COMMISSARIAT A L'ENERGIE ATOMIQUE

INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE

DEPARTEMENT D'ANALYSE DE SURETE

DAS

CEA-CONF--8650

CEA-DAS--244 R1

FRENCH PWR SAFETY PHILOSOPHY

M. CONTE*

KAIF-KNS Conference
Seoul (Republic of Korea)
29 Apr - 2 May 1986

*IPSN/DAS/SRDE

I. SUMMARY

The French electronuclear program launched in 1970 lays down essentially on the design, the construction and the operating of series of identical pressurized water reactor units (PWR), the only modifications being related to the site specificities.

The first 900 MWe units, built under the American Westinghouse licence and with reference to the U.S regulation, were followed by 34 standardized units, CP1 and CP2 series.

Increasing knowledge and lessons learned from starting and operating experience of French nuclear power plants, completed by the experience learned from the operation of foreign reactors, has contributed to the improvement of French PWR design and safety philosophy.

As early as 1976, this experience was taken into account by French Safety organisms to discuss, with Electricité de France, the safety options for the planned 1300 MWe units, P4 and P'4 series. In 1983, the new reactor scheduled, N4 series 1400 MWe, is a totally French design which satisfies the French regulations and other French standards and codes.

Based on a deterministic approach, the French safety analysis was progressively completed by a probabilistic approach, each of them having possibilities and limits.

As a consequence of the global risk objective set in 1977 for nuclear reactors, safety analysis was extended to the evaluation of events more complex than the conventional ones, and later to the evaluation of the feasibility of the offsite emergency plans in case of severe accidents.

.../...

II. THE DETERMINISTIC APPROACH.

II.1 Basic principles

The main goal of safety analysis is to make sure that the risk to public health and the environment, associated with release of radioactive substances arising from normal operation of a plant, abnormal occurrences and accidents, will remain acceptable.

Therefore, safety analysis could be defined as the set of technical measures necessary to evaluate the potential risk as well as the availability and the efficiency of the devices provided to aim an acceptable residual risk level.

From a safety point of view, the advice on the nature and the importance of the residual risk is based on a deterministic evaluation of the radiological consequences induced by a limited number of conventional operating conditions.

The various situations having to be considered are analyzed applying the defence in-depth concept, and the behaviour of the barriers - fuel cladding, reactor coolant system pressure boundary and containment - and that of the various systems, structures and components, are assessed.

II.2 The defense in-depth concept.

The safety approach is based on the defense in - depth concept, making use of several levels of protection.

- At the first level, sufficient safety margins are provided in design, construction and operating stages to ensure a reliable behaviour of the plant during normal operating conditions.

.../...

- At the second level, protection and safety systems are required to have the necessary redundancy to restore the plant to its normal operating condition after all anticipated transients and incidents.

Margins, protection and safety systems aim at preventing accident occurrence

- At the third level, accidents, whose consequences are supposed to cover all accidental sequences resulting from plausible faults, are taken into account. Safety analysis must ensure that safeguard systems have the necessary redundancy, will be correctly actuated and allow to keep the consequences in the environment below given limits, even for accidents postulated under earthquake conditions and with external power supplies deficiency. The analysis is done with conservative assumptions both for the accident scenarios and for the plant behaviour evaluation.

Safeguard systems aim at mitigating the consequences of the accidents.

The increase in theoretical and technical knowledge and lessons learned from operating reactors, including analysis of PWR accidents and abnomalies, have never brought the defense in - depth concept into question.

III. THE PROBABILISTIC APPROACH.

Historically, the probabilistic approach was used to determine the external events to be taken into account for the design of a nuclear reactor. For a given site, the probability order of magnitude of those events can generally be determined.

Although the justification of the design adopted for French nuclear reactors is essentially based on a deterministic analysis, the Ministry in charge of Industry has, as early of 1977, defined the global risk objective for pressurized water reactors in these terms:

"In general, the pressurized water reactors design should be such that the global probability that the reactor being at the origine of unacceptable consequences should not exceed 10^{-6} per year."

.../...

"Furthermore, when a probabilistic approach is used to evaluate whether a family of events should be taken into account for the design of this type of reactors, it should be considered that this series of events should be taken into account if it is likely to induce unacceptable consequences greater than 10^{-7} per year. This value cannot be exceed for the series ef events examined unless it is possible to show that the probability calculation is pessimistic enough".

