Table 2. Key results and input specifications of MAAP 2B runs of TML3-1 accident scenario for VVER 440 and Zion.

THE KEY INPUT DATA	VVER 440	ZION
Contmt vol./thermal power	3.5 e-5	2.5 e-5
Contmt wall area/thermal power	9.8 e-6	3.5 e-6
Primary system volume/ thermal power	1.4 e-7	1.0 e-7
Total sec side volume/ thermal power	1.8 e-6	0.8 e-6
Full thermal power	1.5 GW	3.2 GW
EVENT	**VVER 440**	**ZION**
Steam generators dry	6.7 hr	1.8 hr
RPV fails	8.9 hr	3.8 hr
Reactor cavity dry	-	7.5 hr
Pressure in the containment 1 day into the accident	3 bar	9 bar

5 CONCLUSIONS

VVER 440 plant concept for Finland has several passive safety features. Most important of these are the large water volumes of primary and secondary circuit in respect to the thermal power, residual heat removal capability through natural circulation is good, the plant has a double containment, which has no rooms below the reactor pressure vessel giving a wider erosion margin in core meltthrough accidents.

Severe accidents have been analysed with MAAP 2B computer code. In the analysed accidents the reactor pressure vessel fails at 1.6 ... 11 hours and the containment integrity is maintained at least 65 hours into the accident. The time margin in the containment integrity is mainly due to the heat sink provided by large amount of internal steel and concrete structures in the containment.

FRENCH CONCEPTS OF 'PASSIVE SAFETY'

Y. DENNIELOU
Service Etudes et projets thermiques et nucléaires,
Electricité de France,
Villeurbanne

J.L. NIGON
Commissariat à l'énergie atomique,
Centre d'études nucléaires de Cadarache,
Saint-Paul-lez-Durance

M. SERRET
Service Sûreté,
Framatome,
Paris-La Défense

France

Abstract

N_4 model, the French 1400 MW PWR of the 90's, exhibits many advanced features. As far as safety is concerned, the fully computerized control room design takes advantage of the operating experience feedback and largely improves the man machine interface. New post-accident procedures have been developed [the so-called "physical states oriented procedures"]. A complete consistent set of "Fundamental Safety Rules" have been issued.

This however doesn't imply any significant modification of standard PWR with regard to the passive aspects of safety systems or functions. Nevertheless, traditional PWR safety systems largely use passive aspects : natural circulation, reactivity coefficients, gravity driven control rods, injection accumulators,... and so on.

Moreover, probability calculations allow for comparison between the respective contributions of passive and of active failures.

In the near future, eventual options of future French PWR_s to be commissionned after 2000 will be evaluated ; simplification, passive and forgiving aspects of safety systems will be thoroughly considered.

"Passive Safety" is generally considered as a quite evident way to improve the safety of water cooled reactors. In fact, the evidence of such an improvement has to be ascertained by the careful evaluation of its actual benefit which needs the definition of :

- "Passive Safety" concept itself,
- the present safety level (reference level), the use of more passive safety features is supposed to enhance,
- a common "yard-stick" for a step by step comparison so as to evaluate the appropriate complementary scopes of "passive" and "active" safety.

Such an evaluation has already been made at the beginning of the design of PWRs as these reactors already include passive safety features ; it will be reevaluated in France for the next series of reactors to be built at the beginning of the years 2000.

This communication is intented to summarize the present French findings on that comparison.

Its deals with :

- the passive safety concept,
- the French present safety level (N4 projets),
- the comparison method,
- the French evaluation for the use of more passive features.

1. PASSIVE SAFETY CONCEPT

An IAEA draft working paper (622-I3-TL-633) has been established on Description of Passive Safety Related Terms. The terms defined by this draft paper are used in the present communication, and are briefly recalled as follows :

- Terms specific to passive safety definition :

. Inherent safety characteristic which is equivalent to absolute safety due to the use of the laws of nature only,

. Passive component or system which can only use self acting means at the component level (check valve for instance),

. Self acting system which only uses self acting means at the system level (i.e control features and batteries),

. Active component (or system) which uses active means from other systems,

- Terms non specific to passive safety :

Walkaway safety	Error tolerance
Grace period	Foolproof

If these four last terms may obviously be applied to a plant using only inherent, passive or self acting systems for post accident operation, they do not apply only to such a plant. As a matter of fact, since they do not require any operator action, they may also be applied to fully automatic systems even if they are active. Thus they will not be discussed in this document which is aimed to establish the differences between active and passive features.

