(ips) ite 95000758
FR9503255

IPSN

RAPPORT

RAPPORT DES/226

COMMON SAFETY APPROACH FOR FUTURE PRESSURIZED WATER REACTORS IN FRANCE AND GERMANY

FRISCH W., JAHNS A ,
QUÉNIART D., GROS G

cea INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE
DEPARTEMENT D'EVALUATION DE SURETE

RAPPORT DES/226

COMMON SAFETY APROACH FOR FUTURE PRESSURIZED WATER REACTORS IN FRANCE AND GERMANY

FRISCH W., JAHNS A.*
QUÉNIART D., GROS G.**

ANS, International Topical meeting
on advanced reactors safety,
Pittsburgh, Pennsylvania, April 17-21, 1994

* GRS
** DES/DIR

COMMON SAFETY APPROACH FOR FUTURE PRESSURIZED WATER REACTORS IN FRANCE AND GERMANY

W. Frisch, A. Jahns
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Garching and Cologne, Germany

D. Quéniart, G. Gros,
Institut de Protection et de Sûreté Nucléaire (IPSN)
Fontenay-aux-Roses, France

I. BACKGROUND

In France and Germany all major activities related to future pressurized water reactors are now proceeding in a coordinated way among the two countries. This holds for utilities and industry in the development of a joint PWR project, the "European Pressurized Water Reactor (EPR)" by Electricité de France (EDF), German utilities, Nuclear Power International (NPI), Framatome and Siemens as well as for the technical safety organisations GRS and IPSN who are developing safety objectives for future evolutionary reactors on the basis of a common safety approach adopted by the safety authorities of both countries for plants to operate from the beginning of the next century.

The proposed paper covers this common development of a safety approach and particular technical safety objectives.

Cooperation between GRS and IPSN in the field of nuclear safety has been performed for many years and has been intensified in recent years. One of the major activities is the preparation of a joint safety approach for future pressurized water reactors. The results of these activities are documented in a common report[1] and form the basis for a common proposal of the two advisory committees GPR (Groupe Permanent chargé des Réacteurs nucléaires) in France and RSK (Reaktor-Sicherheitskommission) in Germany, which has been finalized and adopted on May 25, 1993, as "GPR/RSK Proposal for a Common Safety Approach for Future Pressurized Water Reactors"[2]. The national safety authorities BMU (Federal Ministry for Environment, Nature Conservation and Reactor Safety) of Germany and DSIN (Direction de la Sureté des Installations Nucléaires) of France have adopted the content and officially published translations in their national languages.

The main topics of this document will be presented in this paper, together with a rationale for the approach and the recommended technical principles.

II. GENERAL APPROACH

A significant safety improvement in the design of the next generation of nuclear power plants (compared to existing plants) is feasible and necessary despite of the satisfactory safety records of operating nuclear power plants in both countries. It is believed that the appropriate way to achieve this for plants to operate from the beginning of the next century (e.g. near 2005) is the "evolutionary way", taking into account lessons learned from operating experience and from results of PSAs of existing plants as well as results of safety research, notably on severe accidents. Nevertheless, the introduction of "innovative" features must also be considered in the design; especially in the area of severe accident prevention and mitigation.

All these efforts will lead to a significant reduction of the probability of occurrence of accidents and moreover of the radioactive releases during accidents, including severe accidents with major core damage.

The "defence-in-depth" principle remains the fundamental principle of safety, also for these future nuclear power plants; this means e.g. the implementation of several levels of protection including successive barriers against radioactive releases to the environment.

In compliance with the "defence-in-depth" principle and in fulfillment of more stringent limitations of radioactive releases after severe accidents, special attention has to be paid to the containment design (see below). In general, different ways are possible to improve the safety of future PWRs, as illustrated in fig. 1.

