclear Engineering and Design 239, 3048-3053

4.16 Burgazzi, L., 2011. Reliability Prediction of Passive Systems with Multiple Degradation Measures, Nuclear Technology 173, 153-161.

4.17 USNRC, 2007. Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing. US Nuclear Regulatory Commission, NUREG-1860.

4.18 IAEA, 2007. Proposal for a technology-neutral safety approach for new designs. International Atomic Energy Agency, TECDOC-1570, Vienna.

4.19 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.

4.20 Burgazzi, L., 2008c. About Time-variant Reliability Analysis with Reference to Passive Systems Assessment. Reliability Engineering and System Safety 93, 1682-1688.

5. Comparison active vs 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 the concern arising from the factors impairing their performance 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.
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.
- The passive nature of the safety systems reduces the reliance on operator action, which could imply no inclusion of the operator error in the analysis. In fact the minimization of the intrinsic complexity of the system results in improved human

reliability. The natural circulation core heat removal without, e.g., the incorporation of mechanical pumps results in reduction of operating and maintenance staff requirements, generation of low-level waste, dose rates, and improvement of operational reliability and plant safety and security.

- Passive systems must be designed with consideration for ease of ISI, testing and maintenance so that the dose to the worker is much less.
- The freedom from external sources of power, instrumentation and control reduces the risk of dependent failures such as the common cause failures

- Better impact on public acceptance, due to the presence of "natural forces".

- Less complex system than active and therefore economic competitiveness.

– Drawbacks

- Reliance on "low driving forces", as a source of uncertainty, and therefore need for T-H uncertainties modelling.

- Licensing requirement (open issue), since the reliability has to be incorporated within the licensing process of the reactor. For instance the PRA's should be reviewed to determine the level of uncertainty included in the models and their potential impact. In fact some accident sequences, with frequencies high enough to impact risk but not predicted to lead to core damage by a best estimate t-h analysis, may actually lead to a core damage when t-h uncertainities are considred in the PRA model.

- Need for operational tests, so that dependence upon human factor can not be completely neglected.

- Time response: the promptness of the system intervention is relevant to the safety function accomplishment. It appears that the inception of the passive system operation, as the natural circulation, is conditional upon the actuation of some active components (as the return valve opening) and the onset of the conditions/mechanisms for natural circulation start-up

- Reliability and performance assessment in any case and their incorporation in the reactor concepts needs to be tested adequately, due to several technical issues as pointed out in section 4.1. 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.
In the following a summary of the analyzed different reactor concepts, that is AP 1000 and EPR, is provided in table 1: it shows the correspondent implemented safety systems along with reactor CDF (Core Damage Frequency) values. (ref.5.1).

Design	General	CDF	Safety Systems	
EPR	Active	1.0E-6	ECCS (comprised of 4 independent trains)	
AP 1000	Passive	2.4E-7	PXS*	PCS*

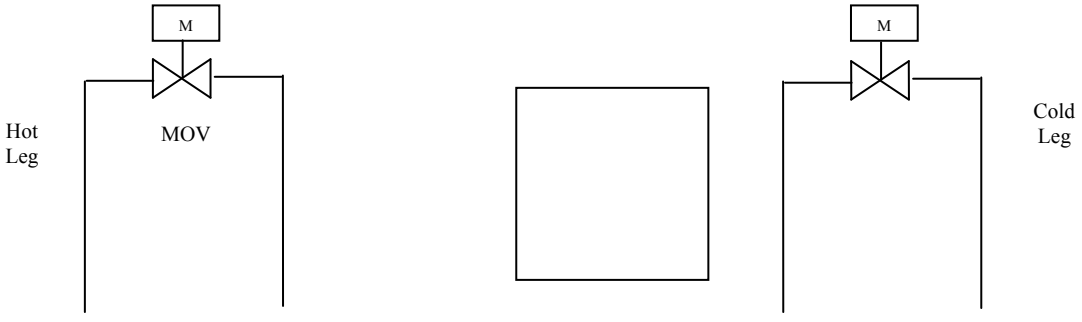
*PXS (Passive Core Cooling Systems) and PCS (Passive Containment Cooling Systems) are classified as type B passive systems

Table 5.1 Summary of Gen III+ PWRs

Among the most important features of the AP 1000 design that contribute to the reduction of the estimated CDF associated with LOOP/SBO (loss of offsite power/station black out) events, are the implemented passive systems as the automatically actuated PRHR, without the need for electrical power (Air Operated Valves, AOV "fail safe" in the open position). In addition the DC batteries are able to support all front line passive safety systems for 72 hours.
Thus the improved reliability of the PRHR system contributes significantly to the reduction of the risk associated with the LOOP/SBO sequences (the function of the PRHR following a LOOP/SBO event is similar to the of the Auxiliary Feed Water system AFW system function in operating PWRs).