The term Fail-safe will also not be discussed in this document. If it can be considered as a particular property of passive or self acting components or systems, the same can also be considered for active ones (e.g : safe position of an active valve in case of lack of control voltage or of instrument air).

A first approach on the technical scope of application of "passive safety" can be drawn up by investigating which kind of safety functions inherent, passive or self acting equipment or systems are able to perform.

The table of appendix 1 which analyses for some safety functions to ensure after incidents or accidents, the possible use of inherent, passive or self acting features in the case of a Pressurized Water Reactor is a first tentative of such an investigation.

In this table as well as in the rest of this presentation the term "possible" means "physically possible". No consideration has been given to practical or economical feasibility.

The following comments on that table can be drawn up :

- Inherent features

Inherent features seems to be possible only for reactor shutdown and this, limited to specific cases as heat up or loss of coolant, using well known physical properties such as Doppler effect or lack of moderator.
The need for a PWR to bring water to the core for its cooling probably prevents the possible use of other inherent features. The conclusion may differ for other reactors (pool type reactors or other reactor types) for which inherent features may be more widely used for safety functions.

- Passive features

Passive features are clearly not practicable where automation using I&C and/or multiple actions are needed in particular for containment isolation, steam and feedwater isolation, for steam generator tube rupture and for fuel handling accident.

They may be used for high pressure core cooling for which they are limited :

- in time, as the use of pressurized capacities limit their volume,
- in efficiency under a given size of break, as the use of another means of heat extraction needs I&C and automation to be put in service (this covers also the total loss of feedwater system).

They may be used for low pressure core cooling using natural circulation at containment pressure with the reactor coolant system flooded but are also limited for the same reasons as above under a given size of break.

They may also be used without limitation for containment heat removal using external natural convection and internal condensation.

Finally they cannot be used for reactor coolant system depressurization which is itself required for long term passive heat extraction.

- Self acting features

In general self acting features use the same physical phenomena as passive features but take advantage of the allowed use of I&C and automation at the system level. Valves instead of check valves are consequently used and operated from signals initiated from, and logic processed at the system level. Consequently they are only limited by volume capacity.

When several self acting systems are used, a centralised protection system may be prefered to several signals and logic treatments (one per self acting system). Such a protection system would be very close to present ones and would be fed for accident conditions by batteries only. When such a protection system is used the self acting systems would become in turn active ones as they have to receive external inputs, but except for the consequences on layout it is a question of definition only.

As a conclusion, the technical scope of application of "passive safety" is such that what may be called a "passive reactor" is a reactor which may include :

- possible inherent features for reactivity control, (counteractions)
- passive features for core residual heat removal for a break above a given size,
- passive features for containment heat removal,
- active or self acting features for all other functions and in particular for core residual heat removal in case of small break or loss of feedwater, for reactor coolant depressurization, and for protection system.

Such a "passive reactor" can be considered as a limit for a design based on present water cooled reactors, to which would be added more or less "passive features".

The feasibility of such a reactor has not yet been established, it may be difficult to reach, particularly for large power reactors.

2. PRESENT SAFETY LEVEL

The safety level of the present water-cooled reactors in operation or under construction already includes existing safety improvements. As for French plants, N4 model, the 1400 MW PWR of the 90's (two units under completion) exhibits many enhanced safety features which have to be taken into account when comparing "present safety" and "passive safety".

The N4 NSSS, of the four loop type is an upgraded high power design. From a safety point of view this design is the result of the development of French safety approach worked out through the design and construction of 54 units by Framatome and Electricité de France including 34 units of the three loop 900 MWe class series and 20 units of the four loop 1300 MWe class series.

The original safety features of the N4 parent four loop plant, the 1300 MWe plants were analysed by NRC in 1986 and termed "a substantial improvement in safety for a number of potential dominant sequences" (NUREG 1206).

The French approach can be globally characterized by the sucessive addition to *conventional design conditions* (those resulting from the 3 basic levels of defence in depth), of *complementary design conditions* defined as the loss of redundant safety systems when called upon, then of *multiple failure accident conditions* including errors of diagnosis or use of the wrong procedure that generated the so called physical state approach, then again of *severe hypothetical accident conditions*. The analysis of additional conditions, performed with realistic assumptions leads to the elaboration of emergency procedures and back-up means.

