COMMISSARIAT A L'ENERGIE ATOMIQUE

INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE

DEPARTEMENT D'ANALYSE DE SURETE

RAPPORT DAS N° 526e

THE SAFETY OF FUTURE NUCLEAR POWER PLANTS
IN FRANCE

D. QUÉNIART*

Conférence internationale ENS/ANS
sur la sûreté des réacteurs thermiques
(Avignon, 2-7 octobre 1988)

*CEA/IPSN/DAS

Octobre 1988

THE SAFETY OF FUTURE NUCLEAR POWER PLANTS IN FRANCE

D. QUENIART, Head of the Safety Analysis Department
(CEA, France)

The present paper concerns certain personal thoughts on the safety of future French power plants, which will come into operation at the beginning of the next century. These reflections, which are made on the author's own behalf and, under no circumstances, implicate at this stage the official views of the French safety authorities, are aimed at defining some directions for the improvement of safety in these future plants as compared with that of plants presently in operation or under construction.

I The French Context

1) Evolution of the nuclear power program

The French nuclear power program is based on the design, construction and operation of standardized nuclear units, the only adaptations being those due to allowances for the specific requirements of the sites selected for the different units of each standardized series of PWR plants.

After the two Fessenheim units and the four Bugey units, the operating utility, Electricité de France (EDF), designed successively:

- the 900 MWe CP1 and CP2 standardized series (totalling 28 units),
- the 1300 MWe P4 and P'4 standardized series (totalling 20 units),
- the 1400 MWe N4 standardized series, the first two units of which are under construction on the Chooz site and should come on line as from 1991. The other N4 series units will be programmed over the next few years and are scheduled for grid connection towards the year 2000.

Estimated electricity requirement increments for the 2000 - 2015 period are limited (3 to 5 GW); the nuclear power plant construction rate will thus much depend on the average life of the early reactors. It should be borne in mind, in this connection, that 34 nuclear power plants came on line between 1977 and 1987. If the presently declared life expectation for these plants is about 40 years, the possibility of their real life span being shorter, about 30 years, cannot be excluded. This would imply that, between the years 2000 and 2015, provision would have to be made for an additional installed capacity of 20 GW, corresponding to about 14 nuclear units, which would constitute a new standardized series, presently called PWR 2000 by EDF.

2) Evolution of the Safety Approach

a) Defence in depth

For the construction of the first units in the French nuclear power program, reference was made to American plants under construction at that time (Beaver Valley for Fessenheim, North Anna for Bugey). During these initial stages, when EDF and the French safety authorities first confronted safety problems in PWR power plants, they drew freely on American regulatory practice (10 CFR 50 and regulatory guides).

The reference approach, known as "defence in depth", is well known. It consists, after assessment of the validity of provisions made regarding prevention, surveillance and limitation of consequences, in finally demonstrating, for each standardized series, that no unacceptable risk is involved, by the deterministic analysis of a limited number of conventional conditions, for which safety margins are defined on the basis of consistently conservative postulates. These conventional conditions are classified into categories according to frequency of occurrence, where the lower the estimated frequency, the more severe may be the acceptable consequences. Event-oriented operating procedures are also defined elsewhere for these conditions.

This reference approach was gradually supplemented in France, as PWR power plant safety problems were analyzed in greater depth, mainly by investigation of two lines of thought: the probabilistic approach and the severe accident approach.

b) Probabilistic approach

As early as 1977, when the main safety options for the 1300 MWe plants were reviewed, the French safety authorities defined an overall probabilistic objective in the following terms:

"Generally speaking, the design of a PWR nuclear unit should be such that the overall probability of that unit being the origin of unacceptable consequences does not exceed 10^{-6} per year.

From hereon, whenever a probabilistic approach is used to judge whether a family of events should be included in the design basis data for such a unit, it shall be considered necessary to include this family of events if the probability of its leading to unacceptable consequences exceeds 10^{-7} per year, etc.

In compliance with the above, EDF shall examine each case and decide whether the simultaneous failures of redundant trains for safety systems have to be included in the design basis. For these analyses, realistic calculation methods and hypotheses may be used".

