EUROPEAN COMMISSION

Community Research

RAPHAEL

Contract Number: 516508 (FI6O)

DELIVERABLE (D-ST4.6)

Application of the PRA and RMPS methodology for modular HTR safety demonstration

Author(s): **J. L. Brinkman (NRG)**
E. van Wonderen (NRG)

Reporting period: 15/04/2006– 14/04/2007

Date of issue of this report : 15/12/2006

Start date of project : **15/04/2005** Duration : **48 Months**

Project co-funded by the European Commission under the Euratom Research and Training Programme on Nuclear Energy within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	
RE	Restricted to the partners of the RAPHAEL project	**X**
CO	Confidential, only for specific distribution list defined on this document	

Distribution list

Person and organisation name and/or group	Comments
Geutjes, A.J.: NRG	
Komen, E.M.J.: NRG	SINTER
Brinkman, J.L.: NRG	"
Manolatos, P.: EU	"
Bogusch, E.: AREVA GmbH	"
Chauvet, V.	"
Pirson, J.: SUEZ-TRACTEBEL	"
Parmentier, F.: SUEZ-TRACTEBEL	"
Ehster, S.: AREVA SAS	"
Mansani, L.: ANSALDO	"
Devictor, N.: CEA	"
Clément, C.: EDF	"
Carretero, J.: EMPRESARIOS AGRUPADOS	"
Carlsson, J.: JRC	"
Peers, K.: AMEC	"
Meloni, P.: ENEA	"
Coe, I AMEC	
Burgazzi, L: ENEA	

ReActor for Process heat, Hydrogen And ELectricity generation (RAPHAEL)		
Sub-project: SP-ST **Work package:** 4	**RAPHAEL document no:** RAPHAEL-0612-D-ST4.6	**Document type:** D=Deliverable
Issued by: NRG NL **Internal no.:** 21678/06.76914/C		**Document status:** Final

Document title

Application of the PRA and RMPS methodology for modular HTR safety demonstration

Abstract

In many innovative reactor designs (HTR / Generation IV) use is made of so called passive systems to mitigate the consequences of accidents. A characteristic of passive systems is that their operation is based on natural driving forces (circulation, convection, radiation, gravitation etc.) and usually need no active actuation to start the process. Disadvantage of these processes is that the magnitude of the driving force is often much less than in the case of active systems. Therefore passive systems are more vulnerable to external conditions or disturbances. This raises the issue of passive system reliability, one of the reasons to investigate whether or not the normal way of assessing the risks of nuclear reactors is also appropriate for reactors fitted with passive systems.
Hereto the currently used PSA methodology and analysis techniques for LWR have been applied on a (V)HTR.
It is concluded that the PSA methodology and analysis techniques are equally well applicable for (V)HTR reactors with build-in passive safety. Notwithstanding the foregoing, there are some issues that represent a departure from the traditional PSA assessment, that need to be resolved before a risk informed approach can be used.
The LWR Core Damage concept and its relelated risk figures Core Damage Frequency and Large Early Release Frequency can not be extrapolated to HTR.
Although the role of passive safety system reliability can be introduced without any problems in the generally applied static event tree/fault tree technique to model the course of accidents, the parctical way to assess the reliability of these passive systems or processes needs development.

Revisions

Rev.	Date	Short description	Author	WP Leader	SP Leader	Coordinator
			J.L. Brinkman, NRG	S. Ehster AREVA NP SAS	J. Pirson SUEZ TRACTEBEL	E. Bogusch AREVA NP GmbH
00	15/12/2006	First issue, for comments by WP4 partners				
01	10/04/2008	Comments processed FINAL			Carmen Angulo SUEZ TRACTEBEL 	

Contents

List of tables

List of figures

List of abbreviations

ACS	Active Cooling System
CCFP	Conditional Containment Failure Probability
CCS	Core Conditioning System
CDF	Core Damage Frequency
CRDM	Control Rod Drive Motor
EPS	Equipment Protection System
FHSS	Fuel Handling and Storage System
GBP	Gas Cycle Bypass Valves
GENIV	Generation 4 reactors
GFR	Gas cooled Fast Reactor
HCV	High pressure Coolant Valve
HICS	Helium Inventory Control System
HPB(C)	High Pressure compressor Bypass (Control) valve
HPT	High Pressure Turbine
HTR	High Temperature Reactor
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IE	Initiating Event
LCV	Low pressure Coolant Valve
LERF	Large Early Release Frequency
LPB(C)	Low Pressure compressor Bypass (Control) valve
LPT	Low Power Turbine
MPS	Main Power System
NUREG	Guide series of the U.S. Nuclear Regulatory Commission
OCS	Operational Control System
PBMR	Pebble Bed Modular Reactor
PCU	Power Conversion Unit
PSA	Probabilistic Safety Assessment
PT	Power Turbine
RBP	Recuperator Bypass Valves
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RPVCS	Reactor Pressure Vessel Conditioning System
RU	Reactor Unit
SAS	Small Absorber Spheres
SCWR	Super Critical Water cooled Reactor
SIV	Start-up blower system Inline Valve
RSS	Reserve Shutdown System
RCS	Reactivity Control System
RCCS	Reactor Cavity Cooling System
RCSS	Reactivity Control & Shutdown System
SBS	Start-up Blower System
VHTR	Very High Temperature Reactor

1 Introduction

In many innovative reactor designs (HTR / Generation IV) use is made of natural processes to mitigate the consequences of accidents. The main reason for this use is the small probability of failure that the required effect is not reached. These natural processes are denoted passive systems or components. A characteristic of passive systems is that their operation is based on natural driving forces (circulation, convection, radiation, gravitation etc.) and usually need no active actuation to start the process. Disadvantage of these processes is that the magnitude of the driving force is often much less than in the case of active systems. Therefore passive systems are more vulnerable to external conditions or disturbances of the process. This is one of the reasons to investigate whether or not the normal way of assessing the risks of nuclear reactors is also appropriate for reactors fitted with passive elements.

2 Goal

The purpose of the current analysis is to investigate if the normally used analysis technique can be used equally well on (V)HTR/GenIV reactors. In particular the ability of present PSA-1 techniques to incorporate the reliability of passive systems is investigated. Furthermore formal techniques to obtain lists of initiating events have been applied to a HTR to see if these techniques are just as well appropriate for these new designs. Finally constructing a complete list of initiating events for a (V)HTR reactor was considered valuable (in this case the design of the PBMR reactor has been the subject of investigation).

3 Scope

A normal PSA-1 analysis takes many months of work. As only the applicability of the PSA methods to (V)HTR/GenIV reactor is assessed, only part of the PSA-1 tasks have been performed in a limited way.

4 Method

The appropriateness of formal PSA-1 techniques has been investigated by applying these techniques to a (global) design of the PBMR reactor unit. By applying the consecutive steps systematically on this reactor including its passive safety systems, one can determine which steps cannot readily be executed or pose some problems. The main questions raised are:

1) Can current techniques to obtain a list of initiating events be applied for HTR/Gen IV reactors?
2) Does the initiating event list differ significantly from initiating event lists of existing reactors?
3) How should the failure of passive systems be incorporated in the usual event tree modelling?

Next to this the Level 1 - Level 2 distinction / transition has been addressed. In the IAEA "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level1) [1] and in NUREG report "A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants" [2] guidance is given on how to execute a PSA level-1 analysis. Using these reports the consecutive steps have been performed in a limited way for the PBMR design and the need for revision or extension of these tasks for this type of reactors is determined, in the light of the presence of passive systems that are considered inherently safe. The recommended tasks are as follows (tasks of importance are mentioned explicitly):

- Management and organisation (tasks 1 to 8)
- Identification of sources of radioactive releases and accident initiators (tasks 9 till 17)
- Task 9 Familiarization with the plant and PSA and information gathering
- Task 10 Identification and selection of site sources of radioactive releases
- Task 11 Determination and selection of plant operating states
- Task 12 Definition of core damage states or other consequences
- Task 13 Selection of initiating events
- Task 14 Determination of safety functions
- Task 15 Assessment of function/system relationships
- Task 16 Assessment of plant system requirements
- Task 17 Grouping of initiating events
- Event sequence modelling (tasks 18 to 23)
- Task 18 Event sequence Modelling
- Task 19 System modelling
- Task 20 Human Performance analysis
- Task 21 Qualitative dependence analysis
- Task 22 Impact of physical processes on development of logic models
- Task 23 Classification of accident sequences into plant damage states
- Data assessment and parameter estimation (tasks 24 to 26)
- Accident sequence quantification (tasks 27 to 31)
- Documentation of the analysis: display and interpretation of results (tasks 32 to 34)

5 PSA analysis steps

5.1 Plant familiarization and information gathering (task 9 IAEA)

Using open information sources insight is gained in the operation and function of several parts of the plant, front line systems and support systems, in as much this information was available for the 2001 version. Some parts like the reactor protection system are described only on a conceptual basis and the layout of the Main Power System has subsequently changed as a result of experience gained in the preliminary safety analysis.

5.1.1 The Fuel

The fuel sphere, which ranges 6 cm in diameter, exists of circa 15000 coated particles containing 9 gram of uranium, with an enrichment of 8%. Each coated particle (kernel) contains the fission fuel uraniumoxycarbide, a layer of porous carbon, 2 layers of pyrolytic carbon (with a very high density type of heat treated carbon) and a layer of silicium carbide (see Figure 1). The layers constitute a very solid primary barrier against release of radioactivity. The design accounts for a very low probability of releasing a significant amount of radioactivity up to some 1600ºC. The main reasons for emission of radioactivity up to 1200ºC are particles with defective layers or contamination with radioactivity (in the fabrication process). The probability of defective layers due to failures during the fabrication process of the fuel particles, complies with very high demands. Up to some 1600°C the probability of release increases due to diffusion processes. Above these temperatures the layers become more porous and can be breached as a result of pressure build-up of gases. In Figure 1 the fraction of failed particles is shown as function of the temperature.

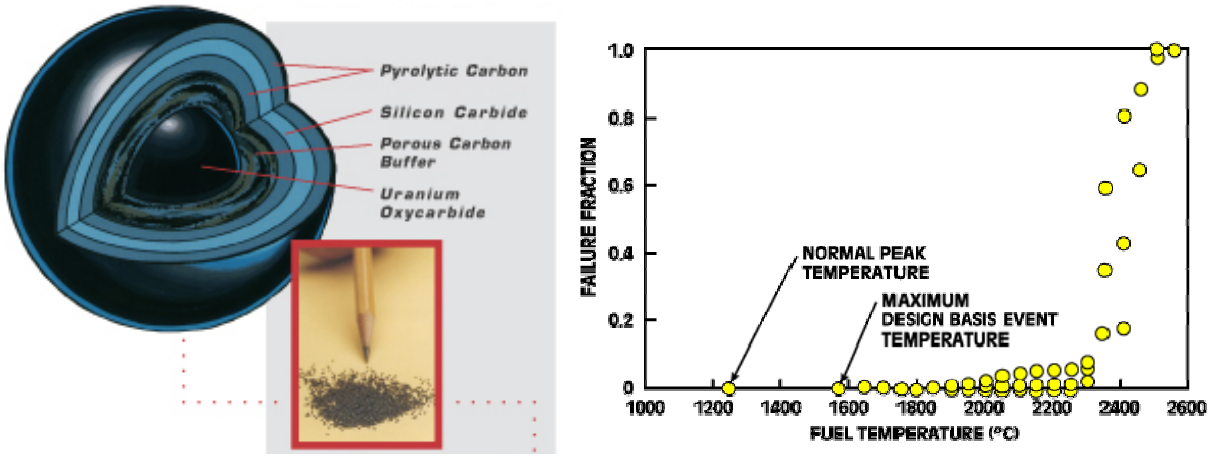


Figure 1 Design of a fuel particle and the failure fraction as function of the fuel temperature

5.1.2 Power Conversion Unit

The primary flow of the helium and thus heat transport from the reactor core is under normal circumstances established by the Power Conversion Unit (PCU), see Figure 2. The heated helium (ca. 900 ^{o}C) drives 2 turbine compressors (High Pressure Turbine: HPT and the Low Pressure Turbine: LPT), where 2 bypass valves are situated (version 2001).

Subsequently the Helium will flow through the gas turbine (Power Turbine: PT) and the recuperator to enhance the efficiency of the cycle. Then the flow passes the Start-up Blower System (SBS). This system is installed for the purpose of start up of the Brayton gas cycle, but is also the preferred way to provide for cooling capacity during shut down of the gas cycle or in case of turbine failure. Behind the SBS the pre-cooler, the LPT driven compressor, the inter-cooler and the HPT driven compressor are located. The flow path can be bypassed by the low and high pressure valve systems. The gas flow can be cut short by opening the Gas Cycle Bypass valves (GBP). The recuperator can be bypassed by opening the Recuperator Bypass valve system (RBP).

