Proceedings of ICON 5:
5th International Conference on Nuclear Engineering
May 26-30, 1997, Nice, France

ICONE5-2160

TSO STUDY PROJECT ON DEVELOPMENT OF A COMMON SAFETY APPROACH IN EU COUNTRIES FOR LARGE EVOLUTIONARY PWRS

Benoît De Boeck
AVN
Avenue du Roi 157
B-1190 Brussels (Belgium)
Phone: ++/32/2/5368335 Fax: ++/32/2/5368585
e-mail: bdb@avn.be

Pieter De Gelder
AVN
Avenue du Roi 157
B-1190 Brussels (Belgium)
Phone: ++/32/2/5368336 Fax: ++/32/2/5368585
e-mail: pdg@avn.be

Daljit Dhuga and Jeremy Rogers
AEA Technology (UK)

Gabriele Del Nero and Gianfranco Capponi
ANPA (Italy)

Maria Teresa Dominguez
CIEMAT (Spain)

Klaus Liesch and Rudolf Kirmse
GRS (Germany)

Thierry Foult
IPSN (France)

Bernd Riegel
RISKAUDIT

ABSTRACT

In pursuance of the objectives of the Council's Resolutions of 1975 and 1992 on the technological issues of nuclear safety, the European Commission (EC) is seeking to promote a sustained joint in-depth study on possible significant future nuclear power reactor safety cases. To that end the EC has decided to support financially a study by a grouping of the European Union's Technical Safety Organisations (TSOs).

The general objective of the study programme is to promote through a collaboration of the European TSOs common views on technical safety issues related to large evolutionary PWRs in Europe, which could be ready for operation at the beginning of the next decade.

The study focuses notably on the European Pressurised Water Reactor (EPR) project developed by the French and German utilities and vendors, but also considers relevant projects, even of plants of different size, developed outside Europe.

The study also makes use of the requirements developed by the European utilities and takes advantage of the recommendations made by the French and German nuclear safety advisory groups: "Groupe Permanent chargé des Réacteurs nucléaires" and "Reaktor-Sicherheitskommission" (GPR/RSK).

Twelve key issues that were judged to have the greatest safety significance were selected for in-depth analysis. This analysis is now being finalised by establishing common TSO Group positions for the twelve key issues.

It can be stated that during this project, an important step forward was made in the development of a common safety approach of the TSOs.

BACKGROUND

In pursuance of the objectives of the Council's Resolutions of 1975 and 1992 on the technological issues of nuclear safety, the European Commission (EC) is seeking to promote a sustained joint in-depth study on possible significant future nuclear power reactor safety cases. To that end the EC decided to support financially a study by a grouping of the European Union's Technical Safety Organisations (TSOs).

This project is a multinational co-operation between the TSOs. RISKAUDIT is the co-ordinator of the project with the EC. The participating TSOs are AVN (Belgium), acting as Technical project leader, AEA Technology (United Kingdom), ANPA (Italy), CIEMAT (Spain), GRS (Germany), and IPSN (France).

This project was carried out in three phases. The work performed under the first two phases was summarised in two reports submitted to EC (RISKAUDIT, 1995 and RISKAUDIT, 1996). The work now being performed in the third phase will be summarised in a report to be submitted to EC in June 1997.

OBJECTIVES AND SCOPE OF THE TSO STUDY PROJECT

The general objective of the study programme is to promote through a collaboration of the European Union Technical Safety Organisations a common view on technical safety issues related to a large evolutionary PWR in Europe, which could be ready for operation at the beginning of the next decade.

The study is focusing on the EPR project developed by the French and German utilities and vendors. It also considers relevant projects developed outside Europe in order to provide elements important for the safety characterisation and which could contribute to the credibility and confidence of EPR, even if plants are of different size.

The study also makes use of the requirements developed by the European utilities and takes advantage of the recommendations made by the French and German nuclear safety advisory groups: “Groupe Permanent chargé des Réacteurs nucléaires” and “Reaktor-Sicherheitskommission” (GPR/RSK).

It is expected that this study will constitute a significant step towards the development of a common safety approach in EU countries.

This project should not be seen as a safety evaluation of the EPR project and does not interfere with bilateral French/German activities.

The scope of the TSO study covers the following tasks:

- Survey of TSO national activities on technical safety objectives
- Survey of large evolutionary PWR conceptual projects
- Consolidated analysis of key issues of EPR and other large evolutionary concepts
- Consolidated review of the European Utility Requirements (EUR)
- Feasibility study to achieve a common safety approach

These tasks are further described hereafter.

SURVEY OF TSO NATIONAL ACTIVITIES ON TECHNICAL SAFETY OBJECTIVES

Each TSO produced a document describing its present views on the technical safety objectives for future PWRs, or those of the national licensing organisation. As far as possible, the national objectives were compared with the common recommendations of GPR and RSK (GPR/RSK, 1993), called hereafter the GPR/RSK proposal. This proposal presents the common opinion of the French and German groups of experts that currently give advice to the regulatory bodies of the two countries on the safety philosophy and approach for the next generation of nuclear power plants. Later, this proposal was complemented by common conclusions of the GPR/RSK published in 1995 (GPR/RSK, 1995).

