DESIGN CRITERIA FOR ADVANCED REACTORS

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

INTRODUCTION

The design and operation of a nuclear power station must satisfy a certain number of criteria.

Amongst these, certain concern safety and are generally imposed by Safety Organizations acting on behalf of the Authorities of the countries where the Nuclear Power Station will be operated.

Some of these criteria are the subject of consensus at international level. Such criteria have been clearly given in the INSAG 3 document, prepared by A.I.E.A.

This consensus is desirable, but also necessary for the following reasons :

- the number of nuclear power station constructors is limited and market rules impose a common language.
- there are many Electrical Operators, who do not always have sufficient capacity to ensure that the nuclear power station network is economically self sufficient. They do not want to be more demanding than their neighbours and want to benefit from the experiences acquired by other Operators.
- the Authorities realized that it was in everyone's interest to have common regulations, not only due to an awareness of trans border effects but also because pooling Research and Development analysis and actions was profitable.

Nevertheless, not only the definition of a certain number of criteria is within the competence of the Operator, and notably, those relative to the power stations operation, but it is desirable that the Operator's advice is taken into consideration during the definition of the safety criteria.

Indeed Operator participation thus enables demands which might not take into account operating constraints to be reduced. They also enable an ratchetting of advocated measures to be avoided which notably could risk increasing the kWh cost, and thus decreasing the appeal of nuclear energy.

A consensus between Operators, in order to contribute to the creation of common safety regulations, thereby simplifying competition between manufactures could prove to be useful. This would also apply with respect to the main plant, with the objective of avoiding a large number of different designs.

This would enable a consistent and high quality design to be achieved and enable the design to benefit from experience feed back.

SITE

The main site related considerations, besides conventionnals aspects concerning its choice (network, heat sink, access, etc ...) is related to the definition or not of an exclusion zone and the need or not to provide for an evacuation plan.

There seems to be some misunderstanding about the reasons leading to the existence of such a plan.

Indeed, for design basis accidents, one can always conceive a reactor which only discharges a moderate quantity of radioactive products.

However, it is possible to postulate a "beyond design basis" event which could lead to a larger release of radioactive material.

In this case of a deterministic approach, measures should be adopted to protect the neighbouring population. These hypothesis correspond to the severe accident situation. This approach can develop with time. As a reminder, it is sufficient to recall the 1966 AEC criteria where there severe accident notion was implicitly classified in the residual risk. The "RASMUSSEN" WASH 1400 report exposed this notion. Following this, and notably after the TMI accident, emergency plans associated to an estimation of a Source Term and a certain probability level resulted.

The extend to which this approach is adopted varies according to the appraisal of each Authority of each Country and the state of knowledge.

Typically in FRANCE, this Source Term level enables the population evacuation to be limited to a zone defined by a radius of 5 km around the power station (for the zone from 5 km to 10 km, it is sufficient to confine people inside their residences). It rests with the designer to take the necessary measures to ensure that the Source Term escaping the radioactive product confinement is limited to this level. Any circumstance leading to a higher Source Term, must have a probability level, sufficiently low to be classified in the residual risk.

For current, reactor design, the probability is less than 10_{-6} per reactor-year.

For a new design project, one can always see to it that the producted probability of an analogous Source Term is lower than those generally accepted at the moment, (which pushes back the residual risk to an even lower value). Howewer, at these very low levels, there are two major difficulties :

- single failures of very low probability but with very serious consequences become dominant (e.g. very strong earthquake) : or, the assesment of the probability of such events is very difficult
- one does not know how to evaluate the risks of human error or common mode at such a low level.

Howewer because of the uncertainties in determining the probabilities of such aspects and for others reasons, it may be necessary for the safety autorities to provide guidance on the values which then would accept at any particular times.

To state that one can build and operate a reactor which offers no radioactive release risk whatsoever is thus likely later on, to hinder the Operator who would have serious difficultie in continuing his operation to respect too strict a criteria that he would have fixed himself "à priori" : an example will enable this matter to be illustrated : for a pressurized water reactor an accident concerning steam generator tube breakages, can result in radioactive product release, which, although the consequences would be considered as benign, can hinder the operator if he had mentioned this unlikely hypothesis during the design phase. Such a discourse would be going back 20 years when the nuclear community used to proclaim that nuclear was safe, period.

MAINTENANCE - REPAIRABILITY

Problems related to maintenance and the possibility of repairing or replacing structures or components of a nuclear power station, do not at first sight appear to be in the Safety domain.