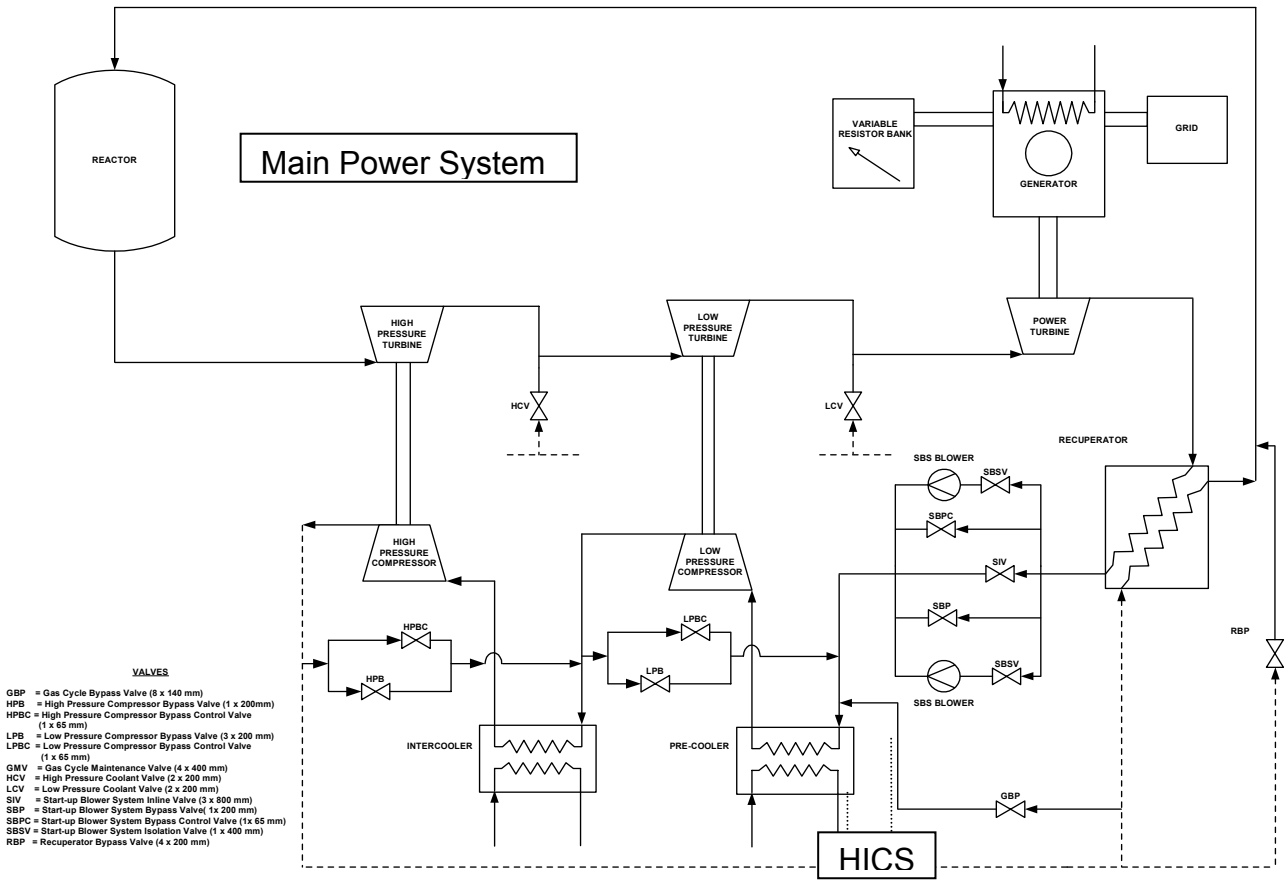


Figure 2 Main Power System (MPS) components

Also indicated is the Helium Inventory Control System (HICS). This system regulates the Helium pressure and is able to lower the inventory with 10%/minute (pump down) in the pressure range of 7 MPa (100% inventory, normal operation) to 2.8MPa (40%). In the lower pressure range the pump down rate is lower. Overpressure will be eliminated by using pressure release devices (2 devices with 2 different set points).

Under and on the top lid of the reactor vessel, the control rods are positioned including the accompanying Control Rod Motors, the Reactivity Control System (RCS) and the Reserve Shutdown Systems (RSS, 17 pieces). A reserve shutdown system contains boron filled absorber spheres (Small Absorber Spheres, SAS) which can be positioned in the side reflectors of the core. The Fuel Handling and Storage System (FHSS) has penetrations at the bottom side of the reactor vessel for the supply and removal of fuel and graphite spheres. Breach or leakage in one of these systems may lead to pressure loss. The position and extent of the leakage/break determines whether or not the helium loss can be isolated or compensated for.

The primary function of the Core Conditioning System (CCS) is to transfer decay heat when the Brayton cycle is not operational. It consists of 3 blowers (3*50%), a water cooler, recuperator and valves (see Figure 3). The task of the CCS is to keep the temperature of the reactor below 400^{o}C during maintenance conditions. When the SBS system is not available this system is also able to cool down the core, however with a much slower rate then the SBS.

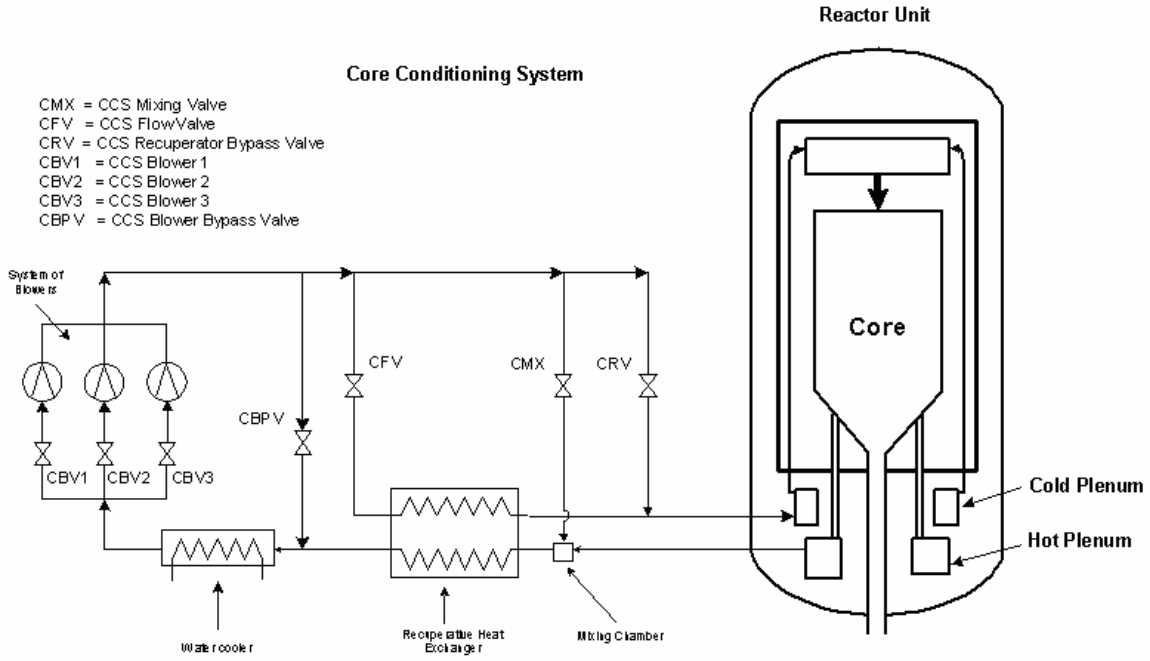


Figure 3 Core Conditioning System

The water coolers in both the PCU and the CCS operate with a much lower water pressure than the helium pressure so in case of a rupture or leakage cooling water can not penetrate the helium coolant system unless the helium pressure is low as a result of depressurisation accident or maintenance conditions. Pressure build up at the waterside of the heat exchangers is prevented by the use of rupture disks.

The Reactor Cavity Cooling System (RCCS) is a cooling system around the reactor vessel that cools the concrete walls of the cavity (see Figure 4), the reactor vessel and the RV supports. The functioning of the RCCS is based on the natural processes of heat transport (air convection and radiation) from the reactor vessel wall to the cooling panels of the RCCS. The RCCS consists of three independent, 100% capacity natural-convection driven cooling systems. In case all cooling units are lost, heat absorption will remain for up to three days due to heat up and boiling of the water in the system.

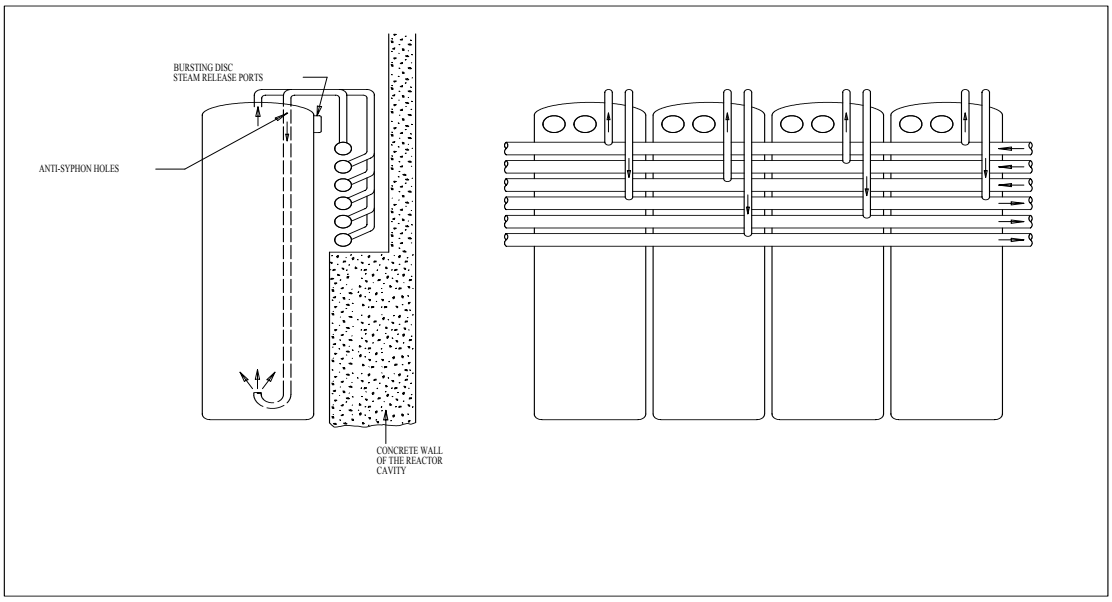


Figure 4 Reactor Cavity Cooling System

5.2 Determination safety functions (Task 14 IAEA, NUREG/CR-2300: 3.4.1)

The functions that must be performed to control the sources of energy in the plant and the radiation hazard are called safety functions:

- Reactor sub criticality;
- Heat removal
    - Secondary heat removal;
    - Primary heat removal;

- Containment[1] function
  - Maintain integrity of fuel particle
  - Maintain integrity of primary reactor coolant boundary;
  - Maintain primary reactor coolant inventory;
  - Maintain spent fuel cooling.

The main questions for this task are which (safety) systems are implemented and which safety functions are necessary to:

1) prevent that an Initiating Event (IE) leads to core damage (radioactivity release), and;
2) to minimise release of radioactivity as much as possible in case of an accident.

Table 1 Safety functions to prevent release of radioactivity

Safety function	**Purpose**
Reactivity control	Shut down reactor to decrease heat production / prevent power excursion
Reactor cooling system, Reactor coolant system inventory control	Maintain coolant medium in the core (maintain coolant medium in proper state)
Reactor coolant system pressure control (maintain integrity of primary reactor coolant boundary)	Maintain pressure coolant within required margins
Core heat removal	Transfer heat from the core to the coolant
Reactor coolant system heat removal	Heat transfer from the coolant to the conversion unit or heat sink
Confinement isolation	Close openings in the insulation to reduce radionuclide releases
Confinement temperature and pressure control system	Prevent damage to confinement and equipment.
Combustible gas control	Remove and redistribute hydrogen to prevent explosion inside confinement
Reduction radioactivity	Scrub radioactive materials from confinement atmosphere

The design of the PBMR discussed here no pressure containment is present. It has however a concrete building (confinement), which is not leak tight but provides for a certain mitigation of releases of radionuclides during accident conditions. A helium leak up to a certain magnitude can be released and filtered through the ventilation system. Greater leak rates will be released without filtering. As no accidents are expected to produce a significant amount of burnable

[1] Containment are all barriers between fuel and environment. It is NOT restricted to the building.

gases (hydrogen, carbon monoxide, graphite dust), the design does not contain burnable gas igniters or recombiners.

In Table 2 the available safety systems (front line systems) of PBMR are mentioned, in relation to the required safety functions (dependency matrix safety function versus front line systems).