Some particular aspects highlighted by the different TSOs are summarised hereafter.

AVN

AVN gave an opinion on what could be some of the requirements for a possible future plant in Belgium. The GPR/RSK proposal was fully endorsed and some additional requirements were proposed.

Increased margins should be available by design to allow flexible operation, so that, even if the operating conditions or core design approach the limits, no breach in the defence in depth is likely to occur.

Quantitative probabilistic safety goals have never been used in Belgium. It was the AVN view that quantitative probabilistic goals should only be used together with a detailed definition of the method to be used to show compliance. As PSA methodology has not yet been standardised, it seemed too early to define quantitative probabilistic safety goals. Regardless of the safety goals, the ALARP principle should be used at all risk levels.

In the accident analyses, the safety margins should also be assessed by discarding the first trip signal and studying the plant response when the second trip signal is taken into account. This is the so-called “back-up signal concept”.

For future plants, the probability of containment bypass should be decreased. In particular, a steam generator tube rupture caused by a secondary line break needs to be addressed specifically, together with appropriate thermal-hydraulic and radiological acceptance criteria. In line with the defence in depth principle, the containment shall be regarded as a very important safety feature, and its performance should be thoroughly assessed, for design basis events and for severe accidents addressed in the design.

AEA Technology

AEA gave the background to the current UK licensing practice. The Safety Assessment Principles (SAPs) contain both probabilistic limits and objectives, and deterministic engineering principles, applicable to any nuclear plant. The SAPs were described, illustrating how they provide the framework for assessment of future plants, in a manner which ensures that safety standards are as high as can be reasonably achieved, taking account of technological developments.

This was compared with the GPR/RSK proposal, outlining both the similarities and differences in approach. One difference is that the proposal requires an increase of the safety of future plants compared to existing plants, whereas the SAPs make no explicit reference to past and future designs. Features which are likely in the evolutionary designs of PWRs (passive safety systems, improved fault tolerance and grace periods, high capability containments, etc.) are consistent with good practice that is encouraged by the SAPs but are not strongly or specifically prescribed. They should have the effect of simplifying the justification of safety against the probabilistic targets.

Concerning the use of PSA to support the safety case, the approach in the UK differs from that proposed by GPR/RSK which states that quantitative probabilistic targets are not seen as requirements, but as “orientation values”. The SAPs however contain both probabilistic limits and objectives. The limits represent the regulator’s view of what is just tolerable and must be met. The objectives represent a target for safety. In practice this is not completely inconsistent, since the limits are set at a high level and the objectives are not mandatory, but subject to ALARP assessment.

In the SAPs, no explicit requirement for the performance of a containment following a degraded core accident is given, but the probabilistic targets for accident radiation doses imply a performance requirement.

ANPA

ANPA provided indications on the expected safety improvements in future NPPs:

- enlarged spectrum of events to be considered in the design, including severe accidents;
- use of inherent safety features and reliable passive safety features as far as possible;
- no need for planned evacuation and avoidance of significant land contamination even in case of severe accidents;
- plant simplification and enhanced reliability of safety functions with less sensibility to human errors.

The following aspects were emphasised:

- the defence in depth concept, and in particular the need to take both prevention and mitigation into account;
- the need to increase safety margins and grace periods;
- the need to improve the containment function: (1) structural resistance to internal accidents (including representative severe accidents) and external events; (2) leaktightness requirements to ensure the required limitation of external consequences after an accident; (3) adequate provisions against single or multiple SGTR with failure of the isolation and against other potential bypass sequences.

CIEMAT

CIEMAT outlined the aspects that, given their importance for safety, should be a priority objective in the design of the new generation of reactors.

The defense in depth principle must be maintained and strengthened according to the philosophy established in INSAG-3 and INSAG-10 recently published. To achieve this principle the following considerations are envisaged as very important for future reactors.

Operational experience should be a very important tool to improve aspects identified as problematic or not sufficiently resolved in existing reactors. Maintenance activities should be thoroughly considered in the design phase to select a system architecture in such a way that during maintenance sufficient reliability is maintained.

It is considered important to stabilize for the application to future reactors the existing deterministic rules applied in the safety demonstration of the capacity to control accidents, taking in consideration the needs derived from the use of new systems, especially those in which software is applied.

To reduce the possibility of significant radioactive releases to the environment, the implementation of design features to control severe accidents is considered a main safety objective for future reactors.

PSA should be used not only for the final evaluation of the fulfillment of probabilistic risk objectives, but also as a design tool. To this end, it is important to define common applications of the probabilistic insights in the licensing process.

Finally a list of areas was given in which an effort should be made by the TSOs to establish common methodologies and acceptance criteria.

GRS

In Germany safety improvement has always been a continuous process, both in backfitting of existing plants and in defining requirements for plants to be built. In recent years - with no new plants being constructed - the development of a new safety approach has been started considering the following facts:

- good operating experience and safety performance exists for Western plants
- Three-Miles-Island and Chernobyl have demonstrated that severe beyond design basis accidents can happen
- there is a world-wide trend in developing new reactor concepts with enhanced safety features.