"*Conventional design conditions*" have been made more stringent for the N4 model on one point, namely the steam generator tube rupture accident, following the evidence that such rupture is not purely hypothetical. The rupture of one tube is considered as a class 3 incident, with rather severe allowable consequences. The rupture of two tubes is studied as a class 4 accident.

A major concern in the design is the progressivity of safety measures. It is necessary to ensure that no cliff-edge effect in design conditions, and no large step in consequences exist when considering events with a slightly lower probability than the design basis events.

In this sense, it was decided to add to the N4 list of conventional design conditions, a number of "*complementary design conditions*" corresponding to the total failure of redundant systems. If these failures are not considered by the deterministic rules they are nevertheless to be taken into account from a probabilistic point of view with regard to the other conventional design conditions. Mitigating means, termed "back-up", and procedures, termed "H", were determined in order to meet the French safety objective for these complementary conditions.

The French safety objective includes a probabilistic criterion :

- no unacceptable consequences should result from the operation of plant with frequency higher than 10^{-6} per reactor-year,

- applied to a particular family of events, no unacceptable consequences should result from this family with a frequency higher than 10^{-7} per reactor-year.

It must be pointed out that formerly this objective was a guidance of the Safety Authority, used only as design condition for man-made natural events. For the first time, on the N4 project, this objective is also applied to justify the complementary conditions, and therefore used in the licensing process.

Unacceptable consequences are interpreted here as severe core degradation, a very conservative definition which ignores the mitigating effect of the containment.

Appendix 2 lists the N4 complementary design conditions, and the corresponding design improvements. Among these improvements is the newly implemented overpressure protection system, which allows bleeding of the Reactor Coolant System in the H2 procedure (RCS bleed/feed following total loss of feedwater in steam generator). The system was originally designed to answer the post-TMI concern on the reliability of the safety or relief valves.

"*Multiples failure accidents*" include errors of diagnostics or use of the wrong procedure, and/or multiple concurrent systems failures beyond what has been considered in the design and can result in severe accident situations.

At this point, it is still possible to manage prevention of severe core degradation. Two measures are implemented on the N4 plant.

The first measure is the development of complete set of accident procedures based on the "physical states approach" or "symptom oriented approach", to replace the event-oriented procedures which are presently implemented on French plants.

This approach which will be first implemented on P'4 plants implies :

. the diagnosis of states based on a survey of parameters used for the different systems (primary circuit, secondary circuit, containment and safeguard systems),

. the identification of operator actions as individual objectives (residual heat removal, restoration of the water inventory, subcriticality ...),

. the prioritization, for each state, of the objectives and immediate actions.

With such a set of procedures, the operating team should avoid diagnosis errors, match unexpected situations and perform actions which are appropriate to the cooling state of the reactor.

The second measure provides for additional capability to cope with successive failures of on-site cooling means which would occur within several days or weeks. The (U3) procedure is developed to be able to connect additional mobile pumps and heat exchanger in order to restore (or increase the redundancy of) heat removal at medium term.

Finally, in the unlikely case where all the above-mentioned measures would have been inefficient, the mitigation of the consequences of "*severe hypothetical accident conditions*" defined as a core melt is considered. Mitigation is performed by ensuring the integrity of the third barrier to fission products, the containment.

This important step of the French approach is also based on the use of procedures and back-up means as for instance the venting pass through a sand filter.

As for design improvements enhancing safety, two new features contribute to improve the operating conditions and the operating safety : the DMAX core control system and an advanced control room design.

The DMAX (Dispositif de Manoeuvrabilité Maximale) is a second-generation core control system, following the DMA (Dispositif de Manoeuvrabilité Accrue) system used on previous units. Both systems use "grey" control rod groups.

With the DMAX system, the axial offset is automatically controlled by an additional closed control loop which adjusts the overlap between the rod groups. Besides operator aid, DMAX achieves very efficient axial offset control during any transients or dynamic perturbations.

The N4 advanced control room is based on ergonomic principles aiming at alleviating the operator tasks and maximizing the understanding of events under all circumstances. Each redundant operator desk is a single working area which allows for a total access to information and control devices. The information display is elaborated in a very synthetic and comprehensive form.

3. COMPARISON BETWEEN "ACTIVE" AND "PASSIVE" FEATURES

Such a comparison would be aimed to define, using cost consideration, the appropriate complementary scopes of "passive" and "active" safety.