Table 2 Safety function and corresponding front line systems

Safety function	Front line system
Reactivity control	Reactor Protection System (RPS) Reactivity Control & Shutdown System (RCSS)
Reactor coolant system inventory/pressure control (maintaining integrity PPB)	Helium Inventory Control System (HICS) Safety Relief Valves
Core heat removal	Core Conditioning System (CCS) Reactor Cavity Cooling System (RCCS) Reactor Pressure Vessel Conditioning System (RPVCS) "Natural conductivity, radiation (and convection)"
Reactor coolant heat removal	Power Conversion Unit (PCU) Start-up Blower System (SBS) in combination with heat exchangers
Filtering / isolation	HVAC / Isolation valves HICS/FHSS

5.3 Selection of initiating events (task 13 IAEA)

5.3.1 Definition of core damage

The investigation into initiating events is in general focussed on those events that have the potential to lead to large releases of radioactivity as in the past surrogate risk figures (CDF, LERF, CCDF) have been defined for LWR's based on the paradigm that the assiociated risk is negligible when fuel integrity is preserved [10]. For the present design of water-cooled reactors the definition of an initiating event is therefore as follows: an initiating event is an event that causes a disturbance in the plant and has the potential to cause core damage. The traditional end point of a level 1 PSA is core damage. This end state of core damage is clear in a PWR/BWR. For an (V)HTR, however, this is not straight forward as the design makes the large scale phenomena as in PWR's/BWR's virtually impossible. The low energy density of PBMR and (large) negative temperature coefficient are aimed at making it impossible to reach high temperatures of the fuel and therefore prevention of release of large quantities of radioactivity under any possible circumstances. Thus, the Core damage concept cannot simply be extrapolated to HTR. An alternative definition of the CDF term is necessary.

Experiments with fuel spheres however have shown that elevated fuel temperatures above the design temperature for considerable periods of time lead to relative small releases of radioactivity in ideal conditions. This would imply that, perhaps, only a very limited number of accident scenarios need to be considered in the PSA to show compliance to governmental risk criteria if any. If the PSA is made with a broader intention, for example to optimise the design, for risk centred maintenance, economic risk or risk based inspection etc., also (very) low release accident scenarios could be included (in which fuel temperatures remain well below 1600^{o}C but above peak temperature). Detailed analyses (thermo-hydraulic analyses) may show that part of these accident scenarios could be screened out because of very low probabilities or assigned to a no-release (insignificant release) category.

As a starting point one could opt for the definition that a fuel temperature above the absolute maximum design temperature (peak temperature) for an individual fuel sphere in normal operating conditions is considered a non-successful end state ("core damage"). This corresponds with the definition used to obtain the list initiating events, where the term "abnormal" or "accidental" condition is used.

An end state in which the fission power not equals zero could also be regarded as a non-successful end state. In that case namely, one could argue that an abnormal situation exists, i.e. the reactor is still not fully under control. The outcome of the event trees depends of course on the time duration of the accident analysis (1 day or 3 days for example).

In [10] a Release Frequency - Consequence curve is suggested as risk criterium.

In this document the following definition of an initiating event is used: each event that leads to an abnormal or accident condition is considered an initiating event. In other words every event that leads to a response of a safety system is treated as an initiating event.

5.3.2 Methods to obtain a list of Initiating Events

To obtain a list of initiating events which is as complete as possible, four methods are recommended:

1) Engineering evaluation,
2) Use earlier produced lists,
3) Master Logic Diagram and
4) Operational experience.

In the following the first three techniques have been applied to the PBMR design with focus on the main process[2]. Engineering evaluation and the use of earlier produced lists are, however, applied in a limited way. It will be clear that Operational experience is not an option.

5.3.3 Engineering evaluation (NUREG/CR-2300: 3.4.2.1)

In this technique all possible (partial) failure modes of all systems (operational plant systems, safety systems) and components that can lead directly or indirectly to accident conditions, also in combination with other failures or problems, are assessed. All disturbances that lead to a scram are of course also initiating events.

Common cause failures require special attention. This relates to simultaneous failure of several identical components by a common cause. The common cause may for example be design deficiencies, procedural errors during maintenance or environmental conditions such as a high temperature.

Per system, each failure mode that might lead to abnormal or accidental conditions possibly in combination with other disturbances should be identified. In Table 3 the most important components are analysed in this way. The events identified are traditionally categorised in a number of classes: Loss of Coolant Accidents (LOCA's), Transients, external events and area events. For PBMR, Loss of Coolant Accidents should be interpreted as loss of (a part of) the helium inventory.

Considering LOCA's, the entire reactor cooling system and associated interfaces with other systems should be investigated in terms of possible leakages or breaches or opening of systems, which could lead to loss of coolant. In many cases the several LOCA types are reduced to 3 or 4 cross sectional opening sizes, based on the demands on mitigating systems. This is also applicable for the PBMR.

Table 3 Engineering evaluation of important parts

Component	**Hazard /problem / transient**	**Response/consequence**
Fuel	temperature increase / oxidation	increased probability of radionuclide release
(top-)Reflector	displacement	change reactivity / fuel temp

[2]: Besides the core / primary system, there are some other systems containing radioactivity: the Spent fuel system, the Used Fuel system and the Waste Storage Tank. In a full PSA, initiating events in relation to these systems should be incorporated.

Component	Hazard /problem / transient	Response/consequence
Core	displacement / compacting	idem
Core support	failure	idem
Reactor Pressure Vessel	rupture / leakage	depressurisation, ingress of air
Piping / Seals / Primary Pressure Boundary (cross duct / RPVCS)	rupture / leakage	depressurisation, ingress of air
High Pressure Turbine / High Pressure Compressor	inadvertent trip / breakdown	change in flow/temp
Low Pressure Turbine / Low Pressure Compressor	inadvertent trip / breakdown	change in flow/temp
Power Turbine	trip / breakdown / cooling failure / leakage	change in flow/temp depressurisation
High/low Pressure Coolant Valves (HCV / LCV)	Inadvertent opening	change in flow/temp
Recuperator	Leakage / rupture / blockage	depressurisation / He-flow decrease
Recuperator Bypass Valve	Inadvertent opening	efficiency reduction / trip
Start-up Blower System (SBS)	Spurious activation	Increase He-flow
SBS	inadvertent trip / breakdown (at shutdown)	loss cooling capacity
High Pressure Compressor Bypass (Control) Valve (LPB/LPBC)	spurious opening	change in cycle temp / pressure / rotational speed turbo units (stop cycle)
Low Pressure Compressor Bypass (Control) Valve (LPB / LPBC)	spurious opening	idem
Gas Cycle Bypass Valve (GBP)	spurious opening	idem
Intercooler	rupture/leakage/blockage	depressurisation/flow & heat removal decrease
Pre-cooler	rupture/leakage/blockage	depressurisation/flow & heat removal decrease

Component	Hazard /problem / transient	Response/consequence
Pressure Relief Valves	inadvertent opening	depressurisation
Generator	breakdown / trip	load rejection
HV breaker	inadvertent opening	load rejection
Variable Resistor Bank	inadvertent actuation	PT trip
Grid / auxiliary power	failure	load rejection
Helium Inventory Control System	loss of control / leakage/rupture	In- or decrease inventory / depressurisation
Core Conditioning System	leakage / rupture /loss of control	depressurisation / cooling capacity in- or decrease
Reactor Pressure Vessel Conditioning System	inadvertent trip / breakdown	RPV temp. increase
Reactor Cavity Cooling System	inadvertent trip / breakdown	RPV (support) temp. increase
Reactivity Control and Shutdown System	spurious operation	change reactivity / shutdown
Equipment Protection System	spurious operation	stop cycle / shutdown
Active Cooling System	Leakage/ rupture /blockage	change water temp, change cooling capacity He-water heat exchangers
Fuel Handling and Storage System	leakage / rupture / blockage / loss of control	depressurisation / reactivity in- or decrease
Computer control (RPS)	inadvertent operation	In- or decrease inventory/reactivity trip

5.3.4 Reference to previous lists

Existing lists may be used as a starting point. The lists should be screened on appropriateness in relation to actual design of the plant or external conditions. In the reports NUREG/CR-2300 [2] and IAEA safety series [1] a number of generic lists are presented. In appendix A these lists are shown. The applicability of each event to the actual design is considered.

Unique systems, especially passive processes or systems like the RCCS have no equivalent in the generic lists in terms of coolant flow/capacity/loss or reactivity and are therefore not produced by this method.

5.3.5 Master Logic Diagram (NUREG/CR-2300: 3.4.2.2)

A master logic diagram (MLD) is a tool in identifying initiating events and ensures to a high degree the completeness of the analysis. It is a top down approach in that it starts with consequence: for instance radioactive releases to the environment. The upper part of this MLD is reproduced in figure 5 for illustration purposes. The complete analysis can be found in [9].

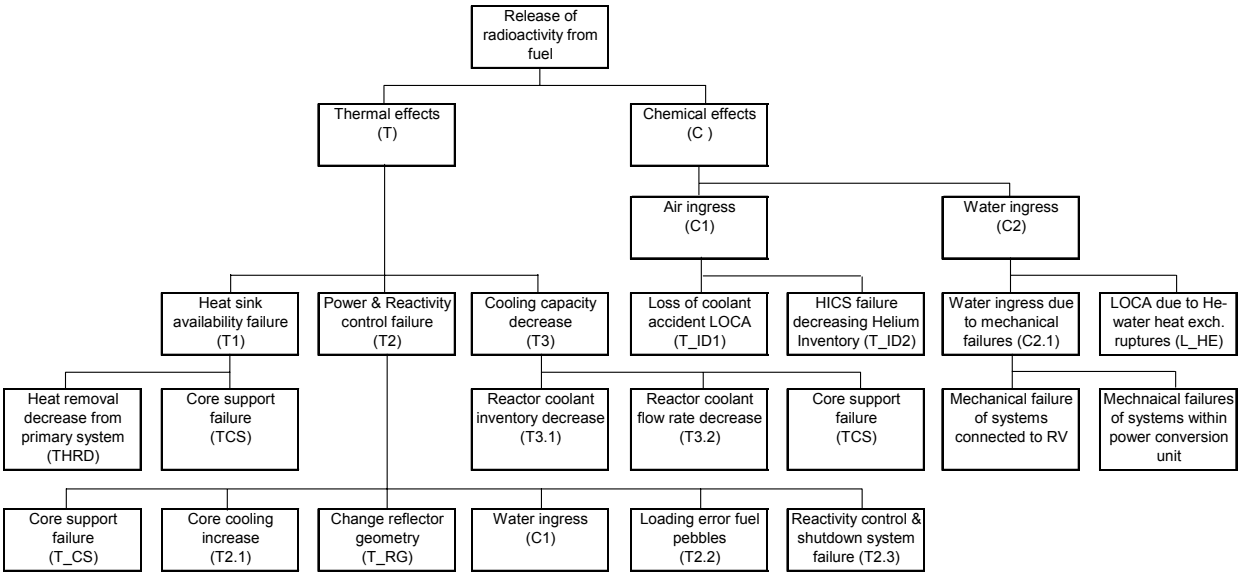


Figure 5 Upper part of the Master Logic Diagram

In this case the starting point of the analysis is the release of radioactivity from the fuel particles. This event is subsequently subdivided in all possible scenarios that can lead to this event. Successful operation of safety systems and other mitigating action should not be considered. The events at the lowest level are candidates for the list initiating events. The events considered are mainly focused on those occurring during normal operation of the plant (including operation at power, reactor shutdown and refuelling). There are several scenarios for pebble bed reactors that may increase the likelihood of emission of radioactivity (challenge of the first barrier, the fuel particles confinement):

1) Chemical Effects [C];
2) Thermal Effects [T].
3) Mechanical effects;
4) Manufacturing defects.

Major source of activity is likely to be activated carbon dust – fission product releases are likely to be much smaller

In the analysis all events that also challenge the second barrier (the primary system) are also taken into account. Events that may breach the third barrier (the containment / confinement building) are not analysed as this is out of the scope of this report. All identified initiating events are listed in appendix B.

Due to the structured way of analysing, the probability of missing initiating events is minimised.
The technique shows to be well suited to obtain a comprehensive list of initiating events for this type of reactor including its passive features.

5.3.6 Operational experience

In this approach, the operational history of the plant (if any) and of similar plants elsewhere is reviewed for any events, which could be added to the list. This approach is considered only supplemental, as it is not likely that it will reveal low probability events.

5.3.7 Summary on initiating events

Summarizing the results of the techniques mentioned above leads to a list of initiating events that are considered applicable on the PBMR design, as shown in Table 4. Appropriateness of certain events is of course dependent on the (final) design of the plant.

Table 4 List of initiating events for PBMR

Inventory
Loss of Inventory (Large / medium / small LOCA) caused by tube ruptures, RPV failure, PPB failure (ingress of air, water)
Leakage/seal failure/break in HICS/HPS/CCS/FHSS/RPVCS
Leakage from control rods (CRDM seal failure / control rod ejection)
Inadvertent opening of a safety/relief valve (stuck)
He/water heat exchanger leakage/rupture (depressurisation / ingress of water)
HICS Pressure regulation fails: inventory decrease /depressurisation
HICS Pressure regulation fails: inventory increase
HICS Pressure regulation fails closed
Turbine
Electric load rejection (HV breaker opening / generator trip or faults)
Electric load rejection with gas cycle bypass valve failure
Turbine trip (loss of offsite power / cooling water / Resistor Bank)
Loss of turbine (bearing / blades/ shaft / disk etc.)
Turbine trip with gas cycle bypass valve failure
Flow
Control valves malfunction cause increase/decrease in pressure and flow:
Gas cycle Bypass Valve (GBP)
High/low Pressure coolant valve (HCV/LCV)
Recuperator bypass valve (RBP)
Start-up blower system inline valves (SIV)
High/low pressure compressor bypass control valves (HPBC/LPBC)
High/low pressure compressor bypass valves (HPB/LPB)

Table 4: List of initiating events for PBMR (cont.)