The Operator attaches considerable importance to the fact that the plant supplied to him to produce electrical energy is easy to maintain, for economic reasons, and for the requirement to limit doses received by its personnel or those of the Companies to whom the maintenance work has been entrusted, but also to limit the risks of human error.

The possibility of repairing relatively easily, all components and structures of the power station is also an appreciable factor for the choice of plant.

This protection of the investment attitude is all the more justified as recent events which have occurred in nuclear power stations have lead to long duration shutdowns and even final shutdowns.

These problems are also of direct interest the Safety Authorities, as much as the Operator.

These considerations result in doubts being expressed on certain new integrated reactors qualified as intrinsically safe, but which are founded on a design slightly or indeed not accessible at all.

"GRACE PERIOD"

In the various international meetings where different advanced reactor models were presented, a notion called "Grace Period" appeared, characterizing the project without clearly defining the reasons leading to the definition of the corresponding time.

The term of "Grace Period" is defined by a paper from A.I.E.A. as a period of time during which safety is ensured without the necessity of personnel action or attendance in the event of an incident/accident.

Also, the Grace Period being suggested varies considerably, giving the impression that this idea has a more public relation aspect than a technical basis.

It would therefore be advisable to consider what is actually meant by "Grace Period".

For example, there are various possibilities related either to the actions of the operators or to those of the Public Authorities.

It would therefore be advisable to define at the beginning, the actions to be carried out and then estimate the time required to do it. Here there example are a few suggestions :

- following an accident, what is the delay given to the operator, in order that he has time to "gather his wits" before any intervention from his side ? Can this delay be a function of the type of event ?
- in a worsening situation, what is the delay required for an analysis team to be formed, and have the time to interpret the information received, in order to usefully advise the Operator.
- What is the delay for measures the application of accident management procedures.
- Following an accident, what is the delay necessary for the Public Authorities to take the decision to implement an emergency plan ?
- Once this decision is taken, what time is required to implement the emergency plan ?
- A solution which seems simple but not necessarily realistic industrially, would be to include all these elemental times.

One thus ends up with a reactor design where no human intervention is involved in the reactor control systems during this defined time. This is in fact the path chosen for the reactors proposed as "intrinsically safe", though, however, the more or less important duration stated, but being at least several days, does not seem to correspond to a well defined criteria.

It would seem more advantageous perhaps to determine the problems and define the criteria case by case.

The problem is made more difficult because it is advisable to take other parameters into account related to the instrumentation and control of the power station, for example : the idea of the forgiving reactor intervenes, as well as that of the possibility or not of letting the operator take certain initiatives.

However, the Operators have a certain part to play in the definition of these criteria.

To satisfy the previous conditions, that is to say, obtain a certain delay, various means can be envisaged.

The first consists in applying redundance at a more or less high level, associated or not with diversification, to limit the common mode effects.

Virtually all existing reactors were conceived in this way. Taking severe accidents into consideration, that is to say, lowering the probability level defining the residual risk, led to wondering about the use of other means to enable the system's thermal inertia to be increased.

The objective is obtained either by increasing design margins, or using systems utilizing "passive" design.

Utilization of passive safety design has already been used, in varying degrees at the beginning of the reactors design. One can cite for example, natural circulation core cooling, gravity insertion of the reactor control systems, use of accumulators during a primary circuit depressurization.

A more extensive use of the passive safety design is conceivable. This generally results in the adoption of major water reserves (under pressure or without), associated or not with systems using the gravity principle (the special case of natural circulation being relative to a closed circuit).

Increasing design margins is more difficult to understand. One imagines that this method can simplify the Operators role. Indeed, trip thresholds are generally more difficult to reach during transients because of the control drift.

The indirect effect on safety, resides therefore in the reduction of the number of calls on the auxiliary circuits, giving lower material loading, and for a given reliability level, a lower degradation risk.

A second aspect concerning these margins is the following : inherently in the determinist method in the design, the margins are really necessary, in order to provide against situations not taken into account in the design. An increase of these margins, thus following the in-depth defense principle, should increase the resistance quality of the various barriers.

On the contrary, a considerable increase of the grace period, so as to gain time, seems difficult to achieve by using this procedure.

How to choose between all these methods : redundance, diversification of active components, passive design and increase of margins during the design of a new project ?

Several parameters have to be taken into consideration to make a judgement : notably past experience, and cost for a required safety level.

THE HUMAN FACTOR

The importance of the human factor in nuclear power station safety, at least in western countries was emphazised by the TMI incident.