To be well balanced the comparison would have to consider :

- the level of definition of new designs,
- the different levels of maturity of the technologies : for example proven (and backfitted) versus new (tested or untested) technologies,

- the eventual use of different methods, rules or safety margins in the design (evolutions, such as realistic calculations or leak before break concept etc, may have only been used for one type of reactor),

- the potential negative counterparts of passive or inherent features : for example a large primary or secondary water inventory which increases the thermal inertia in transient conditions, also increases the mass and energy release to the containment in case of pipe break. Similarly a negative temperature coefficient is detrimental in case of cooling transient.

As for the definition of a common "yard-stick", reliability or probabilistic assessment may be considered as well adapted to the comparison between the respective contribution of passive and active failures, as they have no consideration for a said "present" or "passive" safety. In fact they are the sole quantitative comparison means which can be used. It must nevertheless be performed cautiously as there is - as far as we know - no experience on accident analysis of passive systems, no reliability data of new passive features, no operating experience nor R and D results.

An other way of comparison but only qualitative, is to evaluate which deterministic rules used for "present" reactor design would be or would not be used for passive ones. This applies in particular for the Defence in Depth Concept as applied on French plants (see section 2 of the present document).

Of course the active features which would be maintained in a new design would have to be in accordance with the defence in depth concept ; consequently the following which is the first tentative of such an investigation is only related to the part of passive features of a new plant or to a whole plant if only using "passive features" (as the "passive reactor" defined at the end of section 1).

- Adequation of plant design and quality levels for normal operation

Whatever the safety level (reliability) of "passive systems" called upon after an incident or an accident may be , the quality of plant design and construction has to be maintained at its present level to prevent failure during normal operations for obvious economical reasons (charge factor, protection of the resource invested in the plant) if not for safety ones. Consequently it may be considered that a plant using more or only "passive systems" remain based on the first level of defence in depth as far as normal operation in concerned.

The use of more inherent or passive features for accident prevention may also reinforce this first level of defence in depth.

- Design of control and protection systems to minimize the consequences of abnormal transients or incidents

For the same reasons as above and as the protection system of a passive reactor would already be in fact very close to the system used on present ones (refer to section 1) it may also be considered that such a plant remains based on the second level of defense in depth.

- Use of engineered safety features to mitigate the consequences of postulated accidents

As "passive systems" are used as engineered safety features this third level of defense on depth is obviously taken into account.

The deterministic rules considered for the design of engineered safety features are also to be used for "passive systems" such as :

. single failure criterion (particularly for passive failure),
. seismic qualification,
. protection against internal and external hazards,
. protection against common cause failure,
. surveillance and testability.

- Loss of redudant safety systems.

In principle as a reactor using only "passive features" needs neither external electrical feeding nor active cooling source such multiple failure accident condition (station blackout or heat sink failure) have

not to be investigated. This also applies for a total loss a feedwater which is already taken into account in the design.

As for ATWT they would have to be dealt with on the same manner as for "present plant" as the protection system and the reactor scram system would be anyway identical or similar.

However due to the specific process used for "passive" features, other multiple failure accident conditions according to their estimated frequency may have to be considered with the use of additional feature (back-up).

- Multiple failure accident conditions (physical state approach)

Physical state approach (as well as "symptom oriented one") has no reason to be implemented for a reactor using only "passive features" as by definition (no external input) no human action would be needed for such a reactor.

The walk away concept which is quite opposite to the "safety culture one" does not necessitate in principle any operator action in case of accident.

Consequently, even if for practical reasons the walk away concept has to be limited in time, a total confidence has to be placed in the design and the construction which gives more importance to the first three levels of defence in depth.

This does not exclude the human factor as errors may result from design, construction, testing or maintenance.

- Severe hypothetical accident conditions

In our mind there is no reason to exclude this type of accident (except for fully inherent reactor if any) for "passive" reactors. The walk away concept (full confidence in design) may be considered as increasing the need for such a level of defence.

If the leaktightness of a containment ensuring a passive heat transfer can be ensured, such a containment may be useful for that accident condition. On the contrary due to the venting effect of the external cooling of the containment a leakage would be detrimental (rapid transfer to the environment).

As a conclusion it may be pointed out that the defence in depth concept as applied on French plant may remain a useful basis of design, for "passive reactors". In particular their design may remain based on progressive levels of defence for safety reasons, but also for economical reasons (charge factor, protection of the resource invested in the plant).