"Furthermore, it seems necessary that as soon as possible, Electricité de France will use a probabilistic appproach for the greatest number of events".

Nevertheless, it must be noticed that:

The global probability set at 10^{-6}/year/reactor is an "objective". Safety authorities never required Electricité de France to demonstrate that it is effectively reached.

The global risk objective set at 10^{-7}/year is expressed in terms of "unacceptable consequences" which must be appreciated with regard to the eventual effects due to the site and to the feasibility of public protection.

For the external events, global risk objective set per reactor, per family of events for a given type of aggression and per safety function leads to take into account all types of plausible agressions determined for a given site (explosions, planes, floods...)

With regard to operating conditions to be taken for design, the list adopted in France for the 900 and the 1300 MWe units, complies that of ANSI 18.2 and the following classification has been proposed by Electricité de France for the PWR units.

.../...

Frequency category	Estimated frequency per year	Maximum Radioactive consequences
1	1	Limited by radioactive
2	10^{-2} - 1	effluent releases authorizations (1)
3	10^{-4} - 10^{-2}	5 mSV (entire organism) 15 mSV (thyroid) (2)
4	10^{-6} - 10^{-4}	0.15 SV (entire organism) 0.45 SV (thyroid) (2)

Only the radioactive consequences associated to the first and the second categories are required by regulation. This value is determined for each site, according to its characteristics. For the third and fourth categories, the values have been proposed by Electricité de France and accepted by the safety authorities. Up to now, operating experience has never brought these values into question.

- Furthermore, with regard to the residual risk, safety authorities required in 1980 that studies of accidents not taken into account in the conventional design basis, and including core melt down, be considered in the establishment of the emergency plan.

IV. SAFETY ANALYSIS DEVELOPMENT

IV.1. Overview of the safety problems.

The defense in-depth concept is a very efficient tool for safety analysis providing a thorough examination through its application.

Given the criteria applicable by using the deterministic approach, and especially the single failure criterion, no cumulative failures of mechanical or human origin is postulated in accident studies, no total loss of safety related or safeguard systems and no common mode failures are assessed.

.../...

Furthermore, safety evaluation is based on a standard list of accidents and, quite early, some difficult questions were raised such as whether an exhaustive inventory of plausible accidents has been established and whether the safety level of the plant is consistent with all the plausible accidents.

The most significative illustration of a complex situation an operator has been faced with, up to now, is the THREE MILE ISLAND accident. Due to multiple failures of mechanical components cumulated with human errors, the initial event generates an unforseen accident, severe core damages and core melting.

IV.2. Safety improvements.

Safety has progressed in two main directions :

- search of safety consistency,
- study of severe accidents.

IV.2.1. Search of safety consistency.

IV.2.1.1. Detailed review of the design.

In order to verify that there is no lack of consistency with respect to safety, it was decided that the plant safety should be subject to a detailed review. The approach was purely deterministic, even though lessons learned from operating experience were sometimes used.

The review revealed some weak points needing corrective actions.

- safety related valves.

Some safety valves located in the reactor building could be either flooded or unaccessible after a loss of coolant accident. Their locations have been modified.

.../...

- common mode for cumulative failures.

In-depth evaluation of high energy pipe ruptures and fire conséquences on the real behaviour of the "as built plant" has been performed.

. For high energy pipes, the most conservative ruptures were postulated and, in each concerned building, the consequences of pipe whipping and jet effects were analysed. In one building, the location of the pipe of one system was modified.

. For the fire review, the same approach was applied, assuming fire initiation in various locations of the plants. Fire propagation and consequences were evaluated, taking into account venting systems, fire and smoke detectors, and extinguishers.

- Classification of the " single steam generator tube rupture" event.

In view of the numerous worldwide incidents regarding steam generator tubes, safety authorities requested that, for the N4 project, the complete rupture of a single tube was rated in the third category of design basis events, and the complete rupture of two tubes rated in the fourth category. For the 900 and 1300 MWe units, it was too late to modify the classification; nevertheless safety evaluation of those events are in progress in order to improve the operating procedure to be applied, and to improve the reliability of the discharge and isolating devices and the preventive control technics.