There was a common French-German agreement to develop the safety approach for future reactors jointly. On the German side the Federal Minister for Environment, Nature Conservation and Reactor Safety (BMU) is funding these activities of GRS. A first proposal has been developed by GRS and IPSN as a basis for the GPR/RSK proposal (GPR/RSK, 1993 and 1995). The general objectives are: consolidation of the defence in depth concept, further reduction of the probability of core melt accidents and reduction of radiological consequences of severe accidents.

The basis to reach these objectives is to build upon proven technology, and to use the experience gained through plant operation, and the knowledge from safety research results, and the results of PSAs for existing plants.

Presently, GRS is involved with IPSN in the development of common technical safety principles and guidelines to be applied to PWR concepts, which are more detailed than the general objectives and principles of the GPR/RSK proposal.
Further, the German Atomic Energy Act has been extended in the sense of the defence in depth concept. The content of this text is comparable to the demand in the GPR/RSK common approach to limit the radiological consequences of low pressure core melt situations such that only very limited protective measures in area and time would have to be implemented. This limitation is valid for any new reactor being built in Germany, regardless if it is a PWR or BWR type, as for instance the passive BWR concept, presently under development by Siemens/KWU.

The future task will be to establish the guidelines which determine in greater detail the relevant events as spelled out in this extension of the Atomic Energy Act. In the development of these guidelines consistency has to be achieved with the findings and content of the French/German safety approach.

The above mentioned activities are related to the development of a licensing basis for future PWRs. Other activities related to future reactors are the adaptation of analysis tools to the special features of future reactors (at GRS) and numerous experimental activities especially in the area of severe accidents. A large part of these experimental activities is performed by the Karlsruhe Research Centre.

IPSN

IPSN described the common activities with GRS that converged in 1993 on the GPR/RSK proposal. The main conclusions of this work are the following:

- The defence in depth principle remains the fundamental principle. A general objective is to reinforce the defence in depth on a deterministic basis, supplemented by the use of probabilistic methods. The safety demonstration has to be made in that way.
- The operating experience of existing units is an essential driving force to improve the defence in depth.
- PSAs are another essential driving force to improve the defence in depth. Specific lessons learned from PSAs are: (1) particular attention has to be given to reactor shutdown states, (2) the possibilities of common cause failure have to be minimised as far as possible, and (3) prevention of human errors and lower sensitivity to such errors must be sought.
- A significant reduction of radioactive releases due to all conceivable accidents, including core melt accidents must be achieved. To follow this objective implies on the one hand to "practically eliminate"[1] accident situations that could lead to large early releases, and on the other hand a substantial improvement of the containment function, considering the different possible failures of this function for low pressure core melt situations.

[1] A situation is considered practically eliminated if it is physically impossible or if proper design provisions are taken to make it extremely unlikely with a high degree of confidence.

Discussion

As can be seen from the national contributions, the GPR/RSK proposal has been used as a good starting point to develop a common basis for safety objectives and requirements for future PWR plants in Europe. The main areas in which differences arise are related to radiological consequences for severe accidents in the vicinity of the plant, deterministic/probabilistic bases for the identification of severe accidents to be considered, and the formal use of quantitative safety targets.

In addition to the common platform, each TSO highlighted some specific requirements, stemming from its own experience, from its national regulatory practice, and from the expected safety enhancements for future nuclear power plants.

SURVEY OF LARGE EVOLUTIONARY PWR CONCEPTUAL PROJECTS

A list of documentation on future PWR concepts was established and continuously updated. It gives an overview of the literature available at TSOs, on different PWR designs and includes sections on: overview documents, the European Utility Requirements (EUR), EPRI Requirements, policy making/international guidelines, research & development, and safety studies and particular topics.

To finalise the selection of reactor concepts from this list for in-depth analysis, a matrix was established containing on one side the reactor concepts and on the other side the selection criteria. These were: degree of innovation, advancement of design work, utilities involvement, present activities, EC countries involvement, and availability of documentation.

Based on this matrix the following reactor concepts were selected for further consideration in the first phase: EPR, N4, Sizewell, APWR (1000 and 1300), System 80+, WPBER-600, WWER-640/W-407, WWER-1000/W-392, AP600, KfK containment, PIUS, SIR, and ISIS.

For these selected designs a survey was prepared, consisting of a description based on the table of contents of the GPR/RSK proposal (1993), supplemented by a table with the main characteristics and safety options.

CONSOLIDATED ANALYSIS OF KEY ISSUES OF EPR AND OTHER LARGE EVOLUTIONARY CONCEPTS

In preparation for the consolidated analysis, each TSO produced a short list of high priority safety issues considered to be important for future PWR concepts. The lists were based on the surveys performed for the selected PWR concepts, taking account of INSAG documents, GPR/RSK proposal, and the technical safety objectives and experience of the TSOs. For each safety issue identified, some background was provided, and a work proposal prepared. After comparison of the safety issues, a provisional consolidated list of 30 key issues was produced, which is given in Annex A. The numbering of the key issues does not reflect any safety priority, but results from the broad grouping of issues.