He-water heat exchanger (Intercooler/Pre-cooler/CCS) He-flow decrease
Flow decrease (blockage) recuperator
Inadvertent operation SBS at power
Trip/loss of High Pressure compressor/turbine
Trip/loss of Low pressure compressor/turbine
Trip of both turbo compressors (HPC and LPC)
Low helium flow during startup or shutdown (SBS failure)
High helium flow during startup or shutdown (SBS failure)

Heat removal
He/water heat exchanger(s) water flow decrease (blockage): He-temp increase
He/water heat exchanger(s) water flow increase: He-temp decrease
He/water heat exchanger(s) water flow temp increase/decrease: He-temp change
Loss of generator cooling (leakage / loss of water flow)
Loss of active cooling system ACS (heat sink)
Loss of Core Conditioning System (CCS) (at shutdown)
Inadvertent operation of CCS at power
Loss of Reactor Cavity Cooling System (RCCS)
Loss of Reactor Pressure Vessel Conditioning System (RPVCS)
HE channel blockage

Reactivity control
Uncontrolled Rod (group) withdrawal/insertion at power
Uncontrolled Rod (group) withdrawal in accident event (re-criticality)
Uncontrolled SAS removal/insertion from reactivity control system
Uncontrolled SAS removal/insertion from cold shutdown system
Inadvertent reactivity control unit actuation
Uncontrolled fuel loading (mix up of spheres, detection errors)
Blockage of fuelling pipe
High flux due to rod/SAS withdrawal at startup
Pressure, temperature, power imbalance--rod/SAS-position error
Reflector geometry modification (top reflector drop)

Scram due to plant occurrences
Spurious trip via instrumentation, RPS /EPS /OCS fault
Detected fault in reactor protection system
Loss of computer control (RPS)
Manual scram--no out-of-tolerance condition

Internal/External events
Loss of offsite power
Loss of auxiliary power (loss of auxiliary transformer)
Loss of DC power bus(es)
Heavy Load Drop
External explosion
Seismic event
Core structural support failure
Aircraft crash
(Turbine) Missiles / Projectiles
Floods
Fire within plant

The procedures to obtain the list of initiating events seem to be equally well suited for PWR's/BWR's as for HTR. No significant problems or inconsistencies have been encountered. This shows that application of these techniques on reactor designs with passive systems (Generation IV) is appropriate.

5.4 Grouping of initiating events (task 17 IAEA)

The initiating events can be grouped in such a way that all events in the same group impose essentially the same success criteria on the front line systems as well as the same special conditions (challenges to the operator, to automatic plant responses, etc.) and thus can be modelled using in principle the same event/fault tree analysis.

Of primary importance is the question whether or not the Primary Pressure Boundary (PPB) is breached. If the PPB remains intact, no radioactivity release to the confinement will take place. Breach of the PPB will lead to filtered or unfiltered venting to the environment of the helium with a certain amount of radioactivity. The amount of helium released depends on the possibility of isolating the release (i.e. closing of valves or even the release opening).

All other events will challenge the reactivity control system and heat removal capability. For these events elevated temperatures of the fuel may lead to an increased concentration of radioactive materials in the helium, but will in principle not be released to the environment. If they do lead to a PPB breach (opening of safety valves for instance) they should be transferred at a certain stage of the accident delineation to one of the LOCA categories.

The following groups of initiating events can be distinguished for use in the event tree development:

- LOCA's
  - Large LOCA, non-isolatable
  - Large LOCA, isolatable
  - Intermediate LOCA, non-isolatable
  - Intermediate LOCA, isolatable
  - Small LOCA, non-isolatable
  - Small LOCA, isolatable
- Transients:
  - No heat removal from core (Loss PCU & CCS)
  - Decreased heat removal from core / RPV
  - Power/reactivity increase
  - Miscellaneous

The initiating events in Table 4 can be assigned to one of the event groups, as shown in appendix D. The grouping is a straightforward process independent of reactor type.

5.5 Accident Sequence Modelling (task 18 to 23 IAEA)

In task 18 to 23 the response of the plant on each group of initiating events is established using accident sequence modelling. The end points of each event tree in the level I PSA's of PWR/BWR are in principle a successful end state or an end state with core damage. In case of a HTR like the PBMR two points that are interrelated need some consideration:

1 Definition of Core Damage, see the discussion above in paragraph 5.3.1;
2 Level 1 and 2 issue.

5.5.1 PSA level 1 and level 2

In a Level 2 PSA of BWR/PWR the end point of the Level 1 PSA (core damage) is a more or less an intermediate result. Ultimately, attention is focussed on (large) releases of radioactivity: without Core Damage no large releases. Based on the specific initiating event and the availability of safety systems, the occurrence frequency of radioactivity release from the fuel elements is determined. Hereto success criteria are used, often based on thermo hydraulic analyses.

Eventually this PSA-1 step leads to a considerable number of accident sequences with respect to the status of the core, the reactor vessel, and plant systems. Subsequently an analysis of plant damage states is conducted. In this analysis sequences are clustered based on the damage state of the plant: availability of safety systems, status of the reactor vessel and fuel and the status of the containment barriers. In the level 2 analysis, the continuation of the accident is modelled based on the plant damage state primarily with regard to the containment response, by in principle expanding the level 1 event trees. Eventually this leads to a number of source terms that can in turn be binned into a smaller number of release categories.

This whole process itself from initiating event up to release categories is independent of the fact that core damage can occur. How releases are accomplished - molten fuel, cracked fuel, other sources like dust, is not relevant for the analysis method. Therefore a Level 2 analysis for a (V)HTR is straight forward and no changes in the methodology are needed.

5.5.2 Accident delineation

The following primary systems (front line systems) are important:

- RCS/RSS (Reactivity Control System / Reserve Shutdown System)

- PCU (Power Conversion Unit)
- SBS (Start-up Blower System)
- CCS (Core Conditioning System)
- RCCS (Reactor Cavity Cooling System)
- HICS (Helium Inventory and Control System)

Recovery of these systems after initial unavailability may have a significant influence on the course of the accidents. Although recovery of systems normally is not modelled except for Loss of Offsite Power, taking it into account in the event trees as separate heading events is no problem.

The following systems and recovery actions play an important role in the development of the accident (that is the magnitude of the releases):

- Detection systems of helium leakages
- Possibility of isolation leakage/breach (closing valves)
- Possibility of closing (repairing) the leak opening
- Availability and status of the ventilation system (HVAC)
- Opening overpressure valves and possibility of re-closing these valves (confinement).

The headings of the event trees will thus be formed by a number of these systems or actions. The end states of the event trees are determined by the initiating event, the status and availability of various plant systems (safety systems, support systems, detection systems) and human action as a function of time.
A complicating factor in the modelling of the accident progression is that there may be the possibility of recovery during the course of the accident. This is due to the long period (slow development) of the accident progression (several days), allowing (in some cases) closing of the LOCA opening and establishing forced cooling or closing of the ventilation valves of the HVAC system, preventing further unfiltered release to the environment. The moment in time that isolation will take place (few seconds, minutes or hours) will have a large impact on the amount and timing of the helium release and associated radioactivity release. It must also be considered that there is the possibility of incorrect operator actions making the sequence worse and the modelling of the accident progression over extended periods must include accident management measures as it is inconceivable that no efforts would be made to attempt to recover the situation.

Another important point here is the incorporation of the passive systems in the accident sequences. This will be elaborated in the next paragraph.

5.5.3 *Passive systems*

The term passive system is generally used for systems that perform a certain safety function using a natural process without the support of other operational systems or human action.

In a publication of the IAEA [4] one defines passive systems as systems that have no need for external input, especially energy, to be able to operate. In this reference passive systems are divided in four categories:

a. physical barriers and static structures (characteristics based on material, condition, design and geometrical placement)
b. movement of fluids/gases (due to phase changes, chemical reactions or neutron flux effects)
c. moving of mechanical parts (for example the opening of a spring loaded check valve as a result of a pressure difference)
d. external signals and potential energy (passive action / active actuation)

Usually passive systems refer to the systems/processes of type b.

An important question is how success or failure of passive systems should be incorporated in a PSA-1 analysis. In case of active systems there are only two possibilities; the system operates or it fails (binary logic). If there is mention of more than one component in an active system (there are for example 3 available pumps) the success of performing a safety function is based on design criteria or on detailed thermo-hydraulic analyses, which determines the number of components necessary to perform the required safety function. Based on this information a fault tree is established which assesses the probability that the required number of active components is not available.

In relation to passive systems two problems may occur that are currently under investigation: the passive system does not function at all (the desired operation does not start due to physical processes or conditions) or is being hampered (the function is degraded). In case of degradation the duration of the problem is of importance besides the magnitude of the degradation. The seriousness of the degradation depends heavily on the operating conditions (temperature, pressure and flow ranges of diverse interacting systems in which the passive system should operate). Therefore there is no simple one to one relation between defined success criteria and the probability of compliance of the passive system.

In a branch of the event tree, the probability of a system (or action) not being available is in general quantified by a fault tree. The establishment of the fault trees is termed "Systems Modelling" (task 19 of the IAEA guideline).

Using a certain definition of failure (or success criteria), it seems possible to assess the probability of failure of a passive system by thermo-hydraulic simulation given foreseen margins of the process conditions and uncertainties in the parameters. In that case there is no problem incorporating the passive system within the classical event tree approach.

Within the framework of the 5th FP RMPS project, a methodology has been developed to evaluate the reliability of passive systems characterized by a moving fluid and whose operation is based on physical principles, such as the natural circulation (see appendix E). The reliability evaluation of such systems is based in particular on the results of thermal-hydraulic (T-H) calculations. This methodology can be structured in three parts:

- Identification and Quantification of the sources of uncertainties;
- Reliability evaluations of passive systems using techniques use in Structural Reliability analyses;
- Integration of passive system reliability in Probabilistic Safety Assessment.

The last item is not fully developed. A way of incorporating passive system reliability in the PSA that is consistent with current standards is given in the next paragraph.

5.5.4 Example of incorporating a passive system in an event tree

The safe operation of the PBMR is based on four passive forms of mitigation:

1) Shutdown of the reactor based on the intrinsic negative temperature coefficient
2) Natural heat transport from the core to the surroundings by conduction, heat radiation and convection (if there is sufficient helium pressure)
3) Heat absorption and removal by the reactor cavity cooling system
4) Heat absorption by the concrete of the building

In Figure 6 an example is given how could be incorporated in a part of the event tree. In this example one passive process and one passive component is considered. The passive process concerns heat transport from the fuel spheres to the environment (core support structure, reactor vessel, air in the cavity and the water chambers of the Reactor Cavity Cooling System) by conduction, heat radiation supplemented with convection if here is enough helium pressure. The component that can be operated passively is the Reactor Cavity Cooling System itself. The RCCS consists of 45 water chambers, which are situated around the reactor vessel. By each

pump (2001 situation, 3 in total each 50%) water is pumped through this system and the heat absorbed is dissipated in the Active Cooling System (ACS). In case of pump failure the water in the associated water chambers will heat up and the pressure rise will lead to breaking of a rupture disk. The passive heat removal remains intact, as long as there is sufficient water in the water chamber. Actually besides the passive heat absorption of the RCCS the passive heat absorption of the concrete walls could be modelled. In case the RCCS boils dry or in the case the water content is lost early in the accident scenario (for example by a large earth quake) then the concrete of the reactor cavity will absorb a large portion of the heat produced during the course of the accident.

The first heading related to passivity in the event tree concerns the event that there is a situation of reduced heat transport from the core to the environment (by conduction, heat radiation or convection). The other relates to reduced heat removal by the RCCS.

In the case the Start-up Blower System (SBS) or the Core Conditioning System (CCS) (both systems are able to remove heat from the core) is functioning, it is assumed that the fuel temperature will remain within the "normal" operating range (below peak temperature). In all other cases there will be a (clear) elevated fuel temperature. This situation is indicated with the term "Core out of specification", COOS. In case of an elevated fuel temperature (say above 1200 ^{o}C during a longer period) there is small emission of radioactivity from the fuel spheres, primarily as a result of defective fuel particles. Only in case of leakage/rupture of the Primary Pressure Boundary or supporting systems like the "Fuel Handling and Storage System" or the "Helium Inventory Control System", there is a possibility of a filtered or unfiltered release path to the environment.