Subsequent studies showed the necessity for complementary measures to obtain a satisfactory safety level regarding certain conditions not included in the list of conventional conditions. Specific procedures, called H procedures utilizing where necessary, complementary equipment (to which the design rules are not strictly applied) were defined. We could here mention the H1 procedure "total failure of the heat sink", the H2 procedure "total failure of the steam generator feedwater system", and the H3 procedure "total loss of power (external and internal sources)". These procedures enable the probability of unacceptable consequences to be kept to a value of about 10^{-7} per year, integrating conservatively in the analysis "unacceptable consequences" and the beginning of prolonged core uncovering. They were implemented on all plant units, including, by backfit, the 900 MWe units.

c) The lessons learned from Three Mile Island

The Three Mile Island accident, of course, proved an abundant source of practical safety lessons for the French nuclear power program. In particular, it showed how difficult it is to recover from an accident condition when the operator, owing to a mistaken diagnosis and ensuing plant condition developments, finds himself outside the well defined limits of the event-oriented procedures. A complementary procedure, called the U1 procedure, was then developed in France, based on a reactor cooling condition approach, whereby knowledge of the thermodynamic parameters involved and of the available resources enables the operator to define the actions to be performed in order to recover, insofar as possible, a safe condition, thus avoiding core meltdown. In addition, from the onset of an accident condition, a nuclear safety and radiological protection engineer (one is permanently assigned to each site) joins the shift team in the control room, where he monitors on special equipment the main safety parameters. He will decide if and when the U1 procedure should be implemented.

d) Managing severe accidents

Despite all the precautions taken, as recalled above, it is impossible to exclude entirely the possibility of severe accidents involving core meltdown and more or less extensive loss of containment integrity at a more or less early stage in the accident. Discussions in France on severe accidents were focussed from the outset on controlling the evolution of such accidents and on limiting their consequences by means of a number of suitable actions, whereby, on the one hand, available means in the plant are turned to best advantage and, on the other hand, protective measures for surrounding populations are taken.

Regarding the latter point, the characteristics of French plant sites lead to retaining the possibility, in the first 24 hours, of evacuation of the population within a 5 km radius and sheltering of the population within a 10 km radius.

Severe accidents due to internal causes may be divided into three main classes, all comprising core meltdown:

- accidents leading to early containment failure and release, after a few hours, of the entire radioactivity inventory in the containment, without filtering (source term S1),
- accidents leading to delayed containment failure and release, after at least 24 hours, of the entire radioactivity inventory in the containment without filtering (source term S2),
- accidents leading to delayed containment failure and release, after at least 24 hours, of the radioactivity inventory in the containment via a filtered system (source term S3).

These source terms are defined in the table below (as a percentage of the core radioactivity inventory):

	S1	S2	S3
Noble gases	80 %	75 %	75 %
Organic iodine	0.6 %	0.55 %	0.55 %
Non-organic iodine	60 %	2.7 %	0.3 %
Cesium	40 %	5.5 %	0.35 %
Strontium	5 %	0.6 %	0.04 %

Calculations have shown that the S3 source term is compatible with implementation of the measures for population protection described above.

Under these conditions, the approach adopted consists in devising, without modification to initial design, simple ways of reinforcing the capacity of the containment to fulfill its function as an ultimate barrier against the dissemination of a large quantity of radioactive materials in the event of a severe accident.

To this end:

- a procedure, known as the U2 procedure, provides, by measurement of airborne radioactivity and of the activity in the containment sump water, for detection of possible containment leaks and for action to be taken. This procedure is implemented as soon as an accident situation is declared,

- the ductwork in the containment basemat, which, in the event of basemat melt-through by corium, could form early escape routes to the environment for radioactive substances, will be sealed-off beneath the reactor pit (U4 procedure), between now and the end of 1989,

- to prevent containment failure by overpressure, a device comprising a sand filter, is being installed on all French standardized nuclear units. The purpose of this device is to prevent pressure peaking within the containment from exceeding the design basis value by providing for filtered venting. An efficiency factor of 10 for aerosols was required and obtained, so that an S2 release level could be reduced to the S3 level (U5 procedure).

