WAYS OF IMPROVING SAFETY FOR FUTURE PWRs IN FRANCE

G. Gros, J. Jalouneix, D. Manesse, J.M. Mattéi
Institut de Protection et de Sûreté Nucléaire (IPSN)
CEA - Fontenay-aux-Roses -FRANCE

ABSTRACT

For the design of a new generation of nuclear power plants which could be ordered in France at the end of the nineties, there is a broad consensus on the choice of the evolutionary way, in view of the significant progress in the field of safety which appears possible with this approach, due to feedback of operating experience from a large number of reactors, results of extended safety research and development projects, general technical progress and findings from detailed probabilistic safety studies performed.

This paper presents results of thinkings and studies, conducted within the Institute for Nuclear Safety and Protection (IPSN) in the various fields mentioned, in view of the definition of safety objectives and principles for future PWRs. These results contributed to the preparation of a common safety approach for future plants in France and Germany.

1. THE FRENCH BACKGROUND

The paper "Common safety approach for future pressurized water reactors in France and Germany" (ref. 1), presented at this conference, describes the status of the development of safety objectives and principles common to both countries. As indicated, the work is being performed on the basis of a long lasting experience in the areas of safety research, licensing and plant operation. In both countries, safety improvement has been a continuous process and experience from operation and safety research has always been utilized in backfitting of existing plants, design improvements of new plants and changes in licensing rules and practices.

In this context, for the design of a new generation of nuclear power plants the construction of which could begin at the end of the nineties, there is in France a broad consensus, including within safety organizations, on the choice of the evolutionary way, in view of the significant progress in the field of safety which appears possible with this approach. Indeed, the operating experience from a large number of reactors and the in-depth studies (mainly probabilistic safety assessments and severe accident studies) conducted on the existing power plants constitute two major driving forces towards progress.

The present paper covers the French experience in these fields, which has been used as a basis in the Franco-German development of a common safety approach. Thinkings and studies have been conducted for the last few years (ref. 2 and 3) within the IPSN which is the technical support organization of the French safety authority. The aim of the studies is to identify ways of improving the design of future plants in France, with the main following objectives :

- significant reduction of the global probability of core damage,
- significant reduction of radioactive releases, mainly for severe accident conditions,
- and also reduction of individual and collective doses received by workers.

2. USE OF PROBABILISTIC SAFETY STUDIES

For the first objective, studies are based on the use of the French probabilistic safety assessments performed for existing plants, mainly the 1300 MWe standardized plant series. A number of issues have been retained that should be considered when designing future reactors, including :

- the positive changes made in the design of the 1400 MWe plants ; particularly, as hardware diversification has its limits, it is further functional redundancy which shall be sought ;
- the sequences with a relatively high core meltdown probability ; they have to be thoroughly investigated ;
- the sequences with a high uncertainty on their probability level ;
- the safety-related components and systems which will emerge from the probabilistic studies on the importance of components and systems ;

possible upgrades in component design, installation, operation and maintenance should be proposed (see chapter 3).

The main conclusions are views related to the elimination of sequences leading to core meltdown with possible early failure of the containment (core meltdown under pressure, containment bypass and also sequences in shutdown conditions, the confinement being not fully guaranteed), the reduction of human operating errors during accident situations (for example by increasing the level of automation), the increase of functional redundancies for some safety systems, and the improvement of the design of some equipment. The main points are presented hereafter.

2.1. COMMENTS ON AUTOMATING THE FEED AND BLEED MODE

Feed and bleed is an operating mode initiated on existing plants by the operator, mainly in the events of total loss of feedwater for the steam generators, of steam generator tube rupture and of rupture of secondary piping followed by a loss of the emergency feedwater system (EFWS). The total probability of core meltdown for these sequences is of the order of 1.3 10^{-6}/year. Automating the feed and bleed mode is a possible way to reduce the probability of high pressure core meltdown sequences, even though it may introduce a number of nuisances namely through the generation of spurious signals. However, such course should be studied within a general framework covering all of the functional redundancies liable to be installed, as developed hereafter.