It was decided these issues would be examined only for a subset of the originally selected designs, chosen for their importance and the availability of sufficiently detailed documentation. The selected designs were: EPR, System 80+, Sizewell, AP600, APWR 1300, and WWER-640/W-407.

To enable a sufficiently detailed analysis of the key safety issues, it was necessary to focus on a subset of the original list of 30 issues. After discussing priorities and grouping some issues, 12 key issues that were judged to have the greatest safety significance were selected for in-depth analysis. They are given below:

Key Issue	Title
1	Use of Probabilistic Safety Assessment in design and licensing
2	Reduced environmental source term and emergency plan
3+4	Identification of postulated initiating events (PIEs) and associated acceptance criteria
12	Instrumentation and control systems important for safety (hardware and software aspects)
13+14	System architecture
17	Passive systems behaviour
22	Practical elimination[1] of core melt in shutdown states with open containment
23	Practical elimination[1] of high pressure core melt
24	Practical elimination[1] of core melt with containment bypass
25	Practical elimination[1] of large early releases resulting from containment failure
26	Mitigation of low pressure core melt and vessel melt-through
5+27	Identification of severe accidents: methodology and acceptance criteria

The in-depth analysis of these key issues, which constituted the major work effort during the second phase of the project, was performed interactively amongst the TSOs. Each TSO took the leadership for two key issues, but all TSOs fully contributed to each key issue by providing suggestions and comments on the draft reports. For the application of the key issues to the six selected designs, each TSO was assigned one selected design and performed the application of all the key issues for that design.

All reports on the key issues have a commonly agreed structure:

Section 1	Introduction
Section 2	Description of the key issue
Section 3	State of the art (such as technical safety objectives, R&D, EUR Document)
Section 4	Application of the key issue to the selected designs
Section 5	Conclusions and TSO group position

For the majority of the above key issues, sections 1 to 4 have now achieved a stable state. Section 5 concerning the Conclusions and TSO group position is currently under development and discussion for all the key issues. Finalisation of this section should constitute a significant step towards the development of a common safety approach amongst the TSOs.

To illustrate the technical work being performed within this project, Annexes B and C include a summary of the introduction and description sections for two key issues.

CONSOLIDATED REVIEW OF THE EUROPEAN UTILITY REQUIREMENTS

As the terms of reference of this project foresaw a consolidated review of the European Utility Requirements Document (EURD, 1994 and 1995) a request was transmitted to the EUR group to receive the EURD for consideration within this project. Both revisions, A and B, were received at the end of 1994 and in April 1996 respectively.

The main work performed to date on the EURD consists of a check of completeness of the EURD with respect to the twelve key issues listed above. This work was first performed on revision A and later updated to reflect revision B.

For each key issue, a text on the EURD was provided by the TSO responsible for that key issue. Generally, these texts give an overview of the EURD safety sections relevant to the key issue and they indicate, if applicable, any aspects which are not covered by the EURD or require further clarification.

SUMMARY AND CONCLUSIONS

This paper described the work performed to date on the TSO study project on “Safety of Significant European Projects for Large Evolutionary PWRs and Development of a Common Safety Approach in EC Countries”. The conclusions reflect the interim status of the study.

Each TSO presented its technical safety objectives for future PWRs or those of the national licensing organisation, using the GPR/RSK proposal as a reference. This allowed discussion of particular aspects of the TSO approaches and of any recent evolution in their technical safety objectives. The TSO group was continuously informed by GRS and IPSN on new common positions of GPR and RSK.

A selection of reactor designs for consideration was finalised, based on a matrix of reactor concept and certain selection criteria. Surveys were prepared for the selected designs. These surveys included tables of the main parameters and safety options to allow a comprehensive review or comparison between design concepts.

In preparation for the consolidated analysis of key safety issues, a list of 30 safety issues was prepared, based on the reactor surveys. After prioritising and grouping some issues, 12 key issues that were judged to have the greatest safety significance were selected for in-depth analysis.

The in-depth analysis of these key issues was performed in a very interactive way amongst the TSOs. All reports were written following a commonly agreed structure containing a description of the key issue, an overview of the state of the art including a check of completeness of the EURD, the application of the key issue to the six selected reactor designs, and conclusions and TSO group positions. Work on the TSO group positions is still on-going.

In summary, it can be stated that during this project, an important step forward was made in the development of a common safety approach of the TSOs. This was mainly achieved by in-depth discussions on key issues being defined for future reactor designs. A definition of the common safety positions is in progress. Within this exercise, attention will also be paid to the identification of persisting different viewpoints on particular subjects, if any might appear.

ACKNOWLEDGEMENTS

The TSOs involved in this project are very grateful to the European Commission for the financial support provided for this project.

The EUR group is acknowledged for making available revisions A and B of the EURD to the TSO group.