5.1 Illustrative Example

In the following an illustrative example of comparative analysis between two different (passive and active) safety systems fulfilling the same function is given: to this aim the probabilistic approach is adopted, as specified in section 3. It has to be underlined that PSA methodology is used mainly as a tool for plant improvement and the main concern is the probabilistic comparison of different system designs in order to assess the most reliable one and identify the weak points of each one of them.
Therefore a quite "straightforward" approach to PSA has been chosen, e.g. through a rather generic data base and relatively simple common mode failure quantification models.
We'll consider a quite "basic" system designed for DHR respectively in the active and passive configurations: each loop consists of a heat source, heat sink and heat transfer loop which correspond to the reactor core, heat exchanger, and connection piping respectively, as represented in the figures here below. In addition in the analysis the eventual system redundancy configurations are overlooked.
In the active design the two motor-operated valves are installed parallel at the system inlet and outlet respectively and are closed during normal operation.



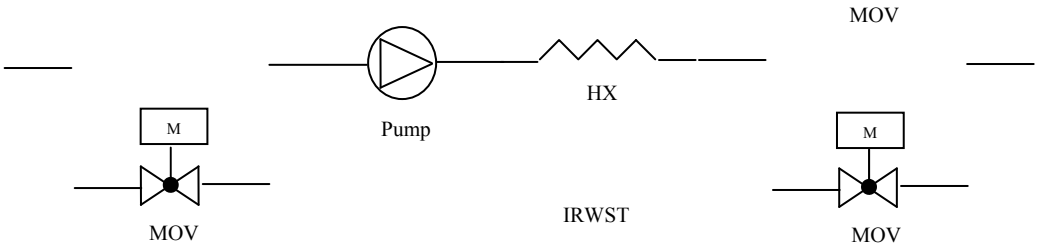


Figure 5.1 Active system configuration

Since our study is concerned with the loss of offsite power accident, it is required to operate the emergency diesel generators (EDGs) when the active system needs to perform its task: we can assume that two identical EDG are installed in parallel and are connected with the active system supplying electrical power.
In the passive design the basic loop is composed of one heat exchanger, two air operated valves which are installed parallel and closed in normal operation, one check valve and one motor-operated valve, which is open in normal operation.

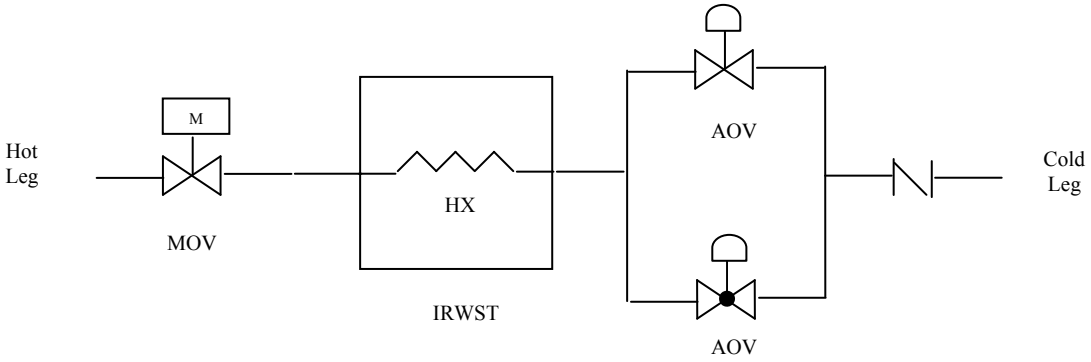


Figure 5.2 Passive system configuration

Hardware reliability
Hardware failure of the active system is evaluated based on major failure modes of the components and the assumption that there is no failure of the IRWST (In containment Refuelling Water Storage Tank) and the two stand-by EDGs are installed and provide power to the active residual heat removal system (ARHR) in the event of offsite power loss.
Reliability data of components reported in tables 2 and 3 refer to available data bases as NRC generic data (ref. 5.2) and relevant studies as in ref. 5.3.