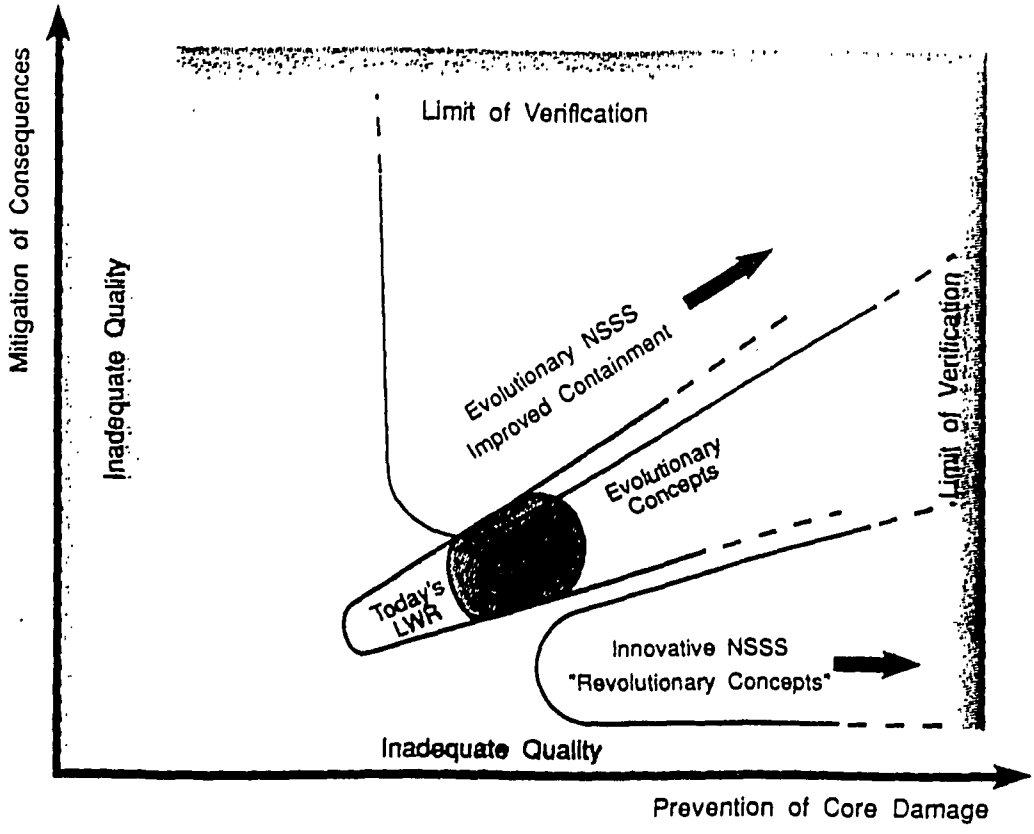

Fig. 1: Possible ways of safety improvement for future reactors

Qualitatively the directions of the two axes indicate preventive measures against core melt (horizontal) and mitigative measures to cope with consequences of core melt situations (vertical). Proceeding along the two axes from the center can also be interpreted as improving the design of the NSSS and the safety system (horizontal) and improving the strength and tightness of the containment (vertical).

Most of today's LWRs can be placed in the marked area, with sufficient distance from the area of inadequate quality and with emphasis on design features to prevent core melt (below a "balance"-line from the center to the right upper corner). "Evolutionary" concepts will probably expand to the right with the same angle. There is an overlap between present and evolutionary plants, because the "evolution" is not synchronous in all countries, which means the respective reference plant to which the new design is an "evolution" is not from the same year for all evolutionary designs. The aim of "revolutionary" or "innovative" designs such as PIUS and SIR is to considerably improve the design against core melt, or even try to completely eliminate core melt, thus not requiring specific containment design features to cope with the consequences of core melt situations (lower right area in fig. 1). The right boundary of fig. 1 indicates that there is a limit to prove a safety improvement (e.g. the reduction of core melt frequency), especially when approaching very low values for core melt frequency.

Another approach in the spirit of the "defence-in-depth" concept is to provide design improvements with respect to both core melt prevention and mitigation of core melt consequences, which is equivalent to drastically reduce the releases of radioactive material after core melt by strengthening the containment functions. This may include the implementation of innovative features. The French-German safety approach is aiming at this direction. This figure indicates that the highest proven safety level can be achieved with a design which is balanced with respect to prevention and mitigation. Compared to present reference plants, more effort shall be devoted to strengthen the containment function.