Basically, the EFWS is a safeguard system having a function on reactors in normal operation mode (removal of the residual power when switching from hot to cold shutdown). As shown by the results of the studies conducted on core meltdown conditional probability and on importance factors, this is one of the reasons why this system is particularly important for safety. The relevance of having an additional system to perform this type of function in normal operation has to be investigated with the aim of reducing the probability of core meltdown under high pressure in the above specified circumstances, provided that this additional system is functionally usable in the event of loss of normal feedwater ; this implying suitable design and installation criteria.

2.2. ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS)

ATWS conditions may be reached because either the emergency shutdown signals are not transmitted or the trip breakers fail to open (this leads to overpressure in the primary circuit) or because a number of rod cluster control assemblies are mechanically jammed (therefore, hot shutdown subcriticality cannot be obtained).

For the first category, it seems satisfactory to renew the solutions used on 1400 MWe plants (diversified transmission of the emergency shutdown command and diversified implementation and increased relief capability of the pressurizer safety valves). For the second category, the necessity of an automatic boration system has to be investigated owing, among others, to the high uncertainty existing on the probability for several rod cluster control assemblies to get jammed.

2.3. DESIGN OF THE ELECTRICAL SUPPLIES

The existing design of electrical power supplies shows two relatively weak points for which improvements have to be searched, particularly against common cause failures. The first point concerns the internal power used to supply the electrical safety switchboards. The designer should study the use of diversified sources of power for all the components needed to cope with a total loss of electrical power. Functional diversity like turbine driven pumps for the EFWS and specific generators for equipment needed in case of blackout has to be investigated.

The second point concerns the reliability of electrical switchboards. Taking into account operational experience they can be liable to common cause failure. To solve this problem, the designer must study for example the possibilty of diversifying the technology and the manufacturer of the electrical switchboards or the possibility of using a local power supply box connected to diversified power sources for some vital safety components.

2.4. PRIMARY BREAKS OUTSIDE THE CONTAINMENT

For these breaks, the conditional probability of core meltdown with containment bypass is 1. The initiator corresponds to the combinations of check valve failures resulting in the loss of the pressure barrier present between the primary system and the low pressure section of the safety injection system (SIS). A

large leak results in a pressure buildup in the low pressure section of the SIS, and in its failure. Under such conditions, the primary system as well as the refuelling water storage tank are suddenly purged outside the containment.

The initiator probability estimate varies from 10^{-9} to 7.10^{-5}/year when taking into account an "internal leak" common mode. The tremendous uncertainty present on the initiator values as well as on the failure modes to be considered are solid ground for dealing with this problem as a priority issue. Moreover, this should be extended to systems carrying primary coolant and presently located outside the containment and to systems located outside the containment and liable to act as a containment barrier, for instance in the event of failure of an exchanger tube carrying primary coolant.

2.5. STEAM GENERATOR TUBE RUPTURE

Some solutions need to be explored to reduce containment bypass possibilities in the event of failure of steam generators tubes (their probability is of the order of 3.3 10^{-7}/year). We can mention mainly bringing the discharge pressure of the safety injection system pumps below the secondary design pressure, inserting relief valves for the steam generators and their relief lines within the containment, installing a device to limit the water refill of the steam generators.

2.6. LOSS OF RHRS PUMPS AT MID-LOOP OPERATION

Whenever switching to residual heat removal system (RHRS) mid-loop operation, there is a risk of vortex generation upon suction by the RHRS pumps which may result in dewatering these pumps. To reduce the impact of this problem, the plant design should be such that the presence of a low level in the primary circuit does not result in losing the RHRS pumps (or that operation of the plant should provide for switching to the RHRS mid-loop operation only when the core is unloaded).

2.7 CONSIDERING BREAKS IN SHUTDOWN CONDITIONS

During one part of the shutdown state, safety injection can only be started manually for some primary break sizes. This results in relatively high core meltdown probabilities given the short time available to the operator. Under such circumstances it seems relevant to investigate the implementation of a new safety injection start-up signal.

3. USE OF OPERATING EXPERIENCE

This chapter deals with the lessons learned from operating experience which are not included in the probabilistic safety assessments. The objective is not only the reduction of the global core meltdown probability but also the reduction of radiological consequences for normal operation. Two themes of thinking are presented : improvement of defence in depth (which remains the fundamental principle of safety for future nuclear power plants) and improvement of the quality of equipment.