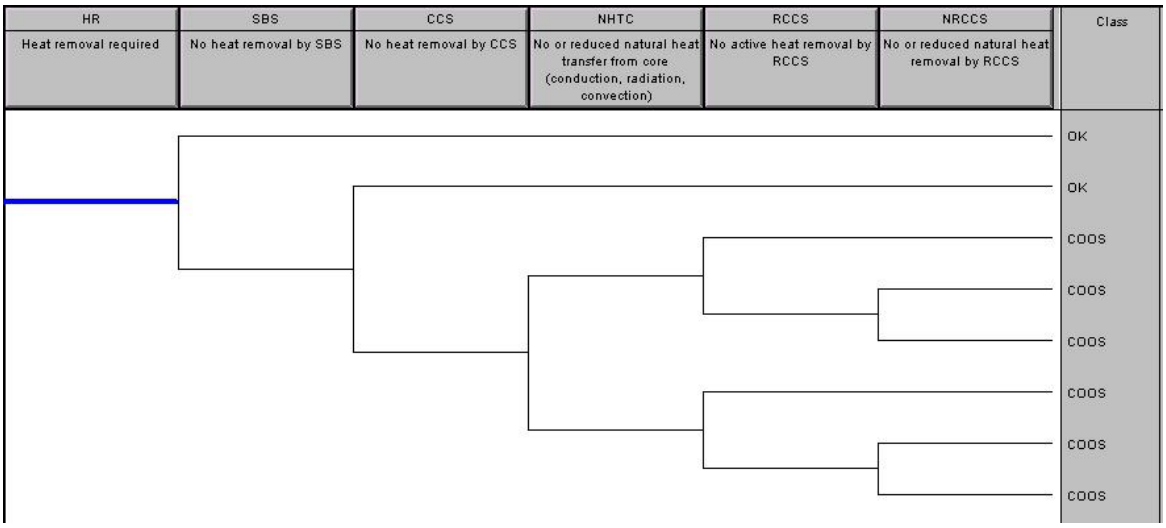


Figure 6 Event tree with passive components/systems

The specific features of passive systems can be incorporated in the event tree by using more branches under one heading or by splitting the system over more than one heading (see Figure 7). Based on the thermo hydraulic analyses, the probability that the passive system is capable of removing a certain percentage of the produced heat and therefore maintain the fuel temperature below a certain level, can be determined. In figure 7 distinction is made between 4 possible fuel temperature ranges: below 1200C, between 1200C and 1350C, between 1350C and 1600C, and above 1600C. Depending on the specific conditions associated for instance with the initiating event, the three branch probabilities could vary or a probability density function giving the probability as function of performanceof the passive system.

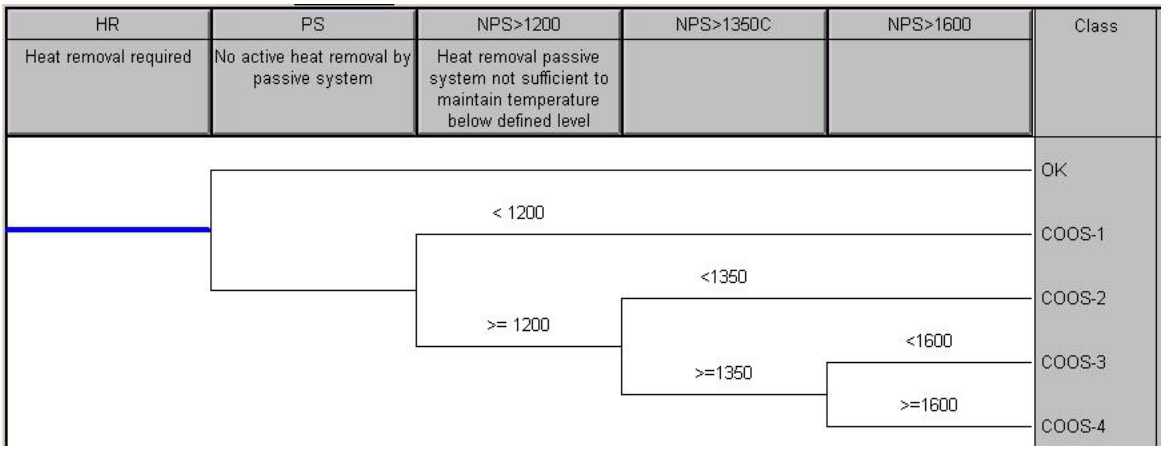


Figure 7 Part event tree depicting 4 system states for a passive system

5.5.5 Event Sequence Modelling PBMR

Based on the groups of initiating events the event tree model can be made using the systems or functions as headings in the trees. For one of the initiating event groups such a tree has been made as an example, without expanding on the subject of passive systems.

LARGE LOCA

In case a large isolatable LOCA (opening size diameter 20cm) takes place the mass flow is high, initially some hundred or more kilograms per second, the actual release rate is dependent on friction and density (temperature) of the gas. As the gas pressure decreases rapidly the release rate also decreases. In a few minutes however a significant part of the entire inventory of the PCU (4500kg) may be released. For an opening size of 6,5 cm it takes some 10 minutes to release upto 90% of the PCU inventory. This shows that pump down has no influence on the large LOCA sizes.

In the first release only the activity already contained in the helium is released (unfiltered), including (resuspended) dust. If the release takes place in the HICS/FHSS system, successful prompt closure of valves will assure that the inventory of the MPS system will not be totally released and cooling can be assured.

In a preliminary version of the PBMR Safety Analysis Report it is shown that in the worst case scenario (depressurised loss of forced cooling) it takes some 12 hours before the maximum pebble fuel temperature in the core reaches the level of 1300^{o}C and some radioactivity release from the fuel will commence as a result of defective particles. A fraction of this radioactivity will eventually escape from the PPB (due to slight differential pressure effects or convection). The delayed release could effectively be stopped if in the mean time the opening could be closed by repair (and some cooling re-established). Finally manual closure of the direct vent path to environment (after the large release is below a certain rate) will assure filtering of the remainder of the release.

In summary the following aspects determine the release:

- Availability RCS
- Prompt isolation of HICS/FHSS system
- Delayed closure of release opening (and probable re-establishment of cooling)
- Closure of direct venting path, re-establishing filtration of confinement atmosphere
- Availability of cooling capacity

In appendix B the event tree made based on the items mentioned above, is shown.

5.6 PSA Level 2/3

In the level-2 analysis a grouping is performed (called source term binning) to obtain a reasonable number of release categories to be evaluated in the level -3 environmental consequence analysis. The most important issue in determining the consequences in the environment as a result of accidents is the release magnitude of the radionuclides as a function of time.

Release categories

The most important matter in the release categories (or source term categories) is of course the magnitude and timing of the various radionuclide releases. This has to do with decay rates of various fast decaying radionuclides (like some of the noble gases) and distribution of nuclides in the environment. Of some importance is the energy (heat) content of the release as this

determines to a certain extent how far the plume rises in the atmosphere and subsequently the concentration distribution.

The release can be subdivided in essentially two release phases; the first release phase in which the system is depressurised and a second phase in which a slow release occurs during heat up of the core and subsequent expansion of the helium. The first phase contains the radionuclide concentration already present in the helium (gases and dust). The second phase contains additional radionuclides as a result of the fuel temperature rise (basically due to defective fuel particles). The amount of radionuclides released in the first phase is directly proportional to the total mass helium released and the possibility of filtering. The radioactivity content of the second release is primarily caused by the fuel temperature distribution (as a function of time) and the ability to filter the release. Therefore the source term binning scheme in Table 5 seems adequate. A more sophisticated scheme could contain a subdivision related to functioning of the RCS, the manual closure of the open vent to the environment (in case of a large early release) and the time point the LOCA opening is repaired.

Table 5 Binning scheme

Early phase	Late phase
Large amount unfiltered	Unfiltered (no manual closure)
Medium amount unfiltered	Filtered
Medium amount filtered	No release (closure of opening)
Small amount filtered	

6 Conclusions

The purpose of the current analysis is to investigate if the currently used PSA analysis techniques for PWR/BWR can be applied just as well on (V)HTR/GenIV reactors that make use of natural processes or passive components to reduce or prevent the consequences of accidents to the environment.

The PSA methodology and analysis techniques are equally well applicable for (V)HTR reactors with build-in passive safety:

1) The way in which initiating event list are established: the "master logic diagram" method, the use of reference lists, the "engineering evaluation" and use of operational experience, are appropriate;

2) The generally applied static event tree/fault tree technique to model the course of accidents is applicable by introducing the passive component or process in the event tree.

3) The meaning of a separate Level 1 analysis is limited, as core damage in the classical sense is non- or practically non- existent.

4) A Level 2 and Level 3 analysis can be conducted without any problem.

Notwithstanding the foregoing, there are some issues that represent a departure from the traditional PSA assessment, that need to be resolved before a risk informed approach can be used.

1 The LWR Core Damage concept and its relelated risk figures Core Damage Frequency and Large Early Release Frequency can not be extrapolated to HTR.

2 Although the role of passive safety system reliability can be introduced without any problems in the generally applied static event tree/fault tree technique to model the course of accidents, the practical way to assess the reliability of these passive systems or processes needs development.

References

[1] Procedures for conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Practices, Safety Series No. 50-P-4, IAEA, Vienna, 1992.

[2] PRA Procedures Guide: "A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Jan 1983.

[3] HTR-L EU Contract FIKI-CT-2001 -00155 Deliverable D10 HTR-L D10 Chapter 1: Conceptual Design Description of the Pebble Bed Modular Reactor (PBMR) Plant: Framatome ANP Report, NGSP7/2003/en/0016

[4] IAEA-TECDOC-626, "Safety Related Terms for Advanced Nuclear Power Plants", IAEA, sept. 1991.

[5] REPAS, "The REPAS approach to the evaluation of passive safety systems reliability", Passive System Reliability workshop, Cadarache, France, NEA/CSNI/R(2002)10, March 2002.

[6] RMPS, Reliability Methods for Passive Systems (RMPS) study -strategy and results, Passive System Reliability workshop, Cadarache, France, NEA/CSNI/R(2002)10, March 2002.

[7] Feasibility study of an advanced GFR design trends and safety options status of France & US studies, Global 2003, New Orleans, november 2003.

[8] Considerations in the development of safety requirements for innovaitive reactors: Application to modular high temperature gas cooled reactors, IAEA-TECDOC-1366, August 2003.

[9] HTR-L D10 - Operating Conditions Classification for a Direct Cycle Pebble Bed Modular HTR Chapter 2: Determination of Initiating Events through a Top/Bottom Approach A.I. van Heek, NRG

[10] PRA use in a Risk-Informed Framework, ST4.1, Draft

appendix A Generic lists initiating events

In report NUREG/CR-2300 [2] and IAEA safety series [1] a number of generic lists have been included. In the following, these lists are shown and the initiating events which might be of importance for PBMR have been noted. The sign "V" indicates that this event is applicable directly or can be translated to an equivalent event in terms of corresponding systems in the PBMR (indicated in bold). The sign "X" means the event cannot easily be translated into an event with a comparable system in the PBMR design or is not applicable at all.

List of BWR transient initiating events (NUREG/CR-2300)

V 1 Electric load rejection
V 2 Electric load rejection with turbine bypass valve failure
V 3 Turbine trip
V 4 Turbine trip with turbine bypass valve failure
X 5 Main-steam isolation valve (MSIV) closure
X 6 Inadvertent closure of one MSIV
X 7 Partial MSIV closure
X 8 Loss of normal condenser vacuum
V 9 Pressure regulator fails open **=>HICS**
V 10 Pressure regulator fails closed **=>HICS**
V 11 Inadvertent opening of a safety/relief valve (stuck)
V 12 Turbine bypass fails open
V 13 Turbine bypass or control valves cause increase in pressure (closed)
V 14 Recirculation control failure--increasing flow
V 15 Recirculation control failure--decreasing flow **=>CPBP / HPB / LPB opening / SIV closure**
V 16 Trip of one recirculation pump **=> HPC / LPC trip**
V 17 Trip of all recirculation pumps
X 18 Abnormal startup of idle recirculation pump
X 19 Recirculation pump seizure
X 20 Feedwater--increasing flow at power
V 21 Loss of feedwater heater **=>Loss of recuperator**
X 22 Loss of all feedwater flow
X 23 Trip of one feedwater pump (or condensate pump)
V 24 Feedwater**=> helium** low flow
V 25 Low feedwater**=> helium** flow during startup or shutdown
V 26 High feedwater**=> helium** flow during startup or shutdown
V 27 Rod withdrawal at power
V 28 High flux due to rod withdrawal at startup
V 29 Inadvertent insertion of control rod or rods
V 30 Detected fault in reactor protection system
V 31 Loss of offsite power
V 32 Loss of auxiliary power (loss of auxiliary transformer)
X 33 Inadvertent startup of HPCI/HPCS
V 34 Scram due to plant occurrences
V 35 Spurious trip via instrumentation, RPS fault
V 36 Manual scram--no out-of-tolerance condition

List of PWR transient initiating events (NUREG/CR-2300)