Component	Failure Mode	Probability
EDG	Fail to start	1.4E-2
	Fail to run	5.0E-2

	T&M unavailability	6.0E-3
	CCF	6.13E-5
MOV	Fail to open	1.75E-3
Pump	Fail to start	5.48E-3
	Fail to run	6.0E-4
	T&M unavailability	2.0E-3
Human Error		3.3E-3
Heat exchanger	Envelope failure	2.4E-5
Check valve	Fail to open	1.75E-3

Table 5.2 Reliability data of hardware for active design

Component	**Failure Mode**	**Probability**
AOV	Fail to open	1.09E-3
	T&M unavailability	5.0E-4
Human Error		3.3E-3
Heat exchanger	Envelope failure	2.4E-6
Check valve	Fail to open	1.75E-3

Table 5.3 Reliability data of hardware for passive design

The hardware failures of the active and passive design for one loop are evaluated to be 1.63E-02 and 1.88E-03 respectively. The major contributors of the hardware failures are EDGs and pumps in the active system and AOV in the passive one.

The other aspect of the analysis is related to the system functional reliability, that is its capability to perform the required function to achieve the given mission.
The results of the system performance assessment by thermal hydraulic simulations are shown in Table 5.4 (ref. 5.4). The values obtained in Table 5.4 are conditional probabilities based upon the natural circulation having already been established. The functional failure probability result of one loop in the passive design is about 0.72, which is too large for practical use.
The result of the two loop configuration passive design functional failure probability is 0.0354, which is comparable to usual system hardware failure.

System type	1 loop	2 loops	3 loops
Passive design	7.23E-01	3.54E-02	9.20E-3
Active design	6.67E-03	3.20E-04	<1.0E-5

Table 5.4 Probabilities of Functional Failure for different parallel loop configurations

As seen an active design has a relatively low values of failure probability in comparison with those of passive designs.
One reason is that the active design has a high mass flow rate compared with that of passive design,

which contributes to increase of performance margin in functional analysis in the system.
In the final stage of the analysis a comprehensive comparison of active and passive designs is performed by including both aspects related to the hardware and failure probabilities: the system failure probabilities are evaluated depending on an increase of loop configurations.
Next table present the result of single loop analysis for active and passive design. Hardware and human error are the most dominant modes of failure in the active design. On the other hand functional failure is an outstanding dominant factor in the passive design. In both cases one more loop needs to be added in order to reduce the hardware failure probability and the functional failure probability by means of increasing heat removal capacity respectively.

Design	**Hardware Failure Probabilities**	**Functional Failure Probabilities**	**System Failure Probability**
Active	1.62E-2	6.67E-3	3.87E-2
Passive	1.88E-3	7.23E-1	7.31E-1

Table 5.5 Failure probabilities of one loop active and passive design (human error probabilities not shown)

Next table presents the results of two loop active and passive design.

Design	**Hardware Failure Probabilities**	**Functional Failure Probabilities**	**System Failure Probability**
Active	9.09E-3	6.67E-3	2.86E-2
Passive	3.61E-3	3.54E-2	4.85E-2

Table 5.6 Failure probabilities of two loop active and passive design (human error probabilities not shown)

Note that in the active design one has only a limited reduction of the failure probability, mainly because of the common cause failures. In this step one can observe that the two alternative designs are comparable in terms of total failure probability, because of the reduction of the functional probability.
Ultimately, Table 5.7 presents the results of three loop active and passive design

Design	**Hardware Failure Probabilities**	**Functional Failure Probabilities**	**System Failure Probability**
Active	9.64E-3	3.2E-4	2.3E-2
Passive	5.4E-3	9.2E-3	2.71E-2

Table 5.7 Failure probabilities of three loop active and passive design (human error probabilities not shown)

The value of 2.3E-2 is the minimum achievable value of the system failure probability for the active design. The results of the passive design analysis shows an increase in hardware failure probability, because the number of components, which are required to work together when the passive system needs to be actuated, is increased due to more loops involved. Further functional failure is still not ignorable.

Summarizing, the comparison of failure probabilities according to loop configurations and failure modes of active and passive design shows a better results for active configurations than passive ones due to functional failures
However a more extensive comparison may require including the uncertainty associated with each failure mode, such as hardware and functional failure: the considerations of these uncertainties can make the results different from the ones presented in this section.

Section 5 References

5.1 Eul, R.C., 2006. The impact of Passive Safety Systems on Desirability of Advanced Light Water Reactor, Master of Science in Nuclear Science and Engineering, Massachusetts Institute of Technology

5.2 NUREG/CR-4550. Analysis of Core Damage Frequency from Internal Events, US NRC,1990

5.3 Westinghouse AP1000 PRA report (AP1000PRA, 2002, AP1000 Probabilistic Risk Assessment, Revision 1, 2002

5.4 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.

