R A P P O R T

RECENT ACHIEVEMENT WITHIN THE FRENCH-GERMAN SAFETY APPROACH FOR FUTURE PWRs

Willi FRISCH, Gilbert GROS,
François ROLLINGER, Manfred SIMON

Rapport IPSN/Département d'évaluation de sûreté N° 397

Décembre 1999

INSTITUT DE PROTECTION ET DE SURETE NUCLEAIRE

RAPPORT DES/397

RECENT ACHIEVEMENT WITHIN THE FRENCH-GERMAN SAFETY APPROACH FOR FUTURE PWRs

Willi FRISCH *, Gilbert GROS **,
François ROLLINGER **, Manfred SIMON *

SMIRT 15
15 - 20 août 1999
Séoul, Corée

* GRS
** IPSN/DES/DIR

Décembre 1999

RECENT ACHIEVEMENT WITHIN THE FRENCH-GERMAN SAFETY APPROACH FOR FUTURE PWRs

W. Frisch (GRS), G. Gros (IPSN), F. Rollinger (IPSN), M. Simon (GRS)

SMIRT - 15
SEOUL, KOREA, August 15-20, 1999

RECENT ACHIEVEMENT WITHIN THE FRENCH-GERMAN SAFETY APPROACH FOR FUTURE PWRs

W. Frisch (GRS), G. Gros (IPSN), F. Rollinger (IPSN), M. Simon (GRS)

ABSTRACT

The development of the common French-German safety approach was accomplished on three working levels: the technical safety organisations GRS and IPSN provided the technical basis, the advisory groups GPR and RSK developed common recommendations, and the authorities BMU and DSIN adopted and issued the recommendations.

The general safety approach issued in May 1993 contains safety objectives, general principles and some technical principles for future PWRs. Based on this general approach, more detailed recommendations have been developed in 1994 on key issues.

The following period from 1995 on was characterised by a further refinement of the recommendations and the treatment of some new subjects such as digital I&C, man-machine-interface and core design.

1. INTRODUCTION

It was in 1992 that the French and German safety authorities decided to establish a common safety approach for future PWRs in parallel with the industrial development of the "European Pressurized Water Reactor (EPR)". The prime objective of the industry was to ensure that the same PWR design be licensable in both countries.

The development of the common safety approach started with two important goals :

- to achieve a considerable safety improvement in the design of future PWRs in an "evolutionary" way and
- to develop this approach jointly for France and Germany.

The safety approach is meant to be applicable to PWRs to be built right at the beginning of the next century. For that reason, the "evolutionary" way was chosen. This ensures that optimal use is made of the operating experience in both countries, which as of now is more than 1000 reactor years. The possibility that some of these new reactors may still be in operation in 2070 or 2080 justifies the establishment of ambitious safety objectives relative to present days.

The restriction to an "evolutionary" approach is not meant to prevent the development of "innovative" concepts with completely different design solutions. If, possibly in a few years, due to the technical development and/or changes in safety philosophy, new concepts are approaching maturity, they can be evaluated outside this approach.

The joint development of the safety approach included an harmonisation process between France and Germany. This process was straightforward in new areas without existing regulation (e. g. mitigation of severe accidents) and more complicated in areas with existing but different licensing practices (e. g. design against air plane crash).

2. THE DEVELOPMENT OF THE SAFETY APPROACH

The development was a continuing process, which started with the development of basic safety objectives (issued in May 1993), followed by the treatment of key safety issues (1993 - 1994) and a further refinement of these key issues and the treatment of other important safety issues (since 1995).

The stepwise development of the safety approach allowed the industry to take into account the content of the approach during the design development. The designer's Conceptual Safety Features Review File (CSFRF) was issued in September 1993 after the basic safety objectives had been issued in May 1993. For the Basic Design Report of the EPR, delivered to the safety authorities in the autumn of 1997, the designer was able to take into account the content of the safety approach for the key issues (beginning of 1995) and part of the subsequent refinement phase.

During the last part of the refinement phase of the safety approach it was possible to take into account information of the Basic Design Report. During 1998 the designer has performed a "Design Optimisation Phase". This phase included numerous parameter changes to optimise the concept, mainly for economical reasons, but also to take into account recommendations from the later phase of the development of the safety approach (e. g. the provision of an extra safety grade boration system).