V 1 Loss of RCS flow
V 2 Uncontrolled rod withdrawal
V 3 Problems with control-rod drive mechanism and/or rod drop
V 4 Leakage from control rods
V 5 Leakage in primary system
V 6 Low pressurizer pressure **=>HICS failure**
V 7 Pressurizer leakage **=>HICS leakage**
V 8 High pressurizer pressure **=>HICS failure**
X 9 Inadvertent safety injection signal
X 10 Containment pressure problems
X 11 CVCS malfunction--boron dilution
V 12 Pressure, temperature, power imbalance--rod-position error
V 13 Startup of inactive coolant pump **=>Startup of SBS during PT operation**
V 14 Total loss of RCS flow
X 15 Loss or reduction in feedwater flow (one loop)
X 16 Total loss of feedwater flow (all loops)
X 17 Full or partial closure of MSIV (one loop)
X 18 Closure of all MSIVs
X 19 Increase in feedwater flow (one loop)
X 20 Increase in feedwater flow (all loops)
X 21 Feedwater flow instabi1ity--operator error
X 22 Feedwater flow instabi1ity--miscellaneous mechanical causes
X 23 Loss of condensate pumps (one loop)
X 24 Loss of condensate pumps (all loops)
X 25 Loss of condenser vacuum
V 26 Steam-generator leakage **=>Inter-cooler leakage**
V 27 Condenser leakage **=>Pre-cooler leakage**
V 28 Miscellaneous leakage in secondary system
V. 29 Sudden opening of steam **=> helium** relief valves
V 30 Loss of circulating water
V 31 Loss of component cooling
V 32 Loss of service-water system
V 33 Turbine trip, throttle valve closure, EHC problems **=>GCBV opening**
V 34 Generator trip or generator-caused faults
V 35 Loss of all offsite power
X 36 Pressurizer spray failure
V 37 Loss of power to necessary plant systems
V 38 Spurious trips--cause unknown
V 39 Automatic trip--no transient condition
V 40 Manual trip--no transient condition
V 41 Fire within plant

Boiling water reactors (table VIII in IAEA)

V 1. Turbine trip
V 2. Loss of feedwater **=> helium** flow
X 3. Closure of main steam isolation valve
V 4. Loss of condenser **=>water cooling**
V 5. Loss of off-site power
V 6. Inadvertent opening of relief valves
V 7. Manual shutdown
V 8. Loss of DC power bus(es)

? 9. Loss of instrument air
V 10. Loss of instrument water
V 11. Loss of dry well **=> RPVCS** cooling
V 12. ATWS with turbine trip
X 13. ATWS with closure of main steam isolation valve (MSIV)
V 14. ATWS with loss of off-site power
V 15. ATWS with inadvertently opened relief valve (lORV)
V 16. ATWS with loss of DC power bus(es)
V 17. Large LOCA **(**inside containment**)**
V 18. Medium LOCA **(**inside containment**)**
V 19. Small LOCA **(**inside containment**)**
X 20. LOCAs outside containment
V 21. Seismic event
V 22. Floods
V 23. Fires

Pressurized water reactors (table VIII in IAEA)

V 1. Large LOCA
V 2. Medium LOCA
V 3. Small LOCA
X 3(a) Interfacing system LOCA .
X. 4. Steam generator tube rupture
X 5. Steam break inside containment
X 6. Steam break outside containment
X 7. Loss of main feedwater
X 8. Trip of one MSIV
V 9. Loss of flow in reactor coolant system
V 10. Core power excursion
V 11. Turbine trip
V 11a) Turbine trip - loss of off-site power
V 11b) Turbine trip - loss of service **=> cooling** water_
V 12a) Reactor trip
V 12b) Reactor trip - loss of component cooling
V 13. ATWS
V 14. Seismic event
V 15. Flooding
V 16. Fires

EXAMPLE OF INITIATING EVENT GROUPING FOR A CANDU NUCLEAR POWER PLANT (table IX IAEA)

V 1. Forced shutdown
V 2. LOCAs
V 2.1 Small LOCA **(**inside containment**)**
X 2.2 Small LOCA outside containment
V 2.3 Medium LOCA **(**inside containment**)**
X 2.4 Medium LOCA outside containment
V 2.5 Large LOCA
V 2.6 Other LOCAs
V 3 Pressure tube rupture
X 4 End fitting failure
X 5 Steam generator tube rupture

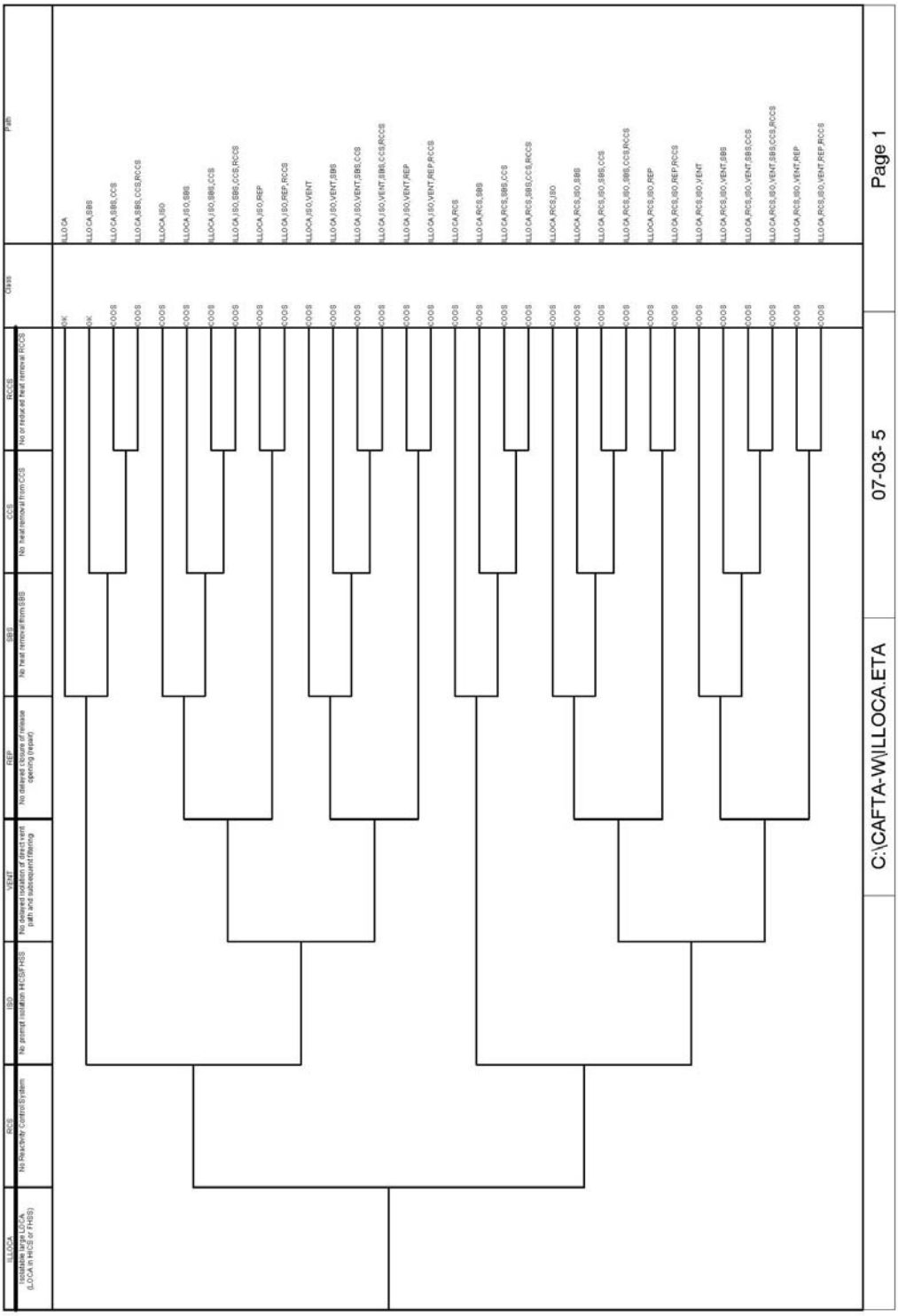
X 6 Loss of high temperature pressure control (low)
X 7 Loss of high temperature pressure control (high)
X 8 Loss of pressure control (high) in solid mode due to loss of controller
V 9 High temperature pressure and inventory control failures
V 10 Any one primary heat transport pump trips **=>HPT/HPC or LPT/LPC or PT**
V 11 Flow blockage (in an individual channel)
V 12 Moderator failure
X 13 Loss of end shield cooling
V 14 Shutdown cooling failures
V 15 Main steam line break **=> cross-duct break**
X 16 Loss of feed water to one or more steam generators
X 17 Feedwater line break
V 18 Turbine trip
X 19 Loss of condenser vacuum
X 20 Reheater drain line break
V 21 Loss of condensate flow **=>water flow in Intercooler / Pre-cooler**
V 22 Unplanned bulk increase in reactivity
V 23 Unplanned regional increase in reactivity
V 24 Loss of computer control
X 25 Loss of low pressure service water open system
V 26 Loss of **(**reactor**)** cooling water system
X 27 Loss of powerhouse upper level service water
X 28 Loss of instrument air
X 29 Loss of cooling to fuel machine in transit
V 30 Loss of bulk electricity supply
V 31 Loss of switchyard

The following initiating events list can now be deduced using the generic lists above:

```
Electric load rejection (Loss of offsite power / auxiliary power /DC)
Electric load rejection with turbine bypass valve (HCV/LCV) failure
Electric load rejection due to generator trip or generator-caused faults
Power Turbine (PT) trip / failure (cooling / bearing / shaft / disk etc.)
High Pressure Compressor/Turbine trip / failure
Low Pressure Compressor/Turbine trip / failure
Power Turbine trip with turbine bypass valve failure

HICS Pressure regulation fails: inventory decrease /depressurisation
HICS Pressure regulation fails: inventory increase
HICS leakage/rupture (inventory decrease / depressurisation))
HICS Pressure regulation fails closed
Inadvertent opening of a safety/relief valve (stuck)
FHSS/CCS/RPVCS leakage/rupture (pressure decrease / depressurisation)
Leakage from control rods / SAS systems?
Leakage/rupture primary pressure boundary /RPV /piping (Large/Medium/Small LOCA)

Turbine bypass or control valves (HCV / LCV / GBP / RBP / SIV /SBP / SBSV) cause
increase/decrease in pressure & flow (blockage)
Control failure HPB / HPBC (change flow/pressure)
Control failure LPB / LPBC (change flow/pressure)

Inadvertent startup SBS (during cycle)
SBS failure during cool down
CCS failure (during cool down)
Loss of RPVCS
Loss of computer control
(Loss of instrument air?)


He/water exchanger He-flow blockage
He/water heat exchanger water flow decrease (blockage)
He/water heat exchanger water flow temp increase / decrease
He/water heat exchanger leakage/ rupture (depressurisation)
(Partial) Loss of component cooling (active cooling system ACS)

Rod / SAS withdrawal at power
High flux due to rod/SAS withdrawal at startup
Inadvertent insertion of control rod or rods / SAS
Pressure, temperature, power imbalance--rod/SAS-position error
Loading error (fuel / graphite spheres)
Scram due to plant occurrences
Detected fault in reactor protection system
Spurious trip via instrumentation, RPS fault
Manual scram--no out-of-tolerance condition

Seismic event
Floods
Fires
```

appendix B Examples of Event trees

Isolatable Large LOCA:



appendix C List of accident initiating events

The list below shows all accidents identified and scrutinized in the previous sections.

1. Chemical effects
   - Air Ingress
   - Water Ingress

2. Thermal effects

   Heat Sink Availability Failure
   - Turbo-machinery failure
   - PCU Cooling Failure Reducing Heat Removal
   - Inadvertent CCS He Flow Rate Decrease
   - Inadvertent CCS Water Flow Decrease
   - Inadvertent CCS Water Temperature Increase

   Cool down Flow Rate Decrease
   - Loss of Coolant Accident due to pipe Break or leakage PPB
   - Loss of Coolant Accident due to Vessel Breach or Leakage
   - Loss of Coolant Accident due to Helium-Water Heat Exchanger Ruptures
   - Spurious Opening of Safety Valve
   - Spurious Helium Bypass Valve Opening
   - Flow Blockage of a Recuperator
   - Flow Blockage of a Pre-cooler
   - Flow Blockage of an Intercooler
   - Turbine Blade Failure
   - Compressor Blade Failure
   - Compressor Wheel Failure
   - Turbine Disk Failure
   - Magnetic Bearing Failure
   - Shaft Break Turbo Machine
   - Shaft Seizure Turbo Machine
   - Pipe Break inside the Primary Pressure Boundary
   - Leakage of seals or Breach Inside the PCU
   - Spurious CCS He Flow Rate Decrease During Cool down
   - Inventory Control System Failure Decreasing Helium Inventory
   - Make-up System Failure Decreasing Helium Inventory