6. Analysis of safety relevant accident sequences with significant core degradation

6.1 Stress Tests

Definition of Stress Test by ENSREG
Considering the Fukushima accident, European Council declared on 24 and 25 March 2011 that "the safety of all EU nuclear plants should be review, on the basis of a comprehensive and transparent risk assessment (stress tests); the European Nuclear Safety Regulatory Group (ENSREG) and the Commission are invited to develop as soon as possible the scope and modalities of these tests [...] in the light of the lesson learned from the accident in Japan [..]; the assessment will be conducted by independent national authorities and through peer review; their outcome and any necessary subsequent measures that will be taken should be shared with the Commission and with ENSREG and should be made public [...]."

Technical scope
ENSREG defines Stress Tests as a "targeted reassessment of the safety margins of nuclear power plants in light of the events occurred at Fukushima: extreme natural events challenging the plant safety functions and leading to a severe accident."
The technical scope of the Stress Tests is to produce an evaluation of the response of a nuclear power plant when facing a set of extreme situations, together with a verification of the preventive and mitigative measures chosen, following a defence-in-depth logic.
The extreme situations that have to be considered in developing the Stress Test for a given nuclear power plant are the follows:

Initiating Events

- Earthquake.
- Flooding.

Consequence of loss of Safety Functions from any initiating events conceivable at the plant site

- Loss of electrical supply (LOOP), including station blackout (SBO).
- Loss of ultimate heat sink (LUHS).
- Combination of both.

As we can see, ENSREG Stress Test claim for an evaluation of the consequences of loss of safety functions as SBO and LUHS, irrespective of the initiating events that cause the loss and their probability to happen.
A deterministic approach, instead of a probabilistic one, is preferred, in order to focus the analysis on the preventive and mitigative measures undertaken to manage the postulated extreme situations.

6.2 EPR

Brief Description of EPR's ECCS
The Emergency Core Cooling System of the EPR, or SIS/RHRS (Safety Injection System/Residual Heat Removal System), consists of four independent and separate trains, each one housed in its own Safeguard Building (SB) which physically protects the system by external hazards as earthquake and flooding. Each train has a separate electrical supply division allocated in the SB. Each electrical division is also supplied by its Emergency Diesel Generator (EDG) which guarantee electrical power supply to the train in case of LOOP (Loss Of Off-site Power). The physical separation of the trains and of their electrical supply reduce the probability that a single common cause failure (CCF) causes the contemporary unavailability of all the trains.
Each train is composed by the following components:

- Medium Head Injection System (MHIS) Pump.
- Low Head Injection System (LHIS) Pump.
- Low Head Injection System Heat Exchanger (LHIS-HX)
- Accumulator.