3.1 IMPROVEMENT OF DEFENCE IN DEPTH

INSAG 3 proposes five levels of defence in depth. The first two levels of defence in depth are intended to preclude accidents, the third to preclude severe accidents, particularly core meltdown, the fourth to preclude unacceptable environmental consequences and the fifth relates to off-site emergency plans.

It has to be noted that the effectiveness of the measures taken to date as regards the first two levels of defence in depth is extremely variable, as the actual or estimated frequency of initiating events varies between 10^{-6} and 10^{-7}/year for the least probable to 10^{-3} to 10^{-4}/year for breaks, 10^{-2}/year for steam generator tube rupture and around 1/year for loss of the main feedwater supply.

It is a fact that the design of the existing facilities is not systematically the subject of special provisions intended to minimise the probability of failures in the normal operating range, although it may be expected that this would have contributed to reducing the frequency of initiating events. For example, systems dedicated to normal operation with no explicit safety functions are not the subject of grading requirements.

It would appear reasonable, for future reactors, to make defence in depth applicable to all or part of these systems with a view to reducing the frequency of initiating events of degraded states of the installation. This could result in setting some reliability objectives, for instance an annual number of scrams, a reduction in the frequency of loss of the main feedwater supply or any other more pertinent factor.

With this in mind, defence in depth in the first two levels should be focused on ensuring that the installation has adequate autonomy and on the

adoption of fault-tolerant designs. In this context, an effort needs to be made to minimize the dependence of the installation on external entities, such as the heat sink and off-site power supplies.

For the first two levels of defence in depth, the approach should be, firstly, to reduce the frequency of initiating events of degraded states of the installation and, secondly, to provide intrinsic resistance of the installation to potential hazards and accidents. Furthermore, the design of future reactors should feature a significant increase in level four of the defence in depth.

Examination of the various types of events likely to affect a nuclear installation shows that, in fact, the four levels set out above do not exist systematically. This is the case, for example, with containment bypass, for which levels three and four do not exist, with the rupture of large components of the reactor coolant system, with meltdown under pressure and cold shutdowns for which level four is not guaranteed. This means that in these cases levels one, two and sometimes three have to be upgraded as far as possible with the aim of attempting to "eliminate" this type of event by taking adequate provisions.

The approach adopted is in its principle mainly deterministic in nature. It consists in identifying a priori the events which could give rise to unacceptable consequences and in suggesting design steps to "eliminate" them. In practice, since a zero risk is meaningless, the term "eliminate" means significantly reducing the frequency of occurrence of the event to a sufficiently low value. The resulting situation may be justified by a probabilistic demonstration, provided for in the design verification stage. Some examples of the approach are given hereafter.

a) Rupture of the vessel during operation

In this case, safety is dependent upon the first two levels of defence in depth. This means that the choice of materials, the quality of manufacture, checks in-factory and on-site, in-service inspection and follow-up during operation are the only levels of defence, and it is worthwhile maintaining, if not increasing, the quality requirements on this component. This also means that steps are taken during the design process to eliminate weak points in the pressure vessel. In this context, the interest of removing the instrumentation tubes from the bottom of the pressure vessel should be examined.

It is also worthwhile limiting the effects of ageing on the pressure vessel, thereby reducing the neutron flux to values as low as possible.

b) Rapid dilution accidents

In the light of our current knowledge, it seems difficult to draw up design rules which could prevent a large incursion of deborated water into the reactor coolant system. Provisions should therefore be made to preclude the phenomenon in the context of levels 1 and 2 of the defence in depth. The most radical solution would be the design of a boron-free core ; alternatively the approach adopted could be as follows :

- upgraded level 1 consisting of several lines of defence :
  - general design of the systems in such a way as to limit the build-up of deborated water and to prevent its injection into the reactor coolant system,
  - increase in the negative reactivity of the control rods in such a way that there is no possibility of an accident occurring during hot shutdown (this represents an increase from 6500 pcm to 10,000 pcm),
  - systematic unloading of the core during cold shutdown if there is no possibility of a pressurized water reactor core which would have a $K_{eff} << 1.05$ during cold shutdown in pure water.
- level 2: detection of incursions of water into the reactor coolant system and monitoring of the boron content.