Power & Reactivity Control

- Spurious Removal of Small Absorber Spheres from the Reactivity Control System
- Spurious Removal of Small Absorber Spheres from the Cold Shutdown System
- Spurious Reactivity Control Unit Operation
- Mechanical Failures of Systems Connected to the Reactor Vessel
- Mechanical Failures of Systems within the Power Conversion Unit
- Change Reflector Geometry
- Inadvertent Operation of the CCS at Power
- Inadvertent PCU Water Flow Rate Increase
- Inadvertent PCU Water Temperature Increase
- Inadvertent Closure of the Helium Bypass Valve
- Loss of External Electrical Load
- Loss of AC Power to the Plant Auxiliaries
- Load Rejection due to generator failures
- Inventory Control System Failure Increasing Reactor Coolant Inventory
- Make-up System Failure Increasing Reactor Coolant Inventory
- Blockage of Fuelling Pipe
- Fuel Handling and Storage System Failure
- Internal Mechanical Failure
- Internal Hazards Challenging the Core Support Function
- Load Drop Challenging the Core Support
- Reactor vessel Mechanical Failure
- Internal Hazards Challenging the Reactor Vessel
- Load Drop Challenging the Reactor Vessel
- PCU/Cross Duct Mechanical Failure
- Internal Hazards Challenging the PCU/Cross Duct
- Load Drop Challenging the PCU/Cross Duct
- Pressure Boundary Challenge
- Heat Removal Decrease from Primary System
- Reactor Coolant Flow Rate Decrease
- Reactor Coolant Inventory Increase
- Differential Pressure Increase
- Reactor Vessel Support Mechanical Failure
- Internal Hazards Challenging the Reactor Vessel Support
- RCCS Pipe Break
- RCCS recirculation Water Loop Failure

appendix D Assignment initiating events to event groups

Large LOCA, non-isolatable

Large Loss of Inventory caused by tube ruptures, RPV failure, PPB failure (ingress of air, water)
Heavy Load Drop
External explosion
Seismic event
Core structural support failure
Aircraft crash
Control rod ejection
Floods

Large LOCA, isolatable

Large Loss of Inventory caused by tube rupture /vessel breach HICS

Intermediate LOCA, non-isolatable

Intermediate Loss of Inventory caused by tube ruptures, RPV failure, PPB failure (ingress of air, water)
Break in CCS/RPVCS
(Turbine) Missiles / Projectiles
He/water heat exchanger tube rupture

Intermediate LOCA, isolatable

Break in HICS/FHSS
Inadvertent opening of a safety/relief valve (stuck)

Small LOCA, non-isolatable

Leakage/seal failure in CCS/RPVCS
Leakage from control rods (CRDM seal failure
He/water heat exchanger leakage

Small LOCA, isolatable

Leakage/seal failure in HICS/FHSS

No heat removal from core (Loss PCU & CCS)

Loss of offsite power
Loss of auxiliary power (loss of auxiliary transformer)
Loss of DC power bus(es)
Fire within plant
Loss of computer control (RPS)
Loss of active cooling system ACS (heat sink)

Decreased heat removal from core / RPV

He/water heat exchanger(s) water flow decrease (blockage): He-temp increase

Electric load rejection (HV breaker opening / generator trip or faults)
Electric load rejection with gas cycle bypass valve failure
Turbine trip (loss of offsite power / cooling water / Resistor Bank)
Loss of turbine (bearing /blades/ shaft /disk etc.)
Turbine trip with gas cycle bypass valve failure

Loss of Reactor Pressure Vessel Conditioning System (RPVCS)
Loss of Reactor Cavity Cooling System (RCCS)
Loss of Core Conditioning System (CCS) (at shutdown)
Loss of generator cooling (leakage / loss of water flow)
He/water heat exchanger(s) water flow temperature increase
He-water heat exchanger (Intercooler/Pre-cooler /CCS) He-flow decrease
Flow decrease (blockage) recuperator
Trip/loss of High Pressure compressor/turbine
Trip/loss of Low pressure compressor/turbine
Trip of both turbo compressors (HPC and LPC)
Low helium flow during shutdown (SBS failure)

Control valves malfunction causing change in pressure and flow:
- Gas cycle Bypass Valve (GBP)
- High/low Pressure coolant valve (HCV/LCV)
- Recuperator bypass valve (RBP)
- Start-up blower system inline valves (SIV)
- High/low pressure compressor bypass control valves (HPBC/LPBC)
- High/low pressure compressor bypass valves (HPB/LPB)

Power/reactivity increase

HICS Pressure regulation fails: inventory increase
Uncontrolled fuel loading (mix up of spheres, detection errors)
Blockage of fuelling pipe
Uncontrolled Rod (group) withdrawal at power
Uncontrolled SAS removal from reactivity control system
Uncontrolled SAS removal from cold shutdown system
High flux due to rod/SAS withdrawal at startup
Pressure, temperature, power imbalance--rod/SAS-position error
Reflector geometry modification (top reflector drop)

Miscellaneous

HICS Pressure regulation fails: inventory decrease /depressurisation
HICS Pressure regulation fails closed (no regulation)
Uncontrolled Rod (group) insertion at power
Uncontrolled Rod (group) withdrawal in accident event (re-criticality)
Manual scram--no out-of-tolerance condition
Scram due to plant occurrences
Detected fault in reactor protection system
Spurious trip via instrumentation, RPS /EPS /OCS fault

He/water heat exchanger(s) water flow increase: He-temp decrease

Uncontrolled SAS insertion from reactivity control system
Uncontrolled SAS insertion from cold shutdown system
Inadvertent reactivity control unit actuation

Inadvertent operation of CCS at power
He/water heat exchanger(s) water flow temperature decrease
Inadvertent operation SBS at power
High helium flow during startup or shutdown (SBS failure)
Low helium flow during startup (SBS failure)

appendix E Synthesis of the works done on the reliability of passive systems

CEA Report CEA/DEN/CAD/DER/SESI/LCFR/NT DO 11 13/06/2006

Direction de l'Énergie Nucléaire
Direction du CEA/Cadarache
Département d'Études des Réacteurs
Service d'Études des Systèmes Innovants
Laboratoire de Conduite et Fiabilité des Réacteurs

CEA/DEN/CAD/DER/SESI/LCFR
DO 41 04/07/06

06PPMO000068

BORDEREAU D'ENVOI

Date : 04/07/2006

Désignation : **Note technique CEA/DEN/CAD/DER/SESI/LCFR/NT DO 11 13/06/06**
Synthèse des études menées sur la fiabilité des systèmes passifs

Auteur : **Michel MARQUES**

Destinataires		Nombre	Observations
TE	J. Pirson F. Parmentier	1	*Pour Attribution*
AREVA-NP	S. Esther-Vignoud B. Carluec		
AMEC-NNC	I. Coe		
ANS	L. Mansani		
EA	J. Carretero		
EDF	C. Clement		
JRC	H. Wider J. Carlsson		
NRG	G. Brinkmann M. Middel		
CEA DDIN/DPSF	P. Anzieu		
DDIN/MR	V. Moulin		
DER/DIR	A. Porracchia		
DER/SESI	J. Rouault G-L. Fiorini		
DER/SESI/LCSI	P. Dumaz D. Barbier J-C. Garnier		Copies 1ère page : DDIN CAD/SCGA C. Le Pennec DER/SPEX DER/SPRC DER/SRES DER/SSTH
DER/SESI/LESA	P. Dufour		
DER/SESI/LCFR	N. Devictor M. Marquès *1ex en circulation*		
Base de données HTREX		1 (PDF)	

Le rédacteur : Michel MARQUES

Le Chef du DER/SESI : Jacques ROUAULT

Commissariat à l'énergie atomique
Centre de Cadarache – Bât. 212 – 13108 Saint Paul Lez Durance cedex
Tél. : 33 – (0)4 42 25 30 05 – Fax : 33 – (0)4 42 25 24 08 – mail : nicolas.devictor@cea.fr

m/D:\Documents and Settings\MM109415\Local Settings\Temporary Internet Files\OLK4DD\DO41.doc

CEA/DEN/CAD/DER/SESI/LCFR/NT
DO 11 13/06/06

06PPBT000011

DIRECTION DE L'ENERGIE NUCLÉAIRE
DIRECTION DU CENTRE DE CADARACHE
DÉPARTEMENT D'ÉTUDES DES RÉACTEURS
SERVICE D'ÉTUDES DES SYSTÈMES INNOVANTS
LABORATOIRE DE CONDUITE ET FIABILITE DES REACTEURS

NT	CEA/DEN/CAD/DER/SESI/LCFR/NT DO 11 13/06/06	0	5H62	A-FIHTR-03-06	DDIN/SFS/FIHTR	1/7
NATURE	CHRONO UNITÉ	INDICE	UNITÉ	ÉLÉMENT D'OTP	CLASSEMENT UNITÉ	PAGE

Note Technique

TITRE : SYNTHESIS OF THE WORKS DONE ON THE RELIABILITY OF PASSIVE SYSTEMS

SYNTHESE DES ETUDES MENEES SUR LA FIABILITE DES SYSTEMES PASSIFS

AUTEUR(S) : Michel MARQUES

RESUME : Le projet RAPHAEL, dans le cadre du 6ème Programme EURATOM, a pour objet de supporter le développement des réacteurs à gaz thermiques à très haute température (RTHT). Au sein de ce projet, l'objectif principal du « Work Package » 4 (approche de sûreté) est de compléter et de consolider l'approche de sûreté européenne pour des réacteurs à haute température modulaire développée dans le cadre du 5ème PCRD. Parmi les nouvelles données d'entrée à intégrer dans l'approche de sûreté, il y a les résultats du projet RMPS (Reliability Methodology for Passive Systems, 5ème PCRD).
Cette note technique décrit une synthèse des résultats du projet européen RMPS, et donne une liste des questions ouvertes à résoudre pour répondre à la question du choix entre systèmes actifs et systèmes passifs. La prochaine étape de ce travail est la définition d'un exercice pour démontrer les capacités de cet outil pour l'évaluation de la performance de la fonction évacuation de la puissance. Cet exercice serait réalisé pendant la seconde période du projet RAPHAEL.

ABSTRACT: The RAPHAEL Project, in the 6th Framework Programme Euratom, focuses on Very High Temperature Reactor (VHTR) technological developments (www.raphael-project.org). In this project, the main objective of the WP4 (Safety approach) is to complete and consolidate the European safety approach for modular HTRs started during FP5. Among the new inputs for the update of the safety approach developed in FP5, there is the results of the Reliability Methodology for Passive Systems (RMPS, FP5).
This technical note describes a synthesis of the European project RMPS results, and gives a list of open questions in order to answer to the question of the choice between active and passive systems. The next step of the works on this task is the definition of an application to demonstrate the capabilities of these tools for the assessment of the performance of decay heat removal function. This application should be performed during the second period of the RAPHAEL project.

KEYWORDS: HTR, RAPHAEL IP, PASSIVE SYSTEM, RMPS
MOTS CLES : RTHT, PROJET INTEGRE RAPHAEL, SYSTEME PASSIF, RMPS

(04/02 - JA-Document1)

	Rédacteur	Vérificateur	Vérificateur Qualité	Approbateur
Fonction			IQ du SESI	Le Chef du SESI/LCFR
visa				P.I F. BERTRAND
NOM	Michel MARQUES	G-L FIORINI	Florence JOYER	Nicolas DEVICTOR
Date	12/6/06	14/6/06	15/06/06	16/06/06

Propriété Industrielle	Cadre de réalisation	Classification					Qualité
		DR	CC	CD	SD	Ss	
En l'absence d'accord ou de contrat, la diffusion des informations contenues dans ce document auprès d'un organisme tiers extérieur au CEA est soumise à l'accord du Chef de Département.	**DOB**..... **DDIN/DPSF** **Domaine**..... **SFS** **Projet** ..... **FIHTR** **Contrat**..... **(PCRD 6) RAPHAEL**					X	Document réalisé sous SMQ certifié AFAQ — ISO 9001

	NT	CEA/DEN/CAD/DER/SESI/LCFR/NT DO 11 13/06/06	0	2/7
	NATURE	CHRONO UNITÉ	INDICE	PAGE

Indice	OBJET DES REVISIONS	DATE	RÉFÉRENCE GCAO
0	Emission initiale	16/06/06	CEA/DEN/CAD/DER/SESI/LCFR/NT DO 11 13/06/06

Contents

1. INTRODUCTION

The RAPHAEL (*ReActor for Process heat, Hydrogen And ELectricity generation*) Project, in the 6th Framework Programme Euratom, focuses on VHTR technological developments needed for industrial reference designs in the areas of reactor physics, safety, fuel and fuel cycle back end, materials and components (www.raphael-project.org).
In this project, the main objective of the WP4 (Safety approach and licensing issues) is to complete and consolidate the European safety approach for modular HTRs, which definition started during FP5 and to obtain the feedback on this approach from a large panel of partners representing European utilities, designers and R&D organisations.
As written in the annex of the contract, *"new inputs will be the basis for an update of the safety approach developed in FP5:*

- *The safety aspects associated with VHTR, indirect cycle and process heat production, in particular hydrogen application (safety strategy, events to be considered in the design, list of safety-related equipment),*
- *The outcomes of the FP5 Safety Workshop and the licensing interactions for current and future reactors (in South Africa and US for modular HTR, in US for the VHTR and other advanced reactors, as well as licensing interactions in Europe for future PWRs),*
- *The consequences on the design of a more risk-informed approach. In particular, the basis of development of Probabilistic Risk Assessment (PRA) methodology and the application of the* ***Reliability Methodology for Passive Systems (RMPS)*** *to modular HTR safety demonstration will be investigated, Besides, the benefit of LBB implementation in the safety demonstration will be assessed."*

Concerning the point "Reliability Methodology for Passive Systems", the CEA is in charge of a synthesis of the European project RMPS results, mainly dedicated to the passive systems of category B according to the IAEA classification. This technical note answers this demand (Section 2), and gives a list of open questions in order to address the concern raised by the choice between active and passive systems (Section 3). To date, it is agreed that methods to assess the reliability of the different kinds of passive systems exist.[1]
The next step of the works on this task is the definition of an application to demonstrate the capabilities of these tools for the assessment of the performance of decay heat removal function. This application should be performed during the second period of the RAPHAEL project.