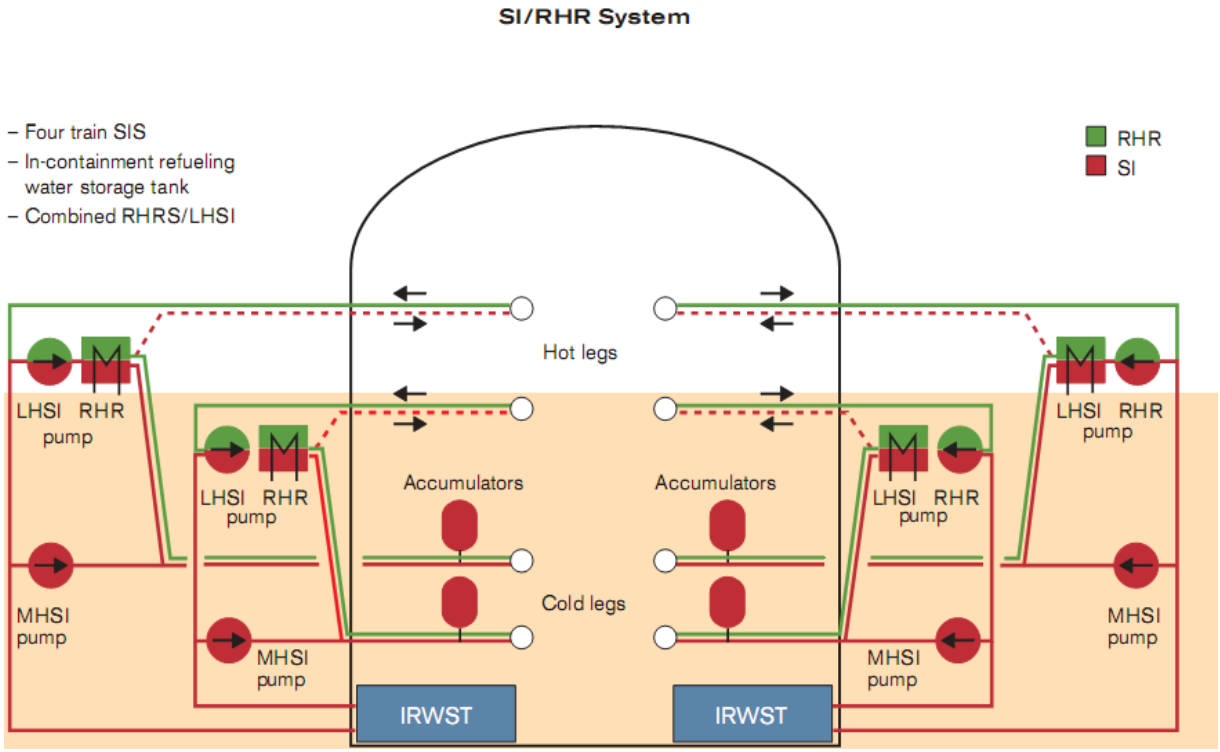


Figure 6.1 EPR's ECCS

The main function of the SIS/RHRS is to provide an appropriate emergency core cooling in case of:

- Loss of primary coolant caused by the impairment of the RCP hydraulic circuit integrity (LOCA accident).
- Reactor Shut Down: the system operating in RHR mode allow to remove from RCP the Residual Heat generated inside the core after reactor shut down.

The whole system is characterised by redundancy 4, i.e. individually each one of the four trains is able to supply the required core cooling.

LOCA

As the primary coolant leak out from the brake, RCS depressurises. When the pressure reaches 91 bar, MHIS Pumps start to inject cooling water directly inside the RCS, via the cold leg, in order to restore the primary coolant inventory. The water injected is driven from the IRWST via a common suction line. LHIS Pumps and Accumulators eventually inject other cooling water inside the RCS if the depressurization continue, depending on the size of the brake (the pressure threshold for Accumulators is 47 bar, for LHIS Pumps is 22 bar).

Residual Heat Removal

Residual heat removal from RCS in shutdown state is performed by SIS/RHRS operating in RHR mode. Primary coolant is drown from RCS via the hot leg by the action of LHIS Pumps, than sent to the LHIS-HX where is cooled. The primary coolant is than re-injected inside RCS via the cold leg.

Immediately after the shut down, when the core is generating an high amount of decaying heat power, RHR is performed by the secondary side, dumping the stem generated inside the SGs (Steam Generators). This process is called Partial Cooldown and requires the continues makeup of secondary coolant inside the SGs. This function is performed by EFWS Pumps (Emergency Feed Water System).
To perform an appropriate cooling of RCS in reactor shut down or post-accident state it is necessary to supply whit electrical power those system charged to the cooling functions (EFWS Pumps, LHIS Pumps). In absence of necessary electrical supply the core damage is reached within few hours from the beginning of the accident sequence.

LOOP and SBO for EPR
Loss Of Off-site Power (LOOP) is defined as loss of both main and auxiliary grid connection. Automatic switchover to house load operation is assumed to fail with a probability of 1. The following analysis covers also the case of Station Black Out (SBO), defined as loss of off-site power together with unavailability of all four Emergency Diesel Generators (EDG).
Let us consider a long term LOOP, or LOOPL (lasting for more than 2 hours and less than 24 hours). The main function challenged in this situation is the residual heat removal, which is provided by different system depending on the reactor state at the beginning of the LOOP.
If the reactor is in power operation state when the LOOP occurs, residual heat removal is performed trough the SGs by dumping the steam generated. In case of LOOPL, the SGs need to be fed by EFWS. In event of SGs failure, the residual heat is removed by Feed and Bleed, which requires the availability of the SIS.
If the reactor is in shutdown state when the LOOP occurs, residual heat remove is performed by the automatic restart of the RHRS trains previously in operation. In event of RHRS failure, the residual heat is removed by dumping the steam generated inside the SGs. This function requires the SGs to be fed by EFWS during LOOPL.
In order to provide an adequate cooling of the core, avoiding its damage, it is necessary to guarantee electrical power supply to the following critical systems:

- EFWS to perform heat removal by SGs steam dumping.
- SIS to perform Feed and Bleed.

Electrical power supply is assured by:

- 4 Emergency Diesel Generators (EDGs) in case of LOOP.
- 2 Ultimate Diesel Generator or SBO-DGs (Station Black Out Diesel Generators) in case of SBO.

Core Damage Frequency
The frequency of LOOP initiating events during reactor operation state, as derived from the EUR, are the follows:

- 6E-02/y for the Short Term LOOP (<2h).
- 1E-03/y for the Long Term LOOP (<24h).

The main accidental sequence the leads to core damage starting from LOOP initiating event is:

- Failure of the 4 Emergency Diesel Generators .
- Failure of the 2 SBO-DG (including operator failure to start the SBO-DG) or failure of EFWS trains supplied by SBO diesels.