Other research results tend to indicate that early containment failure is an entirely unrealistic postulate. Fast interactions between molten fuel and water, as well as local hydrogen detonations or overall explosions are still considered as being physically realistic, whereas sudden steam explosions, overall hydrogen detonations, direct overheating, theoretically capable of inducing early containment failure, are deemed physically entirely unrealistic for the large "drywell" containments used in France. However, despite this conviction, studies on this subject are going on, with a view to achieving a better understanding of the phenomena involved and enhancing even further the "defence in depth", by investigating, for instance, the possibilities of corium cooling by water injection.

With these provisions, source term S1 is excluded and source term S2 is lowered to the level of S3, against which, technically speaking, the population can be satisfactorily protected. In the course of ongoing studies, longer term management of severe accident consequences is being investigated, taking into account concomitant contamination of surface, soil and ground water.

e) Use of operating feedback

In the context of such a large number of identical nuclear plants as those of the French nuclear power program, operating experience is particularly beneficial for the improvement of safety in on-line nuclear units and for design improvements for new units. It is for this reason that the operating utility, on the one hand, and the safety authorities, on the other hand, have installed extensive means to define the lessons to be learned from experience, and notably from incidents, and to implement suitable corrective measures on all the nuclear units. It goes without saying that, among these incidents, much importance is attached to the identification of possible severe accident precursor events.

The rapid increase in the number of reactor-years also implies that, by collecting reliability data, knowledge of the behaviour of different equipment can be deepened and, here again, possible abnormalities or signs of design defects or aging can be detected.

Hundreds of safety related modifications were thus made, or are being made, on all the 900 MWe units.

This abundant source of data is also put to use through the probabilistic safety assessments. The IPSN (Institute for Nuclear Safety and Protection) for the 900 MWe units and EDF for the 1300 MWe units are presently developing tools designed to assess the probability of core meltdown. All the necessary precautions have been taken to ensure, by consistency of data and methods, the coherence of these two tools, designed for relative appraisal of overall standardized plant evolution, by input of real reliability data, and for assessment of the advisability of modifying plants or their technical specifications.

All these elements contribute to a deeper understanding of the French nuclear power plants, built by a single NSSS vendor and operated by a single utility, but for which, despite gradually optimized technological solutions, the basic safety options for the 900, 1300 and 1400 MWe units have been questioned.

II The International Context

Since initial implementation of the French nuclear power program, the international context has changed considerably. If the protection of people and property obviously remains a fundamental responsibility of the government of each country, if industrial and regulatory differences fully justify different practices from one country to another, it is presently clear that safety questions have been on an international footing since the Chernobyl accident and will probably remain so.

Exchanges, whether they be bilateral or multinational, have much increased, resulting in better technical understanding and alignment between different countries: it is in this way that a system to prevent excessive containment pressure peaking by filtered venting, first implemented in Sweden and France, has now been adopted by the Federal Republic of Germany and is being examined by other countries as a means of improving the safety of operating plants with regard to severe, beyond design basis accidents.

The nuclear energy debate, where safety questions largely prevail, has much developed throughout the world, with more clearly defined positions since the Chernobyl accident. Certain countries have decided to abandon nuclear power for their future electricity production or have postponed implementation of nuclear power plant projects or have even decided against putting practically completed plants into service.

However, in preparation for a resumption of nuclear power plant construction programs, plant builders in certain of these countries are today developing new generations of reactors which, according to them, would meet with public approval. It is thus that, in the field of light water power reactors alone, it would seem that, in the United States, there are two trends:

- that of development, with projects for reactors where safety margins are increased and where system simplification is sought,
- that of change, with projects for reactors using "passive" systems, for example for safety injection and containment cooling.

A third investigation area, concerning perhaps the longer term, covers projects for lower power modular reactors, using the high temperature reactor type or the fast breeder with metallic fuel type.