2. RESULTS OF THE EUROPEAN PROJECT RMPS (2001-2004)

Within the framework of the 5th FP RMPS project, a methodology has been developed to evaluate the reliability of passive systems characterized by a moving fluid and whose operation is based on physical principles, such as the natural circulation. The reliability evaluation of such systems is based in particular on the results of thermal-hydraulic (T-H) calculations. This methodology (Figure 1) can be structured in three parts:

- Identification and Quantification of the sources of uncertainties;
- Reliability evaluations of passive systems;

[1] Indeed, for the passive systems of category A (static structures, physical barriers), the structural reliability methods can be used and for the systems of category C and D (check and relief valves, rupture discs,...), the data of experience feedback on similar equipment can be used to quantify the failure rates.

- Integration of passive system reliability in Probabilistic Safety Assessment.

Identification and quantification of the sources of uncertainties

The methodology is applied to a specific accident scenario for which a particular passive safety system is required. Having specified the scenario to be examined, the first step, **identification of the system**, requires fully characterizing the system under investigation. That is, specifying the goals of the system, the modes by which it can fail, and providing a definition of system failure, (i.e., success/failure criteria). **Modelling the system** is also required. This is done using best-estimate (B-E) computer codes. The numerous sources of uncertainties present in the modelling process have to be identified. This includes approximations in modelling the physical process and system geometry and uncertainties in the input variables such as initial and boundary conditions. **Identifying the most important thermal hydraulic phenomena and parameters** for the system that have to be investigated is an important part of the methodology. This can be done using an expert panel having a good understanding of the systems functions, B-E code calculations and a method for developing a relative ranking of the phenomena. The ranking technique implemented in the RMPS project was the Analytical Hierarchy Process (AHP). Having identified the important thermal hydraulic parameters, the next step is to **quantify their uncertainties**. In case of lack of experimental data, this requires expert judgement to identify the range of uncertainty and to select an appropriate probability density function for a given set of variables. The methodology then incorporates a **sensitivity analysis** which will determine, among all the uncertain parameters, the main contributors to the failure risk of the system.

Reliability evaluations of passive systems

The second part of the methodology requires evaluating the uncertainty in the expected performance of the passive system as predicted by the TH code and according to the studied scenario and the uncertainties' modelling. This uncertainty evaluation can be performed using a confidence interval or a probability density function. The RMPS study found that methods giving an uncertainty range of the system performance are not very efficient for reliability estimation. Therefore the use of a probability density function was the approach that was implemented. Then the probability density function of the system performance can be directly used for reliability estimation, once a failure criterion is given. The existing methods for this **quantitative reliability evaluation** are generally based on Monte-Carlo simulations. Monte Carlo simulations consist in drawing samples of the basic variables according to their probabilistic density functions and then feeding them into the performance function evaluated by the TH code. An estimate of the probability of failure can be found in dividing the number of simulations leading to the failure of the system, by the total number of simulation cycles. Monte-Carlo simulations require a large number of calculations. As a consequence, these calculations can be prohibitively long. To avoid this problem, two approaches are possible: the variance reduction techniques in Monte-Carlo methods or the use of **response surfaces**. It is also possible to use approximate methods such as First and Second Order Reliability Methods (FORM/SORM).

Integration of passive system reliability in a Probabilistic Safety Assessment (PSA)

The objective of this last part of the methodology (not included in Figure 1) is the development of a consistent approach for these quantitative reliability evaluation of the passive system and for its introduction in the accident sequence of PSA. Up to now, in the existing PSA of innovative nuclear reactor projects, are only taken into account the failures of the passive system components (valves, pipes…), but not the failure of the physical phenomena on which the system is based. The treatment of this aspect of the passive system failure in the PSA models is a difficult and challenging task and no commonly accepted practices exist. Different possibilities have been discussed within the framework of the RMPS project, but no real consensus between partners was obtained. In coherence with the current standards of Level 1 PSA models, the approach studied by CEA and Technicatome is based on a representation of the accidental scenarios in the form of static event trees. The event tree technique allows the identification of all the different chains of accident sequences deriving from an initiating events and describing the different basic events corresponding to the failure or to the success of the safety systems. This method was applied to a fictitious PWR reactor equipped with two types of safety passive systems. The failures analyses performed on this reactor allowed the characterisation of the technical failures (valves, heat exchanger pipes…) and the ranges of variation of the uncertain parameters that affect the physical process. A simplified PSA was performed starting from a single initiating event. The majority of the sequences addressed by this event tree were analysed by deterministic evaluations using envelope values of the uncertain parameters. For some

sequences where the definition of envelope cases was impossible, basic events corresponding to the failure of the physical process were added to the event tree and quantitative reliability evaluations, based on Monte Carlo simulations and on a TH code were carried out to evaluate the corresponding failure probability. The failure probabilities obtained by these reliability analyses were fed into the corresponding sequences. This approach allows the evaluation of the influence of the passive system on the accidental scenario. In particular, on the studied example, a new design basis of the system has been proposed in order to fully satisfy the global safety objective assigned to the reactor.
The methodology was applied to 3 passive systems : the Isolation Condenser System (ICS) of BWR reactors, the Residual Passive heat Removal system on Primary circuit (RP2) of PWR reactors and the Hydro-Accumulator (HA) system of PWR, VVER type reactors.
In the applications performed by the CEA et Technicatome, the thermal-hydraulic passive system acts as an ultimate system in the management of the scenario. For these conditions, the characteristics of the current Level 1 PSA models are suitable. For the other conditions, the partners of the RMPS project consider that complementary R&D is necessary and leave open number of questions discussed below.

In conclusion

The developed methodology participates to the safety assessment of reactors equipped with thermal-hydraulic passive systems (TH) and is an indispensable tool for the designers who define the architecture of safety systems and for the regulatory authorities in the safety evaluation of passive system.
It should first of all be noted that the concept of intrinsic reliability of a component which exists for an active system or structural component is not directly applicable to a TH passive system. Indeed, the probability or the frequency value associated with the TH passive system is linked to a given scenario (state of the other systems on the circuit, environmental conditions...); the concept of functional margin has been introduced. A methodology to incorporate these reliability data into a single characteristic value, representative of all the possible situations, has not been found to date.
The results of the analyses made show that, in spite of the inherent characteristics of passive systems, which are a priori considered as advantages (simplicity, decrease of the need for human interaction, reduction or avoidance of external electrical power or signals), the decision for the designers to replace an active safety system by a passive system is not easy from a safety point of view. Moreover before making a final decision on this selection, other points which have not been addressed within the framework of the RMPS project, due to limited time and resources, have to be studied in future work. In particular, a very important issue concerns the human factors, which play an important role in the inspection and the maintenance of the passive systems.

3. OPEN QUESTIONS

In addition to the improvement of different topics of the RMPS methodology and in order to answer to the question of the choice between active and passive systems, it is necessary to take into account other points of view that the reliability, such as the efficiency, the simplicity, the robustness, the human factor and economic evaluations, and to develop a tool for helping the systems design's optimisation.

1) About the improvement of the RMPS methodology, two items of the methodology roadmap deserve closer attention: the identification of the relevant parameters and the quantification of uncertainties. In RMPS, the identification of the input parameters is not based on strict rules. Rules, which guarantee a rationale approach to the problem and, which demonstrate that the procedure is based on realistic assumptions, would justify the choice of the uncertain parameters and moreover should convince the designer. In the selection of the relevant input parameters, a clear distinction for the various kinds of uncertainties should be introduced distinguishing between modelling uncertainties on one side and uncertainties dealing with the state of knowledge about the passive systems and their characteristic parameters on the other side.
2) An other important item of improvement is the integration of the passive systems reliability in the PSAs. The first attempts performed within the framework of RMPS have taken into account as well the failures of the components of the passive system as the failures of the physical process involved like basic events in static event trees.
This last choice might seem unsuitable because it does not appear to consider the dynamic aspects of the transient progression including dynamic system interactions, T-H induced failure, and operator actions in response to system dynamics. In fact, we have treated in the RMPS project, examples where the overall reactor, including the safety systems and in particular the passive system, is modelled by the T-H code. This leads to the fact that the dynamic system interactions

are taken into account by the T-H calculation itself. In addition, we have not considered human intervention during the studied sequences, which is coherent with the usual utilization of the passive systems in innovative reactors. So, for a first approach, the event tree presentation seems a good and simple representation for the assessment of accident sequences, including the passive systems.
However in order to generalise the methodology, it is important to take into account the dynamics 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.

3) A very important issue is on the human factors, which play an important role in the reliability assessment of a passive system. Indeed the periodic maintenance and inspection of such systems introduce particular constraints ; unlike an active system that can be more easily isolated or inspected during the shutdown periods, a passive system requires to be tested under its real physical conditions of utilization, and this can generate new specific implementation in the global architecture and safety problems. In addition, the question of whether it is an advantage or a disadvantage that passive systems do not allow operator intervention during its operation, should be investigated.
Before comparing a passive and an active system on the same mission, it is necessary to make sure that the passive system design is optimised in terms of performance. Methods have to be developed to ensure the optimisation.

4) Technical-economical evaluations of the systems must be carried out to provide information that is essential for the comparison between passive and active systems.

4. A LIST OF REFERENCES RELATED TO THIS TOPIC

Note : all deliverables of the RMPS project are available on www.rmps.info.

1. OECD, 2002. Passive system reliability. A challenge to reliability engineering and licensing of advanced nuclear power plants. In Proceedings of an International Workshop, OECD/NEA/ CSNI/R(2002)10, Cadarache, France, 4–6 March.
2. L. Burgazzi, "Evaluation of Uncertainties Related to Passive Systems Performance," *Nucl. Eng. Design*, **230**, 93 (2004)
3. B. Papin. Principle of an operational complexity index for the characterization of the human factor relevance of future reactors concepts. Proceedings of EHPGM'2004, Sandefjord (2004).
4. M. Marquès et al. Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment. Nuclear Engineering and Design 235 (2005) 2612–2631
5. C. Kirchsteiger. A new approach to quantitative assessment of reliability of passive systems. Safety Science 43 (2005) 771 –777
6. L.P. Pagani et al. The impact of uncertainties on the performance of passive systems. Nuclear Technology. Vol. 149 (2005)
7. IAEA-TECDOC-1474. Natural circulation in water cooled nuclear power plants phenomena, models, and methodology for system reliability assessments. November 2005

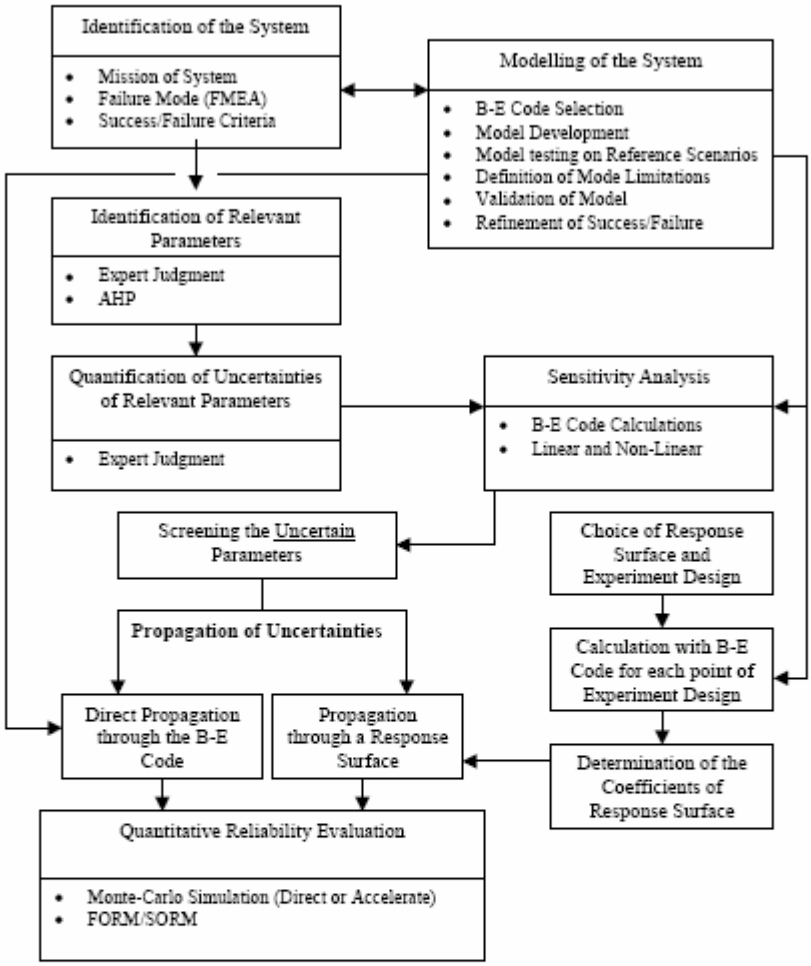


Figure 1 : Approach for RMPS reliability assessment methodology