IV.2.1.2. Inventory of plausible accidents.

With respect to the risk objectives previously defined, the probability and the consequences of the total loss of several redundant systems that are important for the plant safety, have been evaluated :

. electrical power supplies,
. steam generator feedwater,
. ultimate heat sink,
. anticipated transient without scram (ATWS).

.../...

The evaluations led to the following conclusions :

- the probability is higher than 10^{-6} /year/reactor.
  This value can be associated with the fourth category of the design basis accident probability,

- these initial events could lead, within a few hours, to severe core damages.

As early as 1977, Electricité de France was requested, for the 1300 MWe units, to define appropriate actions in order to reduce the probability of those events or decrease the resulting consequences with respect to their probability. The appropriate actions could be complementary devices as well as new procedure to operate the existing systems.

As the order of magnitude of the probability values is around 10^{-5} and 10^{-6} /year, these accidents were considered as complementary situations, and safety authorities agreed studies to be performed on the basis of realistic hypothesis and methods. Risk improvement has been evaluated with regard to the core melting probability. For the nature and the safety requirements associated with the features or devices to be implemented, a case by case examination has been performed for each type of accident.

The complementary devices never induce a remodeling of the initial design. For the 1300 and 1400 MWe units, they were requested at the design stage, and for the 900 MWe units, they were adapted to the preset design.

The following procedures and main devices are planned to cope with these situations:

.../...

- Total loss of electrical power supplies procedure.

  . feedwater to the primary pump seals by the existing test pump, electrically supplied by a turbogenerator. The turbogenerator, feeded by the steam of the steam generators, allows also to supply some protection and measurement systems,
  . resupply of electricity from a house load operating plant. or by a diesel generator of another unit.

- Total loss of steam generator feedwater procedure.

  . Cooling of the core by feed and bleed. The procedure conducts the operator to open the pressurizer relief valves, to initiate safety injection system manually, and to stop the primary pumps.

- Total loss of ultimate heat sink procedure

  . early detection, from the control room of heat sink loss,
  . feedwater supply to the primary pump seals, as for the total loss of electrical power supplies,
  . supply of water to the unit from any another water source possibility on the site (pit, water cooling tower, fire-fighting water...).

- ATWS procedure

  . diversification of the signals ordering turbine trip and start up of auxiliary feedwater system.

.../...

Furthermore, long term reliability studies have been performed on the low safety injection and the spray systems required after a lost of coolant accident to remove the residual heat. These studies led to the conclusion that pumping equipment failures could occur. As the pumping equipment of both systems are redundant and equivalent, the possibility of using any available pump to fulfil any function through a preset connecting pipe has been foreseen in order to improve the reliability of the heat removal function.

IV.2.1.3. Severe accident studies.

According to the defense in depth concept, two main objectives were aimed by studying the severe accidents : prevention of the core degradation, delay and mitigation of their radioactive consequences in the environment.

o In abnormal operating conditions, the safety of a plant is as dependent on the correct operation of the automatic orders and associated systems as it is on operator actions.

To attempt to avoid the degeneration of an initial event into a severe accident leading to core degradation if the proper actions are not taken, Electricité de France has proposed a new operating procedure based on the characterization of every possible cooling state of the core.

Contrary to the standard procedures based on sequential scenarios, this procedure does not prejudice any accident initiator or any accident development sequence. It can also be applied in the case of cumulative failures of human and/or mechanical origin. It specifies the actions to be taken by the operator, on the basis of data relevant to actual reactor status, to restore the situation : i.e. water level measurement, boiling margins, temperature measurement under the containment dome.

.../...

Furthermore, in order to minimize operator errors, including inappropriate scope or wording of operating rules during abnormal situation a Safety engineer (I.S.R.) analyses the plant status and its evolution independently of the operating team evaluation.

This procedure and the operation aid provided by the I.S.R. are presented in another french lecture (Experience gained in operation in French PWR Nuclear Plants. Session 1-B).

o In case of core melt down, the containment should constitute the ultimate barrier wich would avoid or, at least, reduce the radioactive releases in the environment to a level compatible with the feasibility of the emergency plan.

The safety analysis of severe accidents led to some specific procedures to cope with a containment isolation failure, to prevent a direct pathway to the environment in case of base mat melt through, to depressurize preventively the containment through a coarse filter.