III. MAIN SAFETY OBJECTIVES OF THE FRENCH-GERMAN APPROACH

Based on the general approach very briefly sketched above, the main safety objectives stated in the GPR/RSK approach are:

- a significant reduction of the global core melt frequency must be achieved for the nuclear power plants of the next generation,
- accident situations which would lead to large early radioactive releases have to be "practically eliminated". When they cannot be considered as physically impossible, design provisions have to be taken.
- low pressure core melt accidents have to be taken into account in the design such that the associated maximum conceivable release would necessitate only very limited protective measures in aea and in time. This can be expressed by no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in consumption of food,

Another important objective related to normal and abnormal situations is the reduction of individual and collective doses for the workers, which are largely linked to maintenance and in-service inspection activities.

The way in which these objectives can be met is expressed in technical principles to be fulfilled within the design. The most important technical principles are presented in the following paragraphs.

IV. TECHNICAL SAFETY PRINCIPLES

a) Reduction of Core Melt Frequency

The first objective related to a reduction of the frequency of occurrence of accidents can be met by following several technical safety principles such as increasing the quality of design, manufacturing, construction and operation, reducing the frequency of initiating events, improving plant transient behaviour and man-machine interface, optimizing redundancy and diversity of safety system functions and considering passive system functions.

Reduction of Frequency of Initiating Events

A reduction of the frequency of occurrence of accidents (including core melt accidents) has to be obtained among others by reducing the frequency of initiating events. The aim of reducing the frequency of initiating events implies to evaluate operating experience, to increase, as far as possible, the reliability of operational systems and components (e.g. main feedwater system) and to eliminate to the largest extent possible the occurrence of phenomena which appeared to be the cause of significant failures (vibrations, corrosion, cavitation, etc.).

Design solutions to reduce the frequency of initiating events have to be considered for relatively frequent events and also for those less frequent events which nevertheless have a measureable contribution to the total core melt frequency (e.g. small leaks). It is important to consider initiating events during all operating states, including full power, low power, and all relevant shutdown conditions.

Improved Plant Transient Behaviour

Improvements can be achieved by making the plant behaviour less sensitive to operator errors and failures in operational systems, e.g. by proper automatic control and by the provision of sufficiently large coolant capacity in the primary and the secondary coolant systems and in the primary and secondary feed systems. One objective is to increase grace periods for necessary operator actions.

To the extent possible, unnecessary safety system actions shall be avoided, e.g. during all anticipated transients coolant pressure should be limited such that pressurizer valves do not open (risk of stuck open pressurizer valve). One means to avoid unnecessary safety system actions can be the introduction of "limitation systems" which are additional high quality control devices acting when the operational control system is not capable of keeping parameters within given limits.

Redundancy and Diversity

For events which are not controlled by the operational systems (control and limitations systems), protection and safeguard systems are required to keep the plant in a safe state. The reliability of these systems must be consistent with the general objective of reducing the probabilities of occurrence of accidents, taking into account the estimated frequencies of initiating events and the duration of the corresponding actions of the systems. This reliability has to be achieved through the use of redundancy and diversity. Due attention has to be paid to the fact that possible common cause failures limit the potential to reduce the unavailability by adding identical trains, as well as to the fact that diversity can imply more complex systems and maintenance difficulties. (The availability of a redundant safety system consisting

of identical trains probably cannot be demonstrated to be less than 10^{-4} per demand).

Particular attention has to be given to minimizing the possibilities of common cause failures. The principle of physical and spatial separation shall be applied as far as possible. This is also an effective defense against internal hazards such as fires and flooding. Support functions (energy, control, cooling, etc.) shall also be independent to the largest degree possible. Special emphasis has to be placed on the redundancy and diversity of electrical power supply. An emergency control facility from which necessary safety actions can be performed must be provided for the case of evacuation of the main control room.

Active vs. Passive Systems

The advantages and disadvantages of passive systems have to be analyzed. The essential advantage is the independence from external energy supply. Drawbacks are e.g. lower driving heads in fluid systems and less operational flexibility. Furthermore active components may be necessary for startup and shutdown. Special attention has to be paid to difficulties in estimating the reliability of new passive systems in view of the state of knowledge and experience.

Man-Machine Interface

Due consideration has to be given to human factors throughout the design stage, taking into account aspects of operation, testing and maintenance with special emphasis on operating experience.