The authors of this paper are grateful to the many colleagues at the six TSOs who have contributed in an important way to different aspects of this project, in particular to the analysis of the key issues.

REFERENCES

EURD, 1994, European utility requirements for LWR nuclear power plants, revision A March 94.

EURD, 1995, European utility requirements for LWR nuclear power plants, revision B November 95.

GPR/RSK, 1993, GPR/RSK Proposal for a Common Safety Approach for Future Pressurised Water Reactors. Adopted during the GPR/RSK common meeting of May 1993; published in Germany in Bundesanzeiger (BAnz) Nr. 218, 20.11.1993, page 10183 ff. and in France by DSIN letter n° 1321/93 dated 22.07.93.

GPR/RSK, 1995, Common Recommendations of GPR and RSK for Safety Requirements on Future Nuclear Power Plants with Pressurised Water Reactors; published in Germany in Bundesanzeiger (Banz) Nr. 127, 11.07.1995, page 7452 and in France by DSIN letter n° 51/95 dated 13.02.95.

RISKAUDIT Report N° 19, 1995, “TSO Study Project on Safety of Significative European Projects for Large Evolutionary PWRs and development of a Common Safety Approach in EC Countries (Phase 1)”.

RISKAUDIT Report N° 43, 1996, “TSO Study Project on Safety of Significative European Projects for Large Evolutionary PWRs and development of a Common Safety Approach in EC Countries (Phase 2)”.

ANNEX A

ORIGINAL LIST OF KEY ISSUES

I SAFETY OBJECTIVES

1 Use of Probabilistic Safety Assessment in design and licensing

2 Reduced source term and emergency plan simplification

II EVENTS CONSIDERED IN THE DESIGN

3 Identification and categorisation of postulated initiating events and associated acceptance criteria for design basis accidents

4 Identification of postulated events and associated acceptance criteria for beyond design basis accidents

5 Identification of severe accident scenarios addressed in the design

6 Practical exclusion of vessel rupture

III DESIGN BASIS ACCIDENTS

7 Human factors in the control and protection systems design

8 Improvements in the design in view of a better protection against SGTR

9 Depressurisation function (to allow safety injection)

10 Prevention of design basis LOCA and application of the leak before break concept

11 Overpressure protection

12 Instrumentation and control systems important to safety (hardware and software aspects)

13 Regulatory treatment of non-safety systems important for safety

14 System architecture (redundancy, diversity, ...) based on deterministic and probabilistic evaluations

15 Evaluation of new options in the design of the ECCS and of the containment spray system

16 Computerised operator support systems in accidental situations

17 Issues related to the analysis of passive systems behaviour

18 Validation of computer codes used for design verification

IV BEYOND DESIGN BASIS ACCIDENTS

19 Prevention of containment bypass

20 Reactivity accidents

21 Plant protection against BDBA (ATWS, station blackout, multiple SGTRs)

V SEVERE ACCIDENTS

22 Practical elimination of severe accidents during shutdown states

23 Practical elimination of high pressure core melt situations

24 Practical elimination of core melt with containment bypass

25 Practical elimination of large early release (hydrogen and steam explosions)

26 Mitigation of severe accidents with low pressure core melt and vessel melt-through

27 Methodology and acceptance criteria for severe accident analyses

28 Equipment qualification for severe accident conditions

VI EXTERNAL AND INTERNAL HAZARDS

29 Protection against internal hazards

30 Protection against external hazards

ANNEX B

KEY ISSUES 3 AND 4

IDENTIFICATION OF POSTULATED INITIATING EVENTS (PIES) AND ASSOCIATED ACCEPTANCE CRITERIA

1. Introduction

Operating experience and lessons gained from PSAs of present day reactor designs and new insights in safety have induced a tendency to extend the list of PIEs, considered as Design Basis Accidents (DBAs) or Beyond Design Basis Accidents (BDBAs).

The main objective of this Key Issue (KI) is to review the approaches used in new reactor designs for the identification and the analyses of design basis and beyond design basis PIEs and their associated acceptance criteria.

This KI focuses on the deterministic design verification related to DBAs and BDBAs. The use of probabilistic analyses is covered by KI 1 “Use of PSA in Design and Licensing”.

PIEs of the type internal and external hazards, were not dealt with in this KI. Originally KIs 29 and 30, respectively entitled “Protection against internal hazards” and “Protection against external hazards”, were foreseen to discuss these aspects. These KIs are however, for priority reasons, not analysed at this moment. Nevertheless some information on the protection against these hazards can be found for some designs via KI 1 “Use of PSA in Design and Licensing” and via KI 13+14 “System architecture”.

2. Description of the key issue

2.1 PIEs considered as DBAs

Identification of the PIEs considered in the design basis (including for non-power and shutdown states).
In this KI, it is looked at whether some PIEs, which were before not considered at all or which where only considered in the BDBA analysis, are now included in the design basis. Attention was paid to all plant states, including non-power states.

It is also investigated whether any feedback from PSA has been used to decide on the consideration of specific PIEs within the design basis.

For the passive designs, it is looked at whether PIEs are considered other than those considered for evolutionary designs.