This iterative procedure between the industrial design development and the development of the safety approach of the authorities was advantageous for all parties involved for two reasons: firstly, the area and extent of necessary refinement within the safety approach was easier to estimate on the basis of a design concept and, secondly, potential inconsistencies between the basic safety objectives and first design approaches have been identified in an early phase of the development.

The safety approach has been developed according to the following procedure: the technical consultants GRS (Gesellschaft für Anlagen- und Reaktorsicherheit mbH) and IPSN (Institut de Protection et de Sûreté Nucléaire) elaborated the technical basis. Starting from essential background information (description of technical and physical conditions, present licensing practices, knowledge derived from research and development, etc.), common positions of GRS and IPSN have been worked out in the form of comments and recommendations for technical positions, and the need for further information was identified. This detailed work was the basis for a treatment of the subjects within the technical advisory bodies to the safety authorities GPR (Groupe Permanent chargé des Réacteurs Nucléaires) and RSK (Reaktor-Sicherheitskommission) in joint meetings. These activities resulted in GPR/RSK recommendations, which were submitted for adoption to DFD, the German-French Directorate of the safety authorities.

3. THE PHASES OF THE DEVELOPMENT OF THE SAFETY APPROACH

3.1. The Common Safety Approach of 1993

The first set of common recommendations which represented the general safety approach was issued in May 1993 as „GPR/RSK Proposal for a Common Safety Approach for Future Pressurised Water Reactors". It was adopted by DFD in June 1993.

This document, which contains general safety objectives and technical safety principles, is hereafter called the „Common Safety Approach of 1993". It is the basis for all further more detailed and refined recommendations and requirements. The content of this basic approach is summarised briefly. The common opinion of the groups of experts is that the significant improvement aimed at for the next generation of PWRs (to be constructed at the beginning of the next century) can be obtained in the „evolutionary" way if due consideration is given to the lessons learned from operating experience and from in-depth studies like PSA, as well as to the results of research, in particular on severe accidents.

Three important general safety objectives have been set up :

I A further reduction of the core melt frequency.

II The „practical elimination" of accident situations which could lead to large early releases of radioactive material. If those situations cannot be considered as physically impossible, provisions have to be taken to „design them out".

III For low pressure core melt situations the design has to be such that the associated maximum conceivable releases would necessitate only very limited protective measures in area and time (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long-term restrictions in the consumption of food).

A fourth objective can be added: A further reduction of occupational exposure to plant personnel.

The first and second objectives are in line with the present safety concept. The third objectives characterises the development of a safety philosophy in the sense of an extension of the "defence-in-depth" principle by adding an additional level of defence. The technical principles derived from this safety objectives ask for new technical solutions going beyond those which are presently implemented in operating plants for risk reduction.

In addition to the general safety objectives the Common Safety Approach of 1993 also contains important safety principles which essentially support an "evolutionary" development. A few are mentioned here :

- Enhancement of the "defence -in-depth" principles (barriers, levels of protection)
- Deterministic design basis, supplemented by the use of probabilistic methods
- Use of experience feedback from plant operation in both countries

3.2. Treatment of Key Issues

The next development period from 1993 up to the beginning of 1995 was characterised by the treatment of some key issues which were of particular importance in an early phase of design. The following key issues have been covered :

- **Severe Accidents** (general approach, radiological consequences, impact on containment design, R&D needs)
- **System Design and Use of PSA** (general approach, use of PSA, reliability of the shutdown function, consideration of shutdown states, etc.)
- **External Hazards**
- **Primary Circuit Integrity** (break preclusion concept)
- **Radiological Consequences of Accidents**

For these issues detailed recommendations have been developed following the same procedure as mentioned above with the involvement of GRS, IPSN, GPR, RSK, BMU and DSIN. The results have been presented in different conference papers (1), (2), (3). Only two of the key issues are discussed here, External hazards because of the harmonisation effort, Severe accidents because it is an extremely important subject.

3.2.1. External Hazards

With regard to **earthquakes,** the position adopted by GPR and RSK is that the basic design of future nuclear power plants should be based on a safe shutdown earthquake characterised by the response spectrum of the NRC regulatory guide 1.60, scaled to a 0.25 g null period ground level acceleration. This spectrum should actually cover the real response spectra for most French and German sites. Of course, this will have to be confirmed for each site selected, in the context of the licensing process.