c) High pressure core meltdown

In this case it cannot be excluded that the phenomena likely to result from the instantaneous exchange of energy between the molten fuel and the containment atmosphere during penetration through the pressure vessel could jeopardize the confinement function. The fourth level of defence in depth would therefore be lost. So, it would be useful to upgrade the third level of defence in depth by the use of an effective depressurization system of the reactor coolant system.

d) Core meltdown at low pressure accompanied by loss of containment integrity

This is the case when there is a pre-existent leaktightness defect in the containment, it is also the

case with certain shutdown situations when the confinement function might not be guaranteed (opening the air locks and equipment hatches, maintenance of penetrations, etc.). The measures to be taken with regard to defence in depth could be as follows :

- level 1: designing the installation in such a way that a low water level in the reactor coolant system does not cause the residual heat removal system pumps to fail,
- level 2: improving the systems which monitor and watch containment leaktightness,
- level 3: design of an engineered safety system which, in the event of the residual heat removal system being lost, prevents core meltdown,
- level 4: measures to ensure that, in the majority of cases, confinement can be restored under satisfactory conditions.

3.2 REQUIREMENTS ON EQUIPMENT

Thinkings are related to the adequacy of equipment at performing its function (safety classification, qualification, fault tolerance) and to availability of equipment over time (maintenance, periodic tests, location and accessibility).

a) Qualification

The guarantee of the reliability and the availability of items of equipment which have a safety function to perform is based on specific requirements for their design, manufacture and operation. The arrangement of items of equipment into a certain number of safety classes associated with requirements, the severity of which varies according to the safety function to be performed, is one means of ensuring a level of quality in relation with the importance of the items of equipment to safety.

One of the requirements mentioned above is qualification, which is a means of ensuring that items of equipment are fit to perform their function when the installation is under degraded conditions.

For future reactors, qualification must in particular take into account the operating and environmental conditions associated with severe accidents. Special specifications are to be drawn up in this context for items of equipment involved in the confinement function and severe accident management (instrumentation inside the reactor building, resources for the removal of residual heat and for containment isolation, materials used for the barriers, etc.). These equipment must be qualified, if necessary, for the conditions of background, temperature, pressure, humidity, dose rates and doses resulting from a severe accident.

To this end, it can be estimated that qualified instrumentation should make it possible on the one hand to monitor the evolution of the accident by giving the values of significant physical parameters, and on the other hand to detect the occurrence of key phenomena (pressure vessel rupture, hydrogen combustion, corium-basemat interaction).

b) Fault tolerant equipment

In addition to the formal grading requirements, equipment should be designed, as far as possible, individual parts as well as whole systems, with the aim of providing simple, rugged and tested solutions. In other words, technological solutions (material, design of parts, configuration of systems etc.) which can intrinsically resist the operational and environmental conditions which equipment is likely to encounter during its lifetime.

In this context, it is evident, for example, that any solution which can improve the performance of reactor coolant pump seals and thereby reduce the possibilities of associated loss of leaktightness in the reactor coolant system should be adopted as a matter which improves safety.

The selected equipment must be fault tolerant, but it must also be installed in such a way as to minimise the risks of aggression or of degradation of the equipment by its environment. To this end, an attempt could be made to minimise the number of sensitive items of equipment installed inside the reactor building.

Furthermore, the selection of items of equipment and the steps to be taken during their installation for future reactors should take experience feedback from existing reactors into account. In particular, it would be useful to :

- minimize operating conditions likely to result in the degradation of the equipment (water hammer, vibration, erosion, cavitation, etc.) ;
- take measures to ascertain the position of all the isolation devices (safety valves included).

If these steps are followed, the possibilities of human errors will be limited and maintenance will be simplified, which is consistent with the concept of fault tolerant design.

c) Maintenance

Being in a position to guarantee that the quality of equipment remains adequate over time is mainly the result of adequate in-service maintenance. A certain number of general principles relating to maintenance are put forward for future reactors. For instance :

- attempt to reduce maintenance-related common *mode failures*,
- attempt to reduce the duration of unavailability due to maintenance,
- make allowance for testing the equipment in the design.