Categorisation of these PIEs
PIEs for DBAs are in most cases subdivided in several plant conditions, reflecting to some extent the expected frequency of the PIE. New safety insights and operating experience could provide arguments for re-classification of some of the PIEs (for instance, SGTR). Therefore, it is investigated whether new practices in this respect are observed for the selected designs.

Application of the single failure criterion (as well in PIE categorisation as in the accident analysis)
In the deterministic design verification, the application of the single failure criterion plays an important role. The application of the single failure criterion in systems design, is covered by KI 13 + 14 "System architecture". This KI focuses on the application of the single failure criterion in the accident analyses performed for the design verification.

It is looked at whether the application rules for this criterion are clearly indicated for the different selected designs. A particular point of interest is the application of the single failure criterion for plants with passive safety systems. Passive systems are moreover treated in a more detailed way in KI 17 "Passive systems behaviour".

Also the potential impact of the single failure criterion on the classification of the PIEs is investigated.

Grace period for operator actions
In the safety analyses for reactors operating today, a grace period of 30 minutes (time between the first automatic signal and the first remedial operator action) has mostly been the target, although this objective could not always be achieved. It is looked at what grace period has been postulated in the safety analyses for the new reactor designs.

Identification of the acceptance criteria and safety objectives for the different categories of DBAs
For each category of PIEs, acceptance criteria have to be defined for use in the design verification analyses. As well acceptance criteria for core cooling and integrity, as safety objectives for radiological consequences have to be defined.

The intention is to identify and compare new evaluations in this respect.

2.2 *PIEs considered as BDBAs*

Identification of the BDBAs considered in the safety analysis
The PIEs considered as BDBAs are identified for the different selected designs.

As for DBAs, it is be investigated whether any feedback from PSA has been used to identify the BDBA PIEs.

Identification of the acceptance criteria for the BDBAs
Criteria used to decide whether the consequences of BDBA PIE are acceptable, as well for core cooling and integrity, as for radiological consequences, were identified and commented.

3. State of the art

In this section, an overview is given of the state of the art with respect to the items treated in this KI. This is done by discussing existing practices (e.g. ANSI N18.2), the GPR/RSK Proposal, and the European Utility Requirements Document.

4. Application of the KI to the selected designs

This KI was applied to the six selected designs (EPR, System 80+, Sizewell, AP600, APWR 1300 and WWER-640/W-407). A summary of the findings is given hereafter.

For most of the selected reactor designs a deterministic safety analysis forms the basis of the safety evaluation. Some common findings and some differences in the approaches for the selected designs are summarised hereafter.

Identification and categorisation of DBA postulated initiating events

- For some reactor designs, special emphasis is announced concerning PIEs in non-power and shutdown conditions. Other designs include a consideration of these states as well, but more on a probabilistic basis;
- For some designs the list of PIEs to be considered was extended by taking into account the operating experience of existing plants;
- At least for one design, a steam generator tube rupture (SGTR) is classified in the plant condition category (PCC) of limiting faults, “that are not expected to occur”;
- For some designs, the SFC is applied to each PIE in each PCC without reclassifying the initiator; for other designs some PIEs are considered in PCC “n” while the same PIE combined with a single failure is classified in PCC “n+1”;

Analysis of the DBA PIEs

- For most designs, operator grace periods of 30 minutes are announced. For one of the designs, the grace period for all DBAs was postulated to be 24 hours;
- Important differences in the application of the single failure criterion (SFC) were observed amongst the 6 designs. Examples are: to postulate a single failure (SF) in the analysis of all PIEs, from normal operating transients up to hypothetical accidents, and this for all reactor states; to postulate no single failure for normal operating transients, but to consider the same PIE combined with a single failure in a Plant Condition Category of lower frequency; to postulate for each PIE a SF combined with an unavailability for preventive maintenance.

Acceptance criteria for the different Plant Condition Categories (PCCs)

- For some designs, acceptance criteria on radiological consequences as defined in the SRP and/or 10 CFR 100 were applied;
- For one of the designs a list of fourteen acceptance criteria is given and a matrix indicates which criteria have to be applied to each PIE;
- For one of the designs, deterministic acceptance guidelines of a similar nature to the other plants discussed were defined by the utility to enable easier demonstration by the designer that a particular fault sequence had acceptable consequences within the overall plant criterion for radiological consequences.

Identification of BDBAs considered in the safety analysis.

- For all selected designs, BDBA PIEs are identified for which additional analyses have to be performed. In general, they cover scenarios with multiple failures (up to the total loss of some systems) and/or coincident occurrences of PIEs considered in the design basis;
- In all cases, these BDBAs are analysed on a best estimate basis (with no single failure postulated);
- Often, the deterministic analyses on BDBAs are complemented by probabilistic analyses.

5. Conclusions and TSO group position

This paragraph is currently being developed and discussed amongst the TSOs.