Concerning **explosions,** GPR and RSK recommend to take into account, for the design of future plants as a standard load-time function, a steep front triangular pressure wave with a maximum overpressure of 100 mbar and a duration of 300 msec.

Before any decision about the construction of a plant on a specific site is made, the applicant has to prove that the standard protection relative to explosions is adequate, taking into account the actual and planned industrial development near the site. Otherwise administrative measures must be taken or additional protection has to be provided.

With regard to protection against **aircraft crashes**, it proved difficult to find a common approach due to the very different present practices in France and Germany. In-depth technical discussions were necessary, taking into account that relevant parameters have changed in the past and will change in the future. One example is the significant reduction of the number of military aircraft movements in Germany after the political changes in Eastern Europe and the German reunification.

There was an early agreement that the design has to be made on the basis of reference load-time functions which also include impact of military aircrafts. The detailed discussions resulted in a common GPR/RSK recommendation with two load-time functions. The safety functions to be ensured were fully defined (reactor shut-down and prevention of core melt, no de-watering of spent fuel in the pool), and the methods to be used to calculate the various aircraft crash effects (perforation, vibration) were specified.

3.2.2. Severe accidents

The second and third objectives of the approach of 1993 are related to severe accidents. Accident situations which would lead to large early releases have to be "practically eliminated": when they cannot be considered as physically impossible, design provisions have to be taken to design them out. Examples of those situations are core melt situations with containment bypass, conditions after core melt that may threaten the containment integrity and core melt under high primary system pressure. The latter situation is presented here briefly:

In the Common Safety Approach of 1993 it is stated that: „It must be a design objective to transfer **high pressure core melt sequences** to low pressure core melt sequences (less than 15 to 20 bar primary system pressure at time of vessel failure) with a high reliability so that high pressure core melt situations can be "excluded". The designer was asked to propose depressurisation means with due consideration of the expected reliability of the valves; in particular these means must be clearly qualified under representative conditions. The use of specific valves - to be actuated only in case of core melt sequences - should be investigated.

Upon this recommendation, the designer has proposed a design solution with a dedicated bleed valve for primary system depressurisation in case of a failure of the pressurizer valves, which are supposed to be used for depressurisation as a first choice. On this solution more detailed GPR/RSK recommendations have been given recently: Its discharge function must be available in case of loss of off-site power and unavailability of all diesel generators. Once open, the bleed path should stay fully open with high reliability.

Sensitivity studies regarding the discharge capacity, the hot gas temperature and the initiation criteria have to be done for specified relevant scenarios considering delayed bleeding and late reflooding as well as uncertainties of the code models.

Special attention has also been given to **low pressure core melt scenarios**. According to safety objectives III, low pressure core melt situations have to be coped with and the corresponding radioactive releases have to be limited. This implies the investigation of various phenomena and the development of a strategy from which the relevant design criteria can be derived. The findings related to some of these issues are presented here.

Concerning the aspects of energy release from **hydrogen** reactions, the position adopted by GPR and RSK is that the design must cope with a hydrogen production corresponding to the complete reaction of the fuel clad zirconium with water. However, it can be assumed that this amount of hydrogen is not instantaneously released into the reactor building, but as a function of time to be estimated for representative core melt scenarios. Catalytic recombiners can be used to limit the concentration of hydrogen in the reactor building, provided the efficiency of such equipment is clearly demonstrated under core melt accident conditions. Global hydrogen detonations have to be prevented. High local concentrations of hydrogen must also be prevented as far as possible. If it is not possible to demonstrate that the local hydrogen concentration remains below 10 %, specific measures have to be implemented, such as „inertisation" or reinforced walls.

GPR and RSK have stated that the installation of a **liner** should be considered because it would provide additional margins with respect to containment leaktightness, especially considering specific phenomena such as a fast local hydrogen deflagration. They doubt that the present designer proposal (without an internal liner) allows to ensure the defined level of leaktightness. Experiments related to the behaviour of composite liners are underway and will be evaluated with respect to the containment leaktightness function.