Although a significant level of agreement on post TMI measures has been obtained, there is however different conceptions by the designer of the role of the operator post accident after the 20/30 minutes period.

From the original design where the Operator directs the implementation procedure of the various safeguard auxiliary circuits, up to futurist projects where human intervention is not necessary for a period of time sometimes exceeding several weeks, quite a graduation can occur. The interaction with the previously defined time (Grace Period) is evident.

A point however is worth noting. During the progression of an accidental procedure by automatic systems, or the utilization of physical laws (passive system), even if the intervention of the operator is not necessary, can he act or not ? Must he have or not the control console keys mechanism during such a procedure ? Can the operator modify or not what has been established during the design studies ? If yes, is he allowed to make a mistake, and how many times ? That is to say, must it be a forgiving design system, and at what level ? How many successive mistakes can be tolerated : zero, one, two ... ?

This point is worth analysing in the framework of future reactor designs. Indeed one can imagine that advice can be varied. The degree of confidence in human intervention to reestablish a situation, consecutive to an accident which does not progress as foreseen, is of subjective order and it seems difficult to measure its weight. In general, unfortunate consequences due to a human error stay in the memory. Satisfactory actions are never the subject of special reports, and that is good. But do we not ever-estimate the capacity of human intelligence, to foresee all possible eventualities during the design studies, which include poor functioning of the equipment comprising the different systems called into use and whose reliability is not total.

CONCLUSION

In addition to the aspects which have just been broached, one could :

1. The specifications required by the electrical network ; It would be interesting to establish a table of different Operators requirements.

2. The use of probabilistic analysis (P.R.A.) : a meeting organized by AIEA took place in VIENNA in May on this theme. The benefits and limitations of the probabilistic method in new project design was exposed. Many other meetings have taken place or are foreseen on this subject. Initially it would be preferable to prepare a dossier on the comparison of input data and especially date relative to common modes and the human factor.

3. Severe accidents : there is a large consensus of agreement that in the future, the means to control a severe accident should be taken into consideration from the start of the design. But in the current state of knowledge, it is preferable to wait for the conclusions of International, "Severe Accident" working groups as NEA-OECD.

4. Equipment qualifications and especially those required in case of an accident must be the subject of a comparative study. But this point is not a characteristic of advanced reactors and could therefore be taken in another context.

In conclusion, I think these joints should be studied :

- define what is meant by "Grace Period"
- Study the "man-machine" interaction in the sense of operator intervention during an automatic procedure
- the problem of safeguarding the investment, the translation of which is the repairability of the internal structures
- specifications required by the Operator concerning the electrical network
- relation roles of determinate and/or probabilistic approaches
- role of accident management in risk reduction
- means of demonstrating the reliability for revolutionary design (passive system).

RESEARCH AND DEVELOPMENT ON FUTURE LIGHT WATER REACTORS AT THE CEA, FRANCE

A. LERIDON
Direction des réacteurs nucléaires,
CEA, Centre d'études nucléaires de Cadarache,
Saint-Paul-lez-Durance, France

Future Reactors and particularly P.W.R. will have to be safe, competitive and acceptable by public opinion. As the future of international environnement is somewhat difficult to foresee, the Research and development wil have to be open and to take into account various items as:

-Possible evolution of international or "regional" Regulations about waste and Safety, particularly in the field of severe accident.
-New propositions of different kind of Reactors on the international scene.
-Various Strategy on Uranium and fuel cycle.
-New industrial strategy and Utilities agreements.
-...

These are the reasons why, the Commissariat à l'Energie Atomique is involved in an R&D programme, in cooperation with EDF (REP 2000 Programme) and Framatome. Main subjects are as following:

1- Evaluation of different either "evolutionnary" or "passive safety" Reactors under three different aspects:
-Thermalhydraulics and safety margins evaluation in terms of linear power, hydraulic pressure drop, etc.
-Operation problems, particularly when a passive system is not operating.
-Reliability and failure probability with the associated consequences.
2- Absorbers evolution and possible limitation of soluble boron.
3- In core instrumentation.
4- Post accident instrumentation.
5- Severe accident : Prevention and mitigation as long as the core fusion probability cannot be eliminated.
6- Confinement.
7- Operator Assistance.
8- Fuel evolution.

Some of these subjects will be integrated in the REP 2000 Programme. In a preliminary phase, the need of experimental programme will be evaluated but at this stage the R&D will not be related to a given design.