ANNEX C

KEY ISSUES 5 AND 27

IDENTIFICATION OF SEVERE ACCIDENTS : METHODOLOGY AND ACCEPTANCE CRITERIA

1. Introduction

For many years all accidents taken into account in the plant safety analysis were assumed to be successfully terminated by the intervention of the plant safety systems, and severe accidents (SAs), were excluded from any explicit design consideration. This practice was justified because accidents with core melt, which are potentially capable to threaten the containment capability to retain radioactive materials from escaping to the external environment, were considered very remote and thus very unlikely to occur. On the other side, the degree of conservatism used in the design was always judged to be sufficiently high, such as to generate ample safety margins for unpredicted situations beyond the conventional design basis.
The TMI accident, in 1979, confirmed that SAs are possible and there is today an international consensus to include design provisions for preventing and mitigating these events in order to avoid potential unacceptable consequences.
This report represents a preliminary attempt to converge towards a common approach to the identification and quantification of SAs to be explicitly considered in the design of the next generation of Pressurised Water Reactors (PWRs).
The objective is also to provide a link between the general goal addressed by KI 02 (reduced source term and emergency plan) and the particular aspects treated in separate KIs (22, 23, 24, 25, 26).

2. Description of the Key Issues

2.1 Methodology and acceptance criteria for severe accidents

The safety objectives for future nuclear plants are expected to be more demanding than for current plants, and consequently, accidents scenarios beyond the "classical" deterministic design basis will be explicitly considered in their design. There is a general consensus that these additional accident scenarios should be all those accidents, even of very low probability, that are physically plausible. The processes of selection and evaluation of the scenarios are currently not fully homogeneous and international work is in progress to improve the consensus in this field.
The current general trend is to base the selection process, to the largest possible extent, on deterministic analyses, supported where needed, by probabilistic considerations, and engineering judgement. The severe accident situations so identified as relevant have then to be evaluated and either “practically eliminated” if sufficient preventive design and operation provisions are taken, or “dealt with”, that is their consequences are evaluated and found within the capability of the design.
The following aspects are discussed:

- Degree of conservatism in the analyses.
  A conservative approach would allow the demonstration of adequacy and robustness of engineering features, but in some cases, it could be not satisfactory because of the existing uncertainties and then shifting to a best estimate approach remains the only viable choice.
- Qualification of codes for the analysis of SAs.
  The use of computer codes for SAs in a context of best estimate analysis should be limited to those aspects where an adequate degree of validation can be demonstrated.
- Reduction of uncertainties.
  Research programs provide data and basic knowledge of phenomena so allowing the reduction of existing uncertainties and a satisfactory use of a “best estimate” approach. In fields were uncertain situations exist, expert elicitation has been used.
- Acceptance criteria for systems or components provided to cope with SA scenarios.
  There is a trend to consider appropriate, for features provided only for SAs, not to require the same conservative analysis and pedigree that are necessary for systems developed to cope with “classic” design basis accidents. For equipment that is relied upon to cope with severe accident situations, there should be a high confidence that this equipment will survive severe accident conditions for the period that it is needed to perform its intended function.

2.2 Severe Accidents Scenarios and Plant States

The issues on SAs are generated because of the uncertainty that reside in the physical and chemical phenomena expected to occur, inside and/or outside the vessel, after a core melt event. Their importance is measured by the potential they have to progress up to determine a degraded plant situation which could impair the containment integrity. Some additional issues are related to pre-existing degraded plant states which, in case of a SA, could further degrade and increase the adverse accident consequences.

The following phenomena and plant states identified as important in terms of safety impact are discussed:

- High Pressure Scenario
- Reactivity Excursions
- Steam Explosions
- Hydrogen Combustion
- Molten Core Concrete Interactions
- Debris Coolability
- Containment Bypass and Isolation Failure
- Low Power States (shut-down states with open containment)

Many of the issues listed above, are the subjects of other KI reports (KI 22, 23, 24, 25, 26) in which a more detailed technical description and discussion can be found.

3. State of the art

3.1 Research and Development

The TMI accident first and the Chernobyl accident after, put a new impetus on studies and research in the field of severe accidents. Investigation has been mainly addressed to the reduction of the remaining uncertainties and the identification of possible design improvements capable of preventing or mitigating SA phenomena and plant states. The main objective of current research and experimental tests is to provide the basic knowledge to allow the closure of the severe accident issues and to identify features, to implement eventually in the design of future NPPs, to deal directly with the issues and improve the already high level of safety in the operation of NPPs.

Some of the studies (experimental and modelling) on the issues identified (chapter 2) are at a stage for which no additional work is considered justified to significantly improve the level of knowledge. One of this is the “direct containment heating” issue that, through the use of a reliable depressurisation system for the primary system, can be considered “practically eliminated”. Some experiments also proved the intrinsic capability of specific families of containment design layout to mitigate the phenomenon with negligible loads to the containment; some specific design choices still need additional evaluation.