The core damage frequency due to the all accidental sequences starting from LOOP initiating event is 1.5E-07/r.y.

LUHS for EPR

The consequences of Loss of Ultimate Heat Sink, i.e. see water, for EPR reactor, are mitigated by using a diverse heat sink, as atmosphere, for residual heat removal process. RHR is though performed by the secondary side, dumping in atmosphere the steam generated inside the Steam Generators (partial cool-down). In order to perform an adequate refrigeration of the core, it is required a continuous reinstatement of the water inventory of the Steam Generators (dumped as steam in atmosphere) by the EFWS.
The reserve of water used for the reinstatement of the SGs consists of:

- 4 EFWS tanks housed in the safeguard buildings, each one with a volume of 400 m^3. This reserve of water is sufficient to guarantee an adequate refrigeration of the core for at least 2 days, without any external assistance (reactor operating at 100% of its nominal power when LUHS occurs).
- 2 Fire Fighting Tanks, respectively containing 1000 and 3000 m^2 of demineralised water, capable to assure other 7 days of adequate refrigeration of the core.

The total amount of demineralised water stored in the plant assures at least 9 days of residual heat removal through the secondary side, without the necessity of any external action.
In case contemporary occurrence of LUHS and LOCA (primary damaged with steam leaking from the brake in RCS), the refrigeration of the core is performed by the SIS, through Feed an Bleed. The water injected inside the RCS by the Safety Injection System is drown from the IRWST. Residual Heat stored in the steam, dumped inside the containment from the brake on RCS, is removed through the action of Containment Residual Heat Removal System (CRHRS).
For this case, the total amount of demineralised water contained in the plant is sufficient to keep the core covered for several days.
Residual heat removal, in case of LUHS, is guaranteed by the demineralise water stored in the plant, for several days following the accident, without the necessity of external actions (refuel of the water tanks). This mitigative measure avoid the risk of an immediate damage to the core caused by LUHS.

SBO and LUHS for EPR

The Station Black Out (SBO) is the total lack of AC electric power supply to the nuclear power plant, caused by all the following events:

- LOOP (Loss Of Off-site Power).
- Failure of all the 4 Emergency Diesel Generators (EDGs)
- Failure of the 2 Ultimate Diesel Generators (SBO-DGs)

Without AC electric power supply, all the AC electric motors of the plant stop, including those who are connected to the pumps. This results in a out-of-service of several system, among which are the following:

- Essential Service Water System (ESWS).
- Component Cooling Water System (CCWS).

As a consequence of these failures the ultimate heat sink of the plant is lost. So we can state that one of the consequences of SBO is the LUHS.
Since many mitigative measures can be taken in order to avoid core damage in case of LUHS (large amount of water stored inside the plant sufficient to guarantee core refrigeration for many days after the LUHS), this kind of accident results far less dangerous for the integrity of the core than SBO.

Mitigative actions in case of SBO
As previously told, SBO results in a total lack of AC electric power supply. As consequence of that all the pumps of the plant, powered by asynchronous AC electric motors, are inoperative.
Without the pumping actions of those device, the Emergency Feed Water cannot be injected inside the SGs that are drying out because of the evaporation of the water stored inside.
Consequently to a SBO some devices and system of the nuclear power plant, as I&C emergency lighting and electric valves, are still powered in DC current by the banks of batteries (2-h and 12-h), so that is still possible execute the steam dumping from the SGs.
Steam dumping avoid an uncontrolled increase of pressure inside the steam generators that are operating in residual heat removal mode through Partial Cool-down, keeping these devices whole.
Besides the dumping operation allows the residual heat generated inside the core by radionuclides decaying process, to be removed from RCP.
However the evaporation of the water stored inside the SGs causes a rapid drainage of these devices that soon are to suffer a dry-out event.
Dry-out causes the inability of SGs to properly remove the decaying heat power generated inside the core, determining an overheating of the core itself, and also an overpressure if venting is not performed.
Overheating causes several effects as:

- Zr-H_2O interaction (Zr is contained in the fuel clad), with production of flammable H_2 gas (that can cause explosion during venting operations).
- Reaching of UO_2 melting point.

These effects lead to severe core damage, with the risk of partial or total meltdown of the fuel rods.