Concerning the **ex-vessel molten core cooling**, the designer has presented a concept with a large spreading compartment separated from the reactor pit and protected from the thermo-mechanical loads resulting from the reactor pressure vessel failure. Design provisions prevent any flow of condensate into this compartment. Moreover, a steel gate physically separates the reactor pit from the spreading compartment. To prevent basemat penetration a protective refractory layer covered by a cast iron layer is foreseen. The cooling of the melt is achieved by flooding from above by means of a large water tank inside the containment building.

GPR and RSK underline that the validation of such a strategy would require extensive research and development work. The robustness of this concept has to be checked for various scenarios, including late reflooding and low residual power; specific attention has to be paid to the possibility of an early or partial failure of the steel gate. Specific provisions have to be implemented to ensure that the reactor building basemat would remain leaktight in order to prevent contamination of soil and groundwater.

With respect to **containment heat removal**, GPR and RSK emphasise that this function must be ensured without a containment venting device, and that a short-term reduction of the containment pressure must be possible.

The objective of the limitation of radioactive releases implies a substantial improvement of the **containment function**, considering the different possible failures of this function **during core melt situations**. The integrity and leaktightness must be ensured even after the global deflagration of the maximum amount of hydrogen which could be contained in the containment building in the course of low pressure core melt accidents. The design pressure and temperature of the containment inner wall must be such as to allow a grace period of at least 12 hours without containment heat removal.

3.3. Further Refinement of the Approach

During the period from 1995 up to now many subjects have been treated in a more detailed and refined way in order to give more recommendations as a guidance for the designer. Some new subjects (e. g. core design) have also been added.

During that period detailed recommendations have been given on: containment design, various system design issues, radiation protection during normal operation, primary circuit integrity, internal and external hazards, severe accident R&D needs, core design, shutdown states and man-machine-interface. They are partly presented in different publications (2), (3), (4). The most recent recommendations are briefly explained here.

3.3.1. Core Design

Parameters and characteristics of the core design are usually not a fixed part of the reactor design because some freedom is necessary to adopt the core design to different fuel cycle strategies. However, some basic principles have to be followed. GPR and RSK have stated that "*the plant design shall be such that inherent behaviour is stable (e.g. negative moderator feedback)*". They underline that some fuel managements could lead to high boron concentrations at the beginning of life of the core and, consequently, to a positive moderator temperature coefficient. GPR and RSK consider that, in principle, this coefficient must be kept negative from hot zero power to nominal conditions with all the control rods out of the core; the coolant void coefficient has to be negative for all conditions.

3.3.2. Earthquake

This subject had already been treated as a key issue. Recently some complementary recommendations have been specified, mainly with respect to the superposition of earthquake and internal events. Some examples are :

Concerning the combination of the design basis earthquake with a loss of coolant accident for the design of components and structures of future pressurised water reactors, it has been recommended by GPR and RSK *"to consider the complete guillotine rupture of the largest pipe connected to the main coolant lines"* and more precisely, to consider for the design of the internal structures of the reactor vessel, *"a load case combining the design basis earthquake and the rupture of the largest pipe connected to a main coolant line, using "the square root of the sum of the squares" methodology"*.

The aim of the margin assessment is to demonstrate that no cliff-edge effect in terms of radiological consequences would occur for acceleration values postulated beyond the site specific acceleration values; the corresponding methodology has to take into account the actual behaviour of representative equipment and the possibilities of simultaneous failures of equipment.

Concerning the emergency power supplies, it has been indicated that they can be constituted by four main identical diesel generators supplemented by two small diversified diesel generators; to cope with the potential long-term loss of off-site electrical power, all the emergency power supplies have to be seismically designed and qualified.

Systems necessary to cope with reference transients, incidents and accidents have to be designed and qualified for the combination of loads resulting from the corresponding transient, incident or accident and the design earthquake.