Minimizing operator errors and making the plant less sensitive to those errors can be achieved by applying appropriate ergonomic design principles and by providing sufficiently long grace periods for the response. The necessary length depends on the complexity of the situation to be diagnosed and on the actions to be taken.

Sufficient and appropriate information shall be made available to the operators for a clear understanding of the plant status, including severe accident conditions, and for the clear assessment of the effects of their interventions. Emphasis should be laid on the use of computer techniques for reliable diagnosis systems for operator support.

Qualification of Computerized Systems

In order to obtain the necessary high reliability for computerized instrumentation and control systems, the designer has to conduct the qualification of such computerized systems, including software. The problem of on-going qualification of software has to be taken into account. The three main principles for designing computers for safety systems are fault avoidance, fault removal and fault tolerance.

b) Elimination of Situations with Large Early Radioactive Releases

Accident sequences which would lead to large early releases have to be "practically eliminated". An accident sequence is meant to be "practically eliminated" if it is physically impossible (e.g. hydrogen detonation after inertisation of the containment) or if proper design provisions are taken to make it extremely improbable (to "design it out"). Implications for the concerned accident situations are as follows:

- Accident sequences involving containment bypassing (via the steam generators or via interfacing systems) have to be "practically eliminated" by proper design provisions (such as adequate piping design pressure and reliable isolation).
- Reactivity accidents resulting from fast introduction of cold or deborated water must be prevented by design provisions so that they can be "excluded". Within the safety demonstration an event or an event sequence can only be "excluded" if sufficient design and operation provisions are taken so that it can be clearly demonstrated that it is possible to "practically eliminate" this type of accident situation.
- High pressure core melt situations must be prevented by design provisions (such as diversity and automatic actuation) for the secondary side safety systems, the reactivity control system and primary feed and bleed systems. It must be a design objective to potentially transfer the high pressure core melt conditions to low pressure core melt sequences with a high reliability so that high pressure core melt situations can be "excluded". The depressurization must be such that loads from ejected melt into the containment atmosphere ("direct containment heating") and loads on the reactor pressure vessel support and cavity structures can be coped with.
- Global hydrogen detonation and in-vessel and ex-vessel steam explosions threatening the containment integrity must be "practically eliminated".

c) Limitation of Radioactive Releases after Core Melt Accidents

The third objective calling for a significant reduction of radioactive releases, even after core melt accidents, has a considerable impact on the containment design:

- There shall be no path of direct leakage from the containment building to the outside. Where impossible for practical reasons, pipes liable to carry radioactive substances outside the containment building shall lead to peripheral buildings providing adequate confining capabilities. Improvements must be sought for the permanent surveillance of the containment building leaktightness.
- For the containment, an internal liner should be considered in order to assure the low leak rates required after low pressure core melt accidents.
- Due consideration must be given to the different aspects of a spray system inside the containment building for severe accident situations: temporarily it allows lowering both the pressure and the radioactive aerosol concentrations of the containment building. However, a spray system will reduce the inerting influence of steam and increase the flame velocity of hydrogen combustion, if it occurs.
- The residual heat must be removed from the containment building without venting device: This heat removal system should preferably be passive with respect to its primary circuit inside the containment.
- Concerning the possible formation of combustible gas mixtures, it is considered that the containment building must be designed to withstand a global deflagration of the maximum amount of hydrogen which could be contained in this building in the course of core melt accidents and also to withstand a representative fast local deflagration. Besides, provisions must be taken with respect to local detonations and to possibilities of deflagration to detonation transition (DDT) sequences, which might jeopardize this building and its internal structures. Limitation of the concentrations of combustible gases by design of internal structures and the use of catalytic devices and igniters have to be considered. As an alternative, inertisation of the containment may be considered.

V. PROBABILISTIC APPROACH AND METHODS

For the next generation of nuclear power plants, a general objective is to reinforce the "defence-in-depth" of plants. To achieve this, the design should be made on deterministic bases, supplemented by the use of probabilistic methods. The objective should be reached considering the results of operating experience and of in-depth studies like probabilistic safety assessments conducted for pressurized water reactors (PWR).

Such assessments have been conducted for existing French and German plants. They have shown that probabilistic safety assessments are essential tools to gain an in-depth understanding of the relative weaknesses in the plants and to deal with complex situations involving several equipment failures and/or human errors.