7. Comparative analysis for evaluating active and passive systems performance within the accident sequence

7.1 Influence of the use of active and passive systems on the accident sequence

Active System used in EPR

In a Fukushima like accidental sequence we assume the total loss of off-side power supply caused by the failure of the electrical grid. To perform an adequate core cooling in a reactor that uses only active systems (as the European Pressurised Reactor) it is necessary to guarantee an alternative AC power supply to the plant, in order to ensure the operability of those devices needed for reactor cooling as:

- EFWS Pumps for the partial cool-down performed by the Steam Generators (cooling by dumping of steam generated in the secondary side), if the accidental sequence starts when the reactor is at nominal power state.
- SIS/RHRS Pumps if the accidental sequence starts when the reactor is in shut-down state or if the integrity of the primary side is not assured (in this case the SIS system cools the core through feed and bleed).

All those motor-operated pumps need a continuous AC electric power supply to work, so they are defined as Safety Active Systems.
The alternative AC electric power supply is guaranteed by:

- 4 EDG (Emergency Diesel Generators).
- 2 SBODG (Station Black Out Diesel Generators).

The operability of only one of those 6 emergency power generators is sufficient to ensure a adequate electric power supply to the Safety Active Systems of the plants (EFWS and SIS/RHRS, needed for the reactor cooling), for at least 24 h.
The inoperability of all the 6 emergency power generators causes the out-of-work of the Safety Active System. As a consequence of this, the reactor results not properly cooled; this situation leads to a core's fuel road damage within a few hours from the beginning of the accidental sequence.
As previously said the core damage frequency due to Total Station Black-out (LOOP + failure of all the 6 emergency diesel generators) caused by internal events is:

5E-07/r.y.

This results does not include the possible failure of the diesel generators (4 EDGs and 2 SBODGs) due to external events and common cause failures as earthquake, flooding as in the Fukushima accidental sequence. All those events can determine a common cause failure for the emergency diesels generators, provoking the simultaneous failure of those devices.

Passive Systems used in AP1000

The major innovation of AP1000 reactor is the use of passive safety system that significantly reduce the core damage frequency (CDF) and allow the reactor to meet the NRC probabilistic safe criteria whit large margins

Passive safety systems maintain the core cooling and containment integrity with no operator action, even in case of loss of both off-site and on-site electric AC power supply. Safety Passive Systems are than able to guarantee an adequate reactor cooling in case of Total Station Black-out (Total SBO). The same situation leads to core damage in those reactors which use only Active Safety Systems (as EPR).
AP1000 is equipped with the Passive Core Cooling System, that has two main functions:

- Passive decay heat removal
- Passive safety injection

Passive decay heat removal is implemented by Passive Residual Heat Removal (PRHR) system which consists in a PRHR heat exchanger (PRHR-HX) located inside the IRWST and linked to the RCS. The PRHR-HX connects to the RCS by an inlet line from one of the cold-leg and an outlet line from one of the hot-leg. The water contained in the IRWST provides the heat sink for the heat exchanger. The PRHR-HX is elevated above the RCS loop to induce natural circulation flow when RCS pumps are not available.
The Passive Safety Injection System (PXS) is composed by:

- Core Makeup Tanks (CMTs)
- Accumulators
- IRWST.

CMTs function is to inject water inside RCS if inventory is being lost. The accumulators function is to inject water inside RCS if reactor cooling system pressure falls below accumulators pressure. PXS act together with the depressurization system valves (ADS) in order to reduce the RCS pressure up to a level that allow the accumulators and the IRWST (by the only action of gravity) to inject an adequate amount of water inside the primary circuit. It is required primary to mitigate Loss of Coolant Accident (LOCA).

AP1000 response to a SBO accident
Considering a Fukushima like event, with earthquake followed by flooding of the nuclear power plant, and assuming the most conservative situation, we consider all active non-safety related systems and those located outside the nuclear island lost.

- Loss of off-site power
- Loss of diesel generators
- Loss of non-safety related battery banks
- Loss of main and start-up feedwater system
- Loss of normal residual heat removal system.

It is also assumed the inoperability of the following safety system due to the flooding:

- Loss of class 1E battery banks
- Loss of Protection and Monitoring System (PMS).

After earthquake the reactor is automatically tripped; the SCRAM bring the reactor in a shut-down state. We also assume that all the passive safety systems located inside the containment

would resist to the earthquake and also that RCS would not be damaged by the seismic event (i.e. no LOCA occurred).
The residual heat generated inside the core after the shut-down must be removed to prevent core damage.
In case of Total Station Black-out the only system available to operate residual heat removal is the PRHR-HX. This is a passive system, so that no AC or DC current power supply is needed to guarantee its operability. The heat is transferred to the IRWST's water by the heat exchanger. The IRWST's water will reach the saturated temperature within few hours and the steam generated is released in the containment and cooled by PCCWST's (Passive Containment Cooling Water Storage Tank) water. The condensed water is collected and returned to the IRWST. The PCCWST's water has also the function of PCS (Passive Containment Cooling System), avoiding the over-pressurization of the containment for at least 3 days after the accident occurrence.
To prevent core damage is necessary the availability of the following systems:

- PRHR-HX
- Return paths of containment water to the IRWST
- One of the three drain paths of the PCS.