In addition, the conditions under which the maintenance activities are carried out (reactor in power operation, reactor shutdown for refuelling, different outage states, etc.) must be drawn up by taking the following into consideration :

- the duration of the unavailability of the equipment performing a safety function in terms of the repair work needed,
- the action to be taken to ensure requalification of the equipment after repair,
- the period of time during which an item of equipment can be tolerated as unavailable without significantly jeopardising the safety of the installation (requirement expressed in terms of technical operating specifications).

d) Periodic tests

One of the requirements associated with the safety classification is subjecting equipment to periodic tests during operation in order to ensure that it remains available and functions well over time.

For future reactors, measures should be taken in the design stage to ensure that periodic tests can be carried out under conditions as close as possible to those under which the equipment has to perform its safety function. To this end, care should be taken to ensure that :

- it is possible to test whole functional channels, in other words from the sensor to the actuator or to the information of the operator in the control room. In those cases where it is impossible to test all of a channel in a single operation, sufficient overlap of the tests on the various portions of the channel should make it possible to ensure that nothing has been overlooked ;
- it should be feasible to perform the tests avoiding, as far as possible, any interventions likely to adversely affect the reliability of the installation (disconnection of items of equipment, untimely intervening in electrical cabinets, etc.) ;
- it is possible to periodically ensure that the equipment performs well enough to demonstrate safety (e.g. maximum pump flowrate, length of operation representative of use of equipment under post-accident conditions, time taken to operate the valves at the maximum differential pressure encountered under accident conditions etc.).

Generally speaking, periodic tests must be performed according to the technical operating specifications, without adversely affecting the safety of the installation, or interfering with its normal operation, and without causing degradation of the equipment. Methods and resources must therefore be developed, such as test devices, resources relating to the various types of valves, instrumentation for judging the availability and performance of the equipment.

In particular, provisions should be taken during the design stage to provide the systems with a level of redundancy consistent with the periodic tests to be carried out and with the conditions under which maintenance operations are performed in such a way that these actions in no way compromise the overall safety level of the installation.

e) Location and accessibility of equipment

In addition to the measures mentioned earlier and with the main objective of reducing individual and collective doses received by workers, it is also necessary to ensure by means of suitable design and operating rules that access can be secured to equipment important to safety for intervening, checking, testing, repair or replacement, whenever necessary to provide a satisfactory level of safety. In particular, provision should if necessary be made, especially in matters concerning radiological protection, for intervening on active equipment used during accident or post-accident operating conditions.

4. USE OF SAFETY RESEARCH

The concern is the significant reduction of radioactive releases for accident conditions. The general approach consists in taking design provisions :

- at first, in order to "practically eliminate" accident situations which would lead to large early releases : sequences involving containment bypassing, high pressure core melt situations, shutdown states and open containment building, reactivity accidents, global hydrogen detonation and in and ex-vessel steam explosions ;
- then, to design the containment in order to deal with low pressure core melt accidents : removing residual heat without venting device, avoiding the penetration of the basemat by a corium, withstanding a global deflagration of the maximum amount of hydrogen ;
- lastly, to make a substantial improvement of the confinement function : reduction of non-collected and non-filtered leak rates (no path of direct leakage from the containment to the outside), reduction of containment pressure and radioactive aerosol concentrations (use of a containment spray system).

Parametric assessments of radiological consequences have been performed, for design basis accident (DBA) as well as for severe accidents. These assessments deal with radiological consequences at short, middle and long term, including soil and food contamination. The aim is to examine how and to what extent the objective of very limited protective measures in area and in time could be satisfied.

The main common assumptions are :

- a core inventory corresponding to a 1400 MWe PWR at the end of the cycle, with a maximum burn-up of 50 GWd/t,
- for the most important fission products (FP), release of 100 % of noble gases, iodine and caesium in case of core melt and of 2 % of these same FP in case of fuel cladding rupture (DBA),
- 1 % of iodine in organic form,
- for spray, depletion half-life (for aerosols) of 10 mn, with a maximum reduction factor of 1000 for suspended activity,
- without spray, deposition inside the containment leading, for complete core melt, to reduction factors of suspended activities of 50, 500 and 1000 respectively after 1, 2 and 5 days,
- for collected leaks, efficiencies of 1000 for aerosols and 100 for organic iodine,
- release at ground level,
- atmospheric dispersion calculated with the IPSN model (class of stability similar to Pasquill D with a wind speed of 5m/s constant during the whole release), by taking into account the meandering effect for long duration release.