Improvements in plant design can be derived from those probabilistic safety studies already performed for existing plants. However, PSA is also a valuable tool to be applied to the new design itself.

The conduct of probabilistic safety assessments and the establishment of quantitative probabilistic targets are important tools at the design stage to gain an in-depth understanding of the relative weaknesses in the plants and to deal with complex situations.

A PSA at the design stage of future PWRs shall be performed with the following objectives: supporting the choice of design options, including redundancy and diversity of the safety systems, well-balanced safety concept and valuation of expected deviations from present French and German safety practices.

PSA is believed to give valuable supporting information and results with respect to the first safety objective on a significant reduction of core melt frequency.

Evaluation of PSA results against quantitative probabilistic targets can provide useful guidance. But, generally speaking, quantitative probabilistic targets are not to be seen as requirements; they are essentially meant to be orientation values for checking and evaluating the design. In addition, the application of PSA at an early stage of design has to be handled cautiously because the final results will be dependent on the real choice of components, system techniques and operational procedures. However, a PSA applied to an evolutionary concept provides better

substantiated results than for completely new designs because data for components and systems which are already proven in operation can be used.

Concerning the general methodology, the PSA could be carried out in two or more steps: a simplified assessment at the conceptual stage, and more complete studies during the engineering phases, when more precise information on the design becomes available.

VI. HARMONIZATION OF EXISTING NATIONAL SAFETY APPROACHES

In previous chapters such items of the safety approach have been mentioned which aim at a safety improvement compared to existing safety practice. For future reactor concepts many existing safety principles and rules are still applicable. In a common safety approach of two countries which have developed their safety philosophies and approaches independently for a long period of time (though with a considerable amount of similarity) an harmonization process with respect to existing regulations is necessary. These activities are not the subject of this paper, but the areas in which harmonization activities are underway are worth to be mentioned: interpretation of single failure concept, assumptions for accident analysis, list of accidents, methods for calculating radiological consequences, assumptions for extemal hazards, component and system qualification methods and requirements, etc.

VII. STATUS AND FUTURE WORK

In May 1993 the Proposal for a Common Safety Approach[1] has been accepted by GPR and RSK. In the meantime the safety concept of the EPR has been developed by NPI. More details will be given in a presentation at the same conference[2].

Presently GRS and IPSN are further developing the proposal of the common safety approach with respect to degree of detail and concretization of presently more general statements. This development presently concentrates on the following items:

- Severe accident approach and associated radiological consequences
- System design approach
- Probabilistic approach
- Break preclusion concept
- External events
- Radiological consequences of design basis accidents.

This further development of the common safety approach and common technical principles is presently going on in parallel to the development of the conceptual design of the EPR with mutual information exchange between safety institutions and authorities on one side and utilities and vendors on the other side. By this method designers receive early information on the development trend of safety regulation for future reactors, and the safety authorities and institutes get a feedback on how the desired safety improvement can technically be achieved. The content of this paper reflects the status of development at the end of 1993. In the presentation at the conference an update on the latest results will be given.

This paper has concentrated on the proposal for a common French-German safety approach. This work is being performed on the basis of a long lasting experience in both countries in the areas of safety research, licensing and plant operation. In each country safety improvement was always 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. Two examples of these aspects on a national basis are given in two other presentations of this conference on ways of improving safety of future PWRs in France[4] and on safety features for future LWR in Germany[5].

REFERENCES

1. "IPSN/GRS Proposal for a Common Safety Approach for Future PWRs." IPSN/GRS Common Report No. 6, March 1993
2. "GPR/RSK Proposal for a Common Safety Approach for Future Pressurized Water Reactors." Adopted by GPR/RSK on May 25, 1993.
3. B. J. Baumgartl, M.P. Watteau, "The European Pressurized Water Reactor - EPR. Current status of the joint French-German development of the next PWR generation." ARS 94, Pittsburgh
4. G. Gros, J. Jalouneix, D. Manesse, J.M. Mattei, "Ways of Improving Safety for Future PWRs in France". ARS 94, Pittsburgh
5. H.P. Berg, U. Erven, W. Frisch, H. Kalinowski, "Considerations on Safety Features of Future LWR in Germany". ARS 94, Pittsburgh