Emphasis should here be placed on the possible detrimental effects of seeking the approval of the general public. It is thus that terms such as "inherent safety" and "passive safety" are in frequent use and these expressions, which are intended to highlight safety-promoting characteristics, could be misunderstood in the context of the corresponding projects. In known projects, "inherent safety" is in fact very generally related to a specific accident sequence and "passive safety" to the implementation of more passive safety systems. In other words, if the field of severe, beyond design basis accidents is perhaps limited - and a thorough safety analysis would have to be performed to confirm the fact - it nevertheless exists, since passive devices are not, in any case, fail-proof. As the terms used in the nuclear energy debate are not neutral, far from it, circumspection is advisable.

Another point is worth discussion: the development in France of a new standardized series of nuclear power plants implies awareness of the construction of Europe and the industrial and regulatory changes which this may bring about. But, if we consider, for example, the French and German nuclear power plants which were the subject of in-depth comparative studies, we can of course agree that their safety levels are similar, but this result was obtained by means which, from certain aspects, differ entirely. Certain solutions adopted on one side of the Rhine would appear today to be largely unacceptable on the other side, and vice versa. It must be added that a modification in approach on one point can have marked repercussions on the entire nuclear power plant project and that consequently, adopting for each divergence of opinion the solution deemed most safety-prone is an approach which could very well yield no real safety benefits at all, since each power plant project has its specific inherent logic.

III. Ways of Improving the Safety of Future Nuclear Power Plants in France

a) At this stage, a preliminary question must be asked: should the safety of future French nuclear power plants be further improved with respect to the plants under construction? The question is, of course, basically political and it is the public authorities who will define accordingly the corresponding objectives, which are, of course, related to questions of public acceptance.

Technically, there are no grounds for modifying, at the present time, the overall objective defined in 1977, whereby the probability of unacceptable consequences should be equal to or below 10^{-6} per year. Neither would it be useful to define a core meltdown probability criterion since, on the one hand, it would not be easy to assimilate it with the previously mentioned overall objective, on the other hand, the probabilistic approach is not used in France for reactor design and, finally, the most generally postulated criterion for core meltdown (10^{-5} per reactor per year) would appear to have been perceptibly reached, in the light of the first results of the probabilistic assessments performed a posteriori for the 1300 MWe plant units.

However, in the space of 10 years, the notion of "unacceptable consequences" has become more restrictive. By today's standards, it would appear necessary, all probabilities being otherwise equal, to reduce the quantities of radioactive substances released, in view of the particular sensitiveness of public opinion to this aspect.

On the other hand, up till now, surveys on the radiological consequences of accident situations only dealt with dose equivalents which could be received by the populations concerned. Since the Chernobyl accident took place, it has become advisable to examine possible consequences regarding contamination of the ground and of human food products. In the European Community countries reference can obviously be made to the food marketing standards determined after this accident, even if they have no strictly medical relevance. This doubtless constitutes an additional reason for reducing radioactive release.

b) Then we come to a second question: should we decide in favour of development with respect to the previous standardized series or should we rather opt for a radical design change? In the French context recalled above and insofar as the overall safety objective remains the same, there would appear today to be no strong incentive for a radical design change in French nuclear power plants. On the contrary, it would seem indispensable to derive maximum benefit from operating feedback, which is considered by all the various organizations concerned as an essential means of improving safety. Moreover, the probabilistic studies performed for the 900 MWe and 1300 MWe plant units provide a basis for identification of relative weak points in the French nuclear units, thus indicating topics for deeper discussion in the context of relatively constant design features.

However, the impact of new projects developed in other countries must not be underestimated, taking into account that certain such projects have interesting safety features and also the possible influence of a decision to build such a new type of nuclear power plant in another country. At the very least, the solutions envisaged in these new projects have to be carefully investigated; achievement of greater simplicity in plant design and greater passivity of systems used to limit the consequences of a primary break are essential topics for prospective discussion relating to the PWR 2000 standardized series, and this opinion is substantiated by the results of the probabilistic studies mentioned above.

However, it is possible that more extensive research into installation simplicity and system passivity involves an approach to safety questions which is considerably different from the "defence in depth" approach and is, therefore, unlikely to develop significantly in the short term.