Several set of calculations have been performed, by varying the total and non-collected leak rates and the use of spray. One table 1, four representative cases are presented :

- total leak rate of 1 % V/day (value considered in the leakage test of exisiting French double containment reactors) with a non collected leak rate of 0.01 % V/d, without (case A) and with spray in operation (case B) inside the containment,
- total leak rate of 1 % V/d (as previously), but with a non-collected leak rate of 0.1 % V/d (value considered in the (value considered in the leakage test of exisiting French double containment reactors) of existing French double containment reactors) and with spray in operation (case C),
- total leak rate of 0.1 % V/d, with a non-collected leak rate of 0.01 % V/d and with the spray in operation (case D).

On table 1 are presented releases for some important isotopes during the first 7 days and some representative radiological consequences at short-term (passage of the plume), and after one year and two years. One can see that the total leak rate is important only for the release of noble gases and for the external dose, the use of spray (just after the beginning of the accident) leads to a reduction factor of about 15 on the release of aerosols and the non-collected leak rate is the main parameter for the release of aerosols and consequently for the deposition on the ground and the food chain contamination. Concerning the radiological consequences and considering the last International Commission on Radiological Protection (ICRP) publication 63, it appears that :

- the cases B and D (non-collected leak rate of 0.01 % V/d and spray in operation) would not justify, even at the fence of the installation, any protective measure of the public, except some food ban during the first weeks after the accident,
- the cases A (no spray) and C (non-collected leak rate of 0.1 % V/d) should lead to protective measures (administration of stable iodine, temporary relocation, food ban) up to some km.

So, it appears possible to satisfy the objective of very limited protective measures in area and in time. The designer has to propose the total and the non-collected leak rates which can be guaranteed.

3. CONCLUSION

The examples presented show that is it possible to obtain a significant improvement in the field of safety with the choice of the evolutionary way, using the experience from operation and safety research. The work performed by the IPSN has been reviewed by the French advisory committee "Groupe permanent chargé des réacteurs nucléaires" (GPR) at the end of 1992 and beginning of 1993. This contributed to the preparation of the proposal for a common safety approach for future pressurized water reactors in France and Germany (see ref. 1).

REFERENCES

1. W. Frisch, A. Jahns, D. Quéniart, G. Gros, "Common Safety approach for future pressurized water reactors in France and Germany", ARS'94, Pittsburgh, USA, April 17-21, 1994.

2. D. Quéniart, "Safety of future reactors in France", ANP'92, Tokyo, Japan, October 25-29, 1992

3. G. Gros, Y. Cornille, J. Jalouneix, "Allowance for severe accidents in design", ANP'92, Tokyo, Japan, October 25-29, 1992.

TABLE 1

RELEASES AND RADIOLOGICAL CONSEQUENCES
FOR CORE MELT ACCIDENTS ON 1400 MWe PWR

CASE	A	B	C		D	
total leak rate (% V/d)	1	1	1		0.1	
non collected leak rate (% V/d)	0.01	0.01	0.1		0.01	
use of spray	no	yes	yes		yes	
RELEASES (TBq) during 7 days						
Xe 133	$2.5\ 10^5$	$2.5\ 10^5$	$2.6\ 10^5$		$2.7\ 10^4$	
I 131	160	45	310		32	
Cs 134 + Cs 137	39	2.5	24		2.4	
CONSEQUENCES (7 d)						
distance (km)	0.5	0.5	0.5	2	0.5	2
Short term						
plumeshine dose (mSv)	30	28	28	2.5	3.5	0.3
effective dose (mSv)	16	7	65	5.5	7	0.6
thyroid dose (mSv)	350	110	1200	100	110	9
Middle term						
groundshine dose 1st month (mSv)	25	3	30	2.5	3	0.25
groundshine dose 1st year (mSv)	120	15	150	12	15	1.3
activity in fresh food (Bq/kg)	1.10^6	1.10^5	$1.2\ 10^6$	1.10^5	1.10^5	8.10^3
Long term						
groundshine dose 2nd year (mSv)	40	5	50	4	5	0.4