CONCLUSION

Increasing knowledge and lessons learned from operating experience have contributed to the French safety philosophy improvement.

The methodology now applied to safety evaluation develops a new facet of the in depth defense concept by taking highly unlikely events into consideration, by developing the search of safety consistency of the design, and by completing the deterministic approach by the probabilistic one.

Nevertheless, the complexity of nuclear reactors is such that it will never be possible to affirm, in spite of the improvements on reactor design and operating procedures, that a severe accident will never present any difficulty to the operator to cope with it.

Juillet 1986

DESTINATAIRES

DIFFUSION CEA

M. le Haut Commissaire
DSE
DDS
IPSN
IPSN : M. SCHMITT
IPSN : M. CANDES
DRSN : M. BUSSAC
DRSN : M. PELCE
DAS
SRDE
BDSN
LEFH
BAIN
GCSR
SASR
SACP
SAEP
SGNR
SAREP
SASICC
SASLU
SASLU/VALRHO
SEC
SAET
SAED/FAR
Monsieur le Président du G.P.u.
Monsieur le Président du G.P.d. : M. GUILLAUMONT
STAS
SASC
SAM
SPI
BEP
DERS Cadarache
SES Cadarache
SERE Cadarache
SIES Cadarache
SESRU Cadarache
SRSC Valduc
SEAREL
DPS/FaR
DPT/FaR
UDIN/VALRHO
DEDR Saclay
DRNR Cadarache
DRE Cadarache
DER Cadarache
DEMT Saclay
DMECN/DIR Cadarache
DMECN Saclay
DTCE Grenoble
DSMN/FAR
Service Documentation Saclay : Mme COTTON (3 ex.)

DIFFUSION HORS CEA

Secrétariat Général du Comité Interministériel de la Sécurité Nucléaire : M. LAJUS
Service Central de Sûreté des Installations Nucléaires : M. LAVERIE (+ 3 ex.)
Service Central de Sûreté des Installations Nucléaires - FAR
Direction Générale de l'Energie et des Matières Premières : M. FRIGOLA
Conseil Général des Mines : M. MEO
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 nucléaire : M. TANGUY
EDF / Etudes et Recherches (CHATOU - CLAMART)
EDF / SEPTEN (2 ex.)
EDF / SPT
M. BREEST - Bundes Ministerium UMWELT und NATURSCHUTZ und REAKTORSICHERHEIT - BONN (RFA)
M. KREWER - Bundes Ministerium für Forschung und Technologie - BONN (RFA)
M. BIRKHOFER - Technische Universität München - GARCHING (RFA)
M. HOHLEFELDER - Gesellschaft für Reaktorsicherheit - KOLN (RFA)
M. LEVEN - Gesellschaft für Reaktorsicherheit - KOLN (RFA)
M. HAUBER - U.S.N.R.C. - WASHINGTON (E.U.)
M. MINOGUE - U.S.N.R.C. - WASHINGTON (E.U.)
M. GITTUS - U.K.A.E.A. - Safety and Reliability Directorate - RISLEY (G.B.)
M. HANNAFORD - Nuclear Installations Inspectorate - LIVERPOOL (G.B.)
M. GONZALES - Consejo de Seguridad Nuclear - MADRID (ESPAGNE)
M. PERELLO - Consejo de Seguridad Nuclear - MADRID (ESPAGNE)
M. C. BORREGO - Département de l'Environnement - Université d'AVEIRO (PORTUGAL)
M. CARLBOM - Department of Safety and Technical Services - NYKOPING (SUEDE)
M. NASCHI - Direttore Centrale della Sicurezza Nucleara e della Protezione Sanitaria ROMA (ITALIE)
M. INABA - MITI (JAPON)
M. ISHIZUKA - Science & Technology Agency - Nuclear Safety Bureau (JAPON)
M. TAMURA - Science & Technology Agency - Nuclear Safety Bureau (JAPON)
M. FUKETA - JAERI - Center of Safety Research (JAPON)

COPIE (SANS P.J.)

M. CHAVARDES (Attaché près de l'Ambassade de France aux Etats-Unis)
M. FELTEN (Attaché près de l'Ambassade de France au Japon)
M. WUSTNER (Attaché près de l'Ambassade de France en RFA)