But, in the long term, there is very definitely room for the development of new projects in France as, it should be borne in mind, the basic design of the type of nuclear power plant constructed in France, dates back to the 1960's.

c) From the present time, even in a development context, and in connection with the previous point a), an in-depth appraisal of confinement is also required. It has already been shown how, without altering the basic design of French power plants, additional measures were taken or planned to improve the role of the containment in the event of a beyond-design-basis accident.

Today, the clear boundary line which used to separate design-basis and beyond design-basis conditions, has completely disappeared. Investigation of severe accidents must be integrated with design itself along with appropriate rules. In short, confinement must be the best achievable in all conditions, from normal operation up to severe accidents.

This concerns, in the first instance, the containment itself and a comparative analysis of the various types of containment already used in France is required (particularly, single pre-stressed concrete containment with leaktight liner and double containment with inner enclosure in pre-stressed concrete and outer enclosure in reinforced concrete), but the possibility of improvements to the containment should also be investigated at the design stage, for example: preventing or retarding basemat melt-through by the corium and, assuming that it is still necessary, integration of the filtered containment venting system. This also concerns the possibility of containment bypass, with current containment design, particularly with regard to problems arising with steam generator tube breaks. Design modification of the steam generator secondary enclosure must, in this connection, be investigated.

d) More generally, a higher degree of design consistency should be sought for the entire installation. In section 1 of this paper, the manner in which French nuclear power plant design has progressively developed was summarized, but it is quite probable that this historical development has provided very significant safety margins for certain conditions and much narrower, or even unknown, margins for certain other conditions. Probabilistic safety studies performed on 900 MWe and 1300 MWe units reveal, as was stated above, a number of relative weaknesses, but it should be added that these studies take only partial account of common mode hazards (currently, they do not deal with earthquake, fire or internal flood hazards). Common mode hazards, along with various degrade modes, the importance of which has been demonstrated by operating feedback (vibration, erosion, corrosion, cavitation, etc.) call for a more detailed investigation.

e) Taking into account the evolution of ideas on installation design and also the operating feedback regarding equipment operation, the question of equipment qualification which has already been extensively investigated in France, including experimental work, needs to be re-thought by integrating this preoccupation from the design stage, insofar as the choice of equipment is essential for safety.

f) Finally, rethinking is required for the man-machine interface. Certainly, some attention will be paid to the installation simplicity and the passivity of systems. But thought must also be given to the degree of automization of certain actions; it is particularly likely that for certain accident sequehces, a higher level of automatization in French nuclear power plants would be beneficial from a safety point of view.

IV Conclusion

The ideas developed in this paper must, of course, be compared to EDF philosophy regarding the PWR 2000 standardized series. At this stage, there is considerable agreement as to the paths to be explored for improvement of safety aspects of the PWR 2000 series with respect to previous standardized series. Evidence of this can be verified by referring to the paper presented to the American Nuclear Society at Seattle on May 2nd 1988, by Mr. TANGUY, General Inspector for Nuclear Safety at Electricité de France, entitled "EDF Approach to the Safety of the next generation of power reactors".

Technical discussions must be pursued between EDF and IPSN concerning the paths to be investigated.

At a later date, we will enter a more formal phase, where Electricité de France submit their proposed safety options for the PWR 2000 series, to the French Safety authorities. The conclusions of the ensuing investigation of these options will then be notified to EDF in the form of directives, before any request is made for authorization to construct a nuclear unit of the new series.

In view of the contextual development and the time still available, it is clear that a more detailed investigation of the safety of the PWR 2000 series is both necessary and possible. This undertaking has already begun.

Novembre 1988

DESTINATAIRES

DIFFUSION CEA

M. le Haut Commissaire
DCS
DDSN
IPSN
IPSN : M. CANDES
OSSN : M. GUILLEMARD
DRSN : M. BUSSAC
DRSN : M. PELCE
DAS/DIR
DAS/SASICC
DERS Cadarache
SES Cadarache
SERE Cadarache
SESRU Cadarache
SRSC Valduc
SEMAR
DPS/FAR + DPS/DOC : Mme BEAU
DPT/FAR
DSMN/FAR
CDSN/FAR : Mme PENNANEAC'H
UDIN/VALRHO
DEDR Saclay
DERPE/DIR Saclay
DRNR Cadarache
DRE Cadarache
DEMT Saclay
DMECN/DIR Cadarache
DRE/STT Grenoble
DRE/SETH Grenoble
Service Documentation Saclay : Mme COTTON (3 ex.)
DERS/DOC/Cadarache : Mme REY