3.3.3. Man-Machine-Interface

Previous conclusions of GPR and RSK indicate that *"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. The general aim is to take advantage of the human abilities, while minimising the possibilities for human errors and making the plants less sensitive to these errors ... Improving the man-machine interface shall be applied in all the locations where men interact with technical equipment."*

More precisely, concerning the control room, conclusions of GPR and RSK state that *"sufficient and appropriate information shall be made available to the operators for a clear understanding of the plant statutes, including severe accident conditions, and for the clear assessment of the effects of their interventions. Emphasis should be placed on the use of computer techniques for reliable diagnosis systems for operator support."*

After complementary discussions on these topics, GPR and RSK consider that the designer has to elaborate at an early stage of the design, a comprehensive human factors engineering programme which covers also maintenance and testing activities in order to ensure consistency and tracking of human factor issues and design choices in a well-structured and state-of-the-art human factors approach.

3.3.4. System Design Issues

Various system design issues have been treated at several occasions, e. g. in connection with event classification, system classification and requirements, shutdown states, etc. An elaborate classification concept has been set up in agreement with the defence-in-depth principle. This concepts includes the definition of 7 plant operation states from full power to cold shutdown with unloaded core. This distinction was necessary because of the different system availabilities, e. g. one intermediate state is defined as "intermediate and cold shutdown with the residual heat removal system in operation and the primary coolant system closed."

Internal events are also classified according to there frequency of occurrence. They are called plant conditions categories (PCC) :

PCC-1	Normal Operation
PCC-2	Reference Transients
PCC-3	Reference Incidents
PCC-4	Reference Accidents

A list of events to be analysed in each category is specified. The PCCs are the design bases events relevant for plant and safety systems design.

According to the extension of the defence-in-depth principle two categories in the area of risk reduction ("beyond design basis accidents") are defined (Risk Reduction Categories RRC) :

RRC-A	Prevention of core melt after a complete failure of a safety function (multiple failure conditions)
RCC-B	Limitation of radiological consequences after low pressure core melt scenarios.

For both categories the events to be analysed are specified. The classification of safety functions and safety systems is arranged in such a way that sufficient diversity is guaranteed in order to minimise the effect of common cause failures, e. g. Safety Functions F1 are specified to cope with PCC events, while Safety Functions F2 (diverse from F1 functions, less stringent requirements than on F1 functions) are required to cope with multiple failure events (RRC-A). The entire list of events and the system classification will be checked by a PSA at the end of the detailed design.

3.4. Guidelines

The recommendations given so far by GPR and RSK are not yet put into a particular structure, because they have been continuously developed with time priorities partly given by the design process. Therefore it is intended to restructure the recommendations in terms of a complete set of technical guidelines. This work is underway now. The technical guidelines are structured according to the defence-in-depth principle in 5 parts :

A Principles of the Safety Concept
B Conceptual Safety Features
C Accident Prevention and Plant Safety Characteristics
D Control of Reference Incidents and Accidents
E Protection against Multiple Failure Situations and Core Melt Accidents
F Protection against Hazards

It is intended to complete the technical guidelines in the third quarter of 1999. Their content shall be identical to the GPR/RSK recommendations. They are meant to be the key tool to evaluate a new reactor design within a licensing process.

4. CONCLUSION

The driving force for the development of the common approach was twofold: to achieve a significant increase in the safety and to aim at a harmonisation between France and Germany. In both areas the achievements were very satisfactory. The objectives of the safety approach are very demanding and within the iteration process with the design development there are clear indications that technical solutions which fulfil these demanding requirements are possible and feasible. There was also considerable progress in the harmonisation of requirements between France and Germany despite of some significant differences in the national practices. This harmonisation process aims at a well balanced common approach rather than at adding up all sets of requirements of both countries.

REFERENCES

1. Quéniart, D. and Frisch, W., *"Assessment of Basic Safety Issues"*, SFEN/KTG Conference on the EPR Project, Strasbourg, France, November 13-14, 1995

2. Birkhofer, A. and Livolant, M., *"Harmonisation of Franco-German Safety Requirements as a Milestone of an Overall European Standard of Safety"*, ENC'98, Nice, France, October 25-28, 1998

3. Frisch, W. and Gros, G., *"Key Issues Recently Treated within the French-German Safety Approach"*, 2nd International Conference on Advanced Reactor Safety, ARS '97, Orlando, USA, June 1-4, 1997

4. Frisch, W. and Gros, G., *"Status of the Harmonisation Process of the French and German Licensing Requirements"*, 11th PBNC, Banff, Canada, May 3-7, 1998