All these systems operate without any operator actions or necessity of electric power supply, thanks to AP1000 passive safety systems design.
In the event of PRHR-HX failure, causing the lacking of residual heat removal, RCS will over-pressurize. To prevent high-pressure core damage it is necessary a full depressurization of RCS operated by the ADS (Automatic Depressurization System).
Depressurization of RCS allows the safety injection of borated water from the ACCs and IRWST to the reactor. When the reactor cavity reach a designed level, the recirculation path is actuated for a long term cooling. As for the PRHR-HX success case, the reactor will be in a safety state for at least three days, assumed that the PCS is actuated.
In case of Total SBO (including also the 1E class battery failure), depressurization of RCS is manual actuated from DAS (Diverse Alternative Systems) instrument cabinet (supposed undamaged after a flooding + earthquake scenario).

The AP1000's core damage frequency due to a SOB accidental sequence are the follows:

- Core Damage with Reactor at High Pressure, due to PRHR's and ADS's failure:

  1.05E-7/r.y.

- Core Damage with Reactor Depressurization, due to PRHR's failure, success of ADS and failure of either IRWST's injection and reactor recirculation:

  2.33E-7/r.y.

7.2 Assessment of the consequences for reactors with passive and active systems

Let us compare the CDFs (Core Damage Frequency) due to SBO accident, for EPR (with active safety systems) and AP1000 (with passive safety systems):

- EPR: 5.0E-7/r.y.
- AP1000: 2.33E-7/r.y.

We can see that a passive safety reactor, as the AP1000, has a less Core Damage Frequency than an active safety reactor as the EPR. However the two values of CDFs are close enough to say that the two reactors have a comparable safety margin for a SBO accidental sequence.
The low value of SBO's CDF for EPR is due to the presence of 6 emergency diesel generators (4 EDGs + 2 SBODGs). to guarantee an adequate core cooling for at least 24h is sufficient the operability of only one of the six emergency diesel generators located in the nuclear power plant. The presence of a such high number of emergency generators devices makes very unlikely the contemporary unavailability of all of them.
The Fukushima accident has shown as a common cause failure, as earthquake and flooding of the nuclear power plant, can cause the failure of all the diverse electric AC power sources supplying the power plant (electric grid connections plus emergency diesel generators).
As consequence of this event result the unavailability of all the active safety systems necessary to guarantee an adequate reactor cooling, in order to prevent core damage.

8. Conclusions

Main focus of the present study is the evaluation of NPP active and passive system response to cope with safety relevant accident sequences, as emerging from the Fukushima Dai-ichi events analysis.
For this reason both active and passive systems designed to accomplish the required safety functions, as the decay heat removal, have been deeply investigated mainly in terms of their safety performance and reliability.
The analysis revealed some important insights, calling significant efforts to be invested in new projects to fulfil the ambitious safety goals.
With reference to passive systems, it is recognized that their reliability assessment is still an open issue, mainly due to the amount of concerned uncertainties, to be resolved among the community of researchers in the nuclear safety. Moreover a comparative analysis shows that their safety achievement is comparable to or even less than the active systems' one, since the claimed higher reliability and availability are challenged by some important functional aspects, impairing their performance.
Considering the results of the SBO's probabilistic safety assessment for EPR and AP1000 reactors, shown in the previous chapter, we can state that the safety levels reached by active safety systems reactors of GEN III+ (EPR) are comparable to those of passive safety system reactors (AP1000). However the EPR reactor is able to achieve these high safety levels by increasing the redundancy of the safety system. This is the case of EPR that has 6 emergency diesel generators (4 EDG + 2 SBODG) that supply electric power to the plant in case of LOOP, with a redundancy logic of 1:6. Increasing the redundancy causes the growing of the plant complexity (more components, more devices, etc...) that is itself a risk factor (it is more difficult to control the state of the plant).

Moreover the redundant safety devices are often of the same type (electric diesel generators to emergency power supply), so that a common cause of failure (as was flooding for Fukushima accident) is able to affect all the devices, causing the contemporary failure of all of them.
Finally we can state:

for Passive Safety Systems Reactors that:

- their claimed higher reliability and availability are challenged by some important functional aspects, impairing their performance.

for Active Safety System Reactors that:

- the higher level of redundancy causes an higher level of complexity of the plant, that is a risk factor itself
- using safety systems of the same type makes the plant vulnerable to common cause of failures.