DIFFUSION HORS CEA

Secrétariat Général du Comité Interministériel de la Sécurité Nucléaire
Conseil Général des Mines : M. DE TORQUAT
Service Central de Sûreté des Installations Nucléaires : M. LAVERIE (+ 3 ex.)
Service Central de Sûreté des Installations Nucléaires - FAR
Monsieur le Président du G.P.d. : M. GUILLAUMONT
Direction Générale de l'Energie et des Matières Premières : Mlle TISSIER
FRAMATOME : M. le Directeur Général
NOVATOME : M. le Directeur Général
TECHNICATOME : M. le Directeur Général
TECHNICATOME : Service Documentation
EDF / L'inspecteur général de sûreté et de sécurité nucléaires : M. TANGUY
EDF / SEPTEN (2 ex.)
EDF / SPT
VIENNA INTERNATIONAL CENTRE LIBRARY : Mrs ROSLYN M. STIRLING
M. HOHLEFELDER } Bundes Ministerium für UMWELT, NATURSCHUTZ
M. BREEST } und REAKTORSICHERHEIT - BONN (RFA)
M. KREWER - Bundes Ministerium für Forschung und Technologie - BONN (RFA)
M. BIRKHOFER - Gesellschaft für Reaktorsicherheit - KOLN (RFA)
M. JAHNS - Gesellschaft für Reaktorsicherheit - KOLN (RFA)
M. HAUBER - U.S.N.R.C. - WASHINGTON (E.U.)
M. BECKJORD - U.S.N.R.C. - WASHINGTON (E.U.)

.../...

M. J.S. MACLEOD - Nuclear Installations Inspectorate - LONDON (G.B.)
M. GONZALES - Consejo de Seguridad Nuclear - MADRID (ESPAGNE)
M. José DE CARLOS - Consejo de Seguridad Nuclear - MADRID (ESPAGNE)
M. C. BORREGO - Département de l'Environnement - Université d'AVEIRO (PORTUGAL)
M. E. HELLSTRAND - STUDSVIK ENERGITEKNIK AB - Nuclear Division, Safety and System Analysis - NYKOPING (SUEDE)
M. NASCHI - Direttore Centrale della Sicurezza Nucleara e della Protezione Sanitaria - ENEA - ROMA (ITALIE)
M. P. VANNI - Direttore relazioni esterne e informazione - ENEA - ROMA (ITALIE)
M. ZHANG YU MAN - National Nuclear Safety Administration (CHINE)
M. MA FUBANG, Director of the Nuclear Electricty Office - MIN (CHINE)
M. Itsuro MISUMI - MITI (JAPON)
M. KENICHI MURAKAMI - Science & Technology Agency - Director of the Nuclear Safety Bureau (JAPON)
M. HIROSHI HIROI - Science & Technology Agency - Nuclear Safety Bureau (JAPON)
M. FUKETA - JAERI - Center of Safety Research (JAPON)
M. JAE CHOON LIM - Director of the Nuclear Reactor Division (COREE)
M. Mohamed KARBID - Secrétaire général du Ministère de l'Energie et des Mines (MAROC)

M. CHAVARDES (Attaché près de l'Ambassade de France aux Etats-Unis)
M. DURAND (Attaché Energie près de l'Ambassade de France en Corée)
M. MORIETTE (Attaché près de l'Ambassade de France au Japon)
M. LALERE (Conseiller nucléaire auprès de l'Ambassade de France en Chine)

COPIE (SANS P.J.)

SRDE
LEFH
BAIN
GCSR
SASR
SACP
SAEP
SGNR
SAREP
SAPN
SASLU
SASLU/VALRHO
SEC
SAET
SAED
STAS
SASC
SAEG
SAM
SPI

M. GOURIEVIDIS (Conseiller Nucléaire près de l'Ambassade de France en RFA)