4. FRENCH EVALUATION FOR THE USE OF MORE "PASSIVE FEATURES"

Due to the French context (series of standardized reactors) the evaluation of the use of more passive features will be included in the studies engaged for the definition of a new series of standardized reactors.

Although the project N4 whose first two constructions are under way on the CHOOZ site, in the ARDENNES area, represents a product of advanced reactor, studies have been undertaken for the design of pressurized water reactor plants which, in the beginning of the years 2000, should replace the existing plant becoming obsolete and satisfy the increase in the consumption of electrical power.

These are still preliminary studies which should be followed by a preliminary design stage allowing evaluating the interest of each innovation in particular from an economic point of view.

These studies mainly deal with the following points :

- Evolutive approach complying with a standardized plant series policy, as was the case over the twenty past years with the successive standardized plant series : CP0, CP1, CP2, P4, P'4 and N4 :

  . estimation of the grid requirements at the time considered,

. implementation of the feedback from the operating experience acquired on French nuclear plants (some fifty reactors) and foreign nuclear plants,

. taking account, at the design level, of specific measures allowing limiting the consequences of severe accidents,

. search for improvements allowing the reduction of the costs of investments and fuel cycle,

. development of a fuel supply strategy taking account of the predictible evolution of the uranium prices and the plutonium market during the XXIst century.

- Taking account of new designs of the pressurized water reactor core, using fuel with a higher plutonium content than that used during plutonium recycling in the existing reactors and aiming at an optimum use of fissile materials such as the "RCVS" concept (Spectral Shift Convertible Reactor).

- Taking account of the use of more "passive" features proven to be reliable and economical.

APPENDIX 1

POSSIBLE USE OF "PASSIVE FEATURES"

SAFETY FUNCTIONS	*INHERENT FEATURES*	*PASSIVE FEATURES*	*SELF ACTING FEATURES*
Reactor shutdown	Possible in specific cases: Doppler effect: Loss of moderator	Possible in specific cases use of high boron concentration accumulator in case of depressurization	Possible (I&C and automation at the system level)
Core water covering	Not possible	Possible (tanks and check valves) but limited in time for high pressure injection	same as a above but limited in time for high pressure injection
High pressure heat removal through a break above a given size (LOCA condition)	Not possible	Possible as long as core water covering is achieved	Possible (I&C and automation at the system level) but as long as core water covering is achieved
High pressure core heat removal with a break under a given size (another cooling means needed)	Not possible	Not possible (automation needed: e.g. to put in service high pressure heat exchanger)	same as above
Depressurization (needed as core water covering is limited in time at high pressure)	Not possible	Not possible as clearly needs an action	Possible (I&C and automation at the system level)

SAFETY FUNCTIONS	INHERENT FEATURES	PASSIVE FEATURES	SELF ACTING FEATURES
Low pressure core heat removal through the break (above a given size)	Not possible	Possible by natural circulation at containment pressure with the RCS flooded	Same as above by natural circulation at containment pressure with the RCS flooded
Low pressure core heat removal with a break under a given size (another cooling means needed)	Not possible	Not possible (I&C and automation required e.g to put in service a heat exchanger)	Same as above but using e.g an heat exchanger also flooded
Containment heat removal	Not possible	Possible if the pressure boundary of the containment may act as a heat exchanger surface with an external natural connection	Possible may improve passive features
Containment isolation	Not possible	Not possible	Possible (I&C and automation at the system level)
Steam and feed-water isolation closure	Not possible	Not possible	Same as above
Radioactive release limitation in case of :			
. Steam generator tube rupture	Not possible	Not possible (intelligence needed)	Same as above
. Fuel handling accident	Not possible	Not possible	Same as above

APPENDIX 2

N4 COMPEMENTARY DESIGN CONDITIONS AND CORRESPONDING DESIGN IMPROVEMENTS

N4 - COMPLEMENTARY DESIGN CONDITIONS	
- Reactor TRIP system failure	(ATWS)
- Total loss of ultimate heat sink	(H1)
- Total loss of feedwater in S.G.	(H2)
- Total loss of electrical power	(H3)
- Long term total loss of LHSI pumps or CSS pumps or HX	(H4)

CORRESPONDING DESIGN IMPROVEMENTS
- Diversified ATWS - Mitigating system
- RCS bleed/feed using the pressurizer pilot operated safety valves
- Additional turbo-generator set allowing . RCP seal injection . Emergency batteries power supply
- Cross-connections between SIS and CSS allowing long term mutual back-up