Among the important issues still open, but with extensive work in progress that will eventually allow the closure are:

- fuel (core-melt) - coolant interaction (covering both violent and mild interactions). Included under this class are the aspects of steam explosion, steam spike, debris bed coolability, core-concrete interaction in presence of water, in-vessel coolability by ex-vessel cooling, cooling through a core catcher device etc..
- hydrogen behaviour. Some important experimental activities are addressing the behaviour of passive catalytic recombiners. Some efforts are still devoted to the transition from deflagration to detonation and to the ability to predict hydrogen concentrations in the containment system (development of 3D computer codes). Also some attention is posed to the behaviour of CO (from corium-concrete interaction).
- fission product behaviour. The importance of going into some very detailed aspects of interaction between fission products species and structures or various substances in severe accident conditions is justified by the more demanding request of retention capability inside the containment.

3.2 International/National Safety approaches

For future NPP designs, the main safety objective is a significant reduction of the probability of occurrence of core melt accidents and the potential release of radioactive materials. To achieve this objective, accidents beyond the “classical” deterministic design basis have to be addressed at an early stage of the design.

The approach is to “practically eliminate” (as proposed by GPR/RSK and, using different terms, by the EUR rev. B Document) severe accident sequences which could lead to large early releases and improve the capability of the plant systems in order to “deal with” (mitigate) all other severe accident sequences (i.e. robust design of the containment system, emergency or auxiliary systems survivability for a required time in severe accident condition to fulfil a required function).

According to the GPR/RSK proposal the design of future NPPs should be made on deterministic bases, supplemented and supported by the use of probabilistic methods, with the general objective to reinforce the "defence in depth". Operating experience, in-depth studies like PSAs conducted for PWRs and the progress in knowledge of the physical phenomena should be taken into account. Severe accident situations which would lead to large early releases have to be “practically eliminated” that is, when they can not be considered as physically impossible, design provisions have to be taken to design them out. Low pressure core melt accidents have to be "dealt with", so that the associated maximum conceivable release would necessitate only very limited protective measures in area and in time.

According to the EUR Document (EURD), safety policy should be based upon the well established deterministic methods augmented by probabilistic using appropriate numerical targets and analysis. Both deterministic and probabilistic methods shall be employed to identify the accidents which are to be addressed. These shall be subdivided in:

- accidents included in the Design Basis Conditions (DBC) and
- accidents included in the Design Extension Conditions (DEC).

PSA approach (Level 1 and Level 2) is intended to be used extensively and required to verify the compliance of plant design with the probabilistic targets (10^{-5} per reactor year for the core damage cumulative frequency and 10^{-6} per reactor year for the cumulative frequency of large release) and, in addition, to identify the sequences to be considered as DECs.

In addition to the GPR/RSK and EURD safety approaches summarised above, the following international and national positions have been also considered : IAEA, USA (EPRI, NRC), France, Germany and Italy.

4. Application of the KI to selected designs

The six NPP designs considered in the KI present some differences in their approach to the issues outlined in this report because of their own specific origins. They can be located in a time sequence that justifies the differences in the methods and criteria considered in their design.

Sizewell B is an operating plant that was designed to conform to the Safety Assessment Principles (SAP) of the UK licensing authority. These are based on the principle that risks should be As Low As Reasonably Practicable (ALARP). For this design the approach has been basically the same that has been used for operating plants, with the difference that a very in depth analysis has been done to verify the plant robustness to severe accident conditions. PSA approach was extensively used to demonstrate that numerical risk targets were achieved and that the contribution to the total risk from the plant from SAs is very small.

System 80+ and APWR, are US designs developed a few years later compared to Sizewell and are supposed to comply with the EPRI utility document for evolutionary plants. As for the UK plant, an acceptability criteria based on the compliance with defined safety targets has been used. No plants like these are yet in operation.

AP600 has introduced some changes in the "classical design" by specifically taking into account severe accident conditions. The accent is on passive systems (for the residual heat removal system, the containment cooling, cavity flooding, etc.) and on specific design choices (low fuel power density, water inventory, etc.). In addition, for this design it is required for any accident sequence a limited release in the short term (24h), lower than that from designs like System 80+ and APWR. The design of this plant is supposed to comply with the EPRI utility document for passive plants.

EPR design considers Beyond Design Basis Accidents (BDBA) and SAs in such a way that, even for the SAs "dealt with" in the design, the off-site radiological consequences are limited in area and time. This design will follow compliance with the GPR/RSK proposal. Both the design and the proposal are in an evolving phase.

For the WWER-640/W-407 very little information is available. It is clear from publications and from the Preliminary Safety Analysis Report (PSAR) that SAs are addressed in the design of this reactor concept. In addition severe accident procedures are foreseen (SAM) with the aim to return the plant into a controllable state. Work is still underway to substantiate the application of engineered features with the highest priority to prevent corium melt-through of the reactor pressure vessel in case of a postulated core melting.

It is evident that for all six designs accidents beyond the "classical" deterministic design basis have been considered.

Some more involvement of the interested European countries, devoted to discussion and exchange of information (like for example what has been done for the present work) will be the natural way to reach an agreement on a satisfactory common approach to safety.

5. TSO Group position

This chapter is still at a preliminary stage. Work is in progress to define the common TSO group position on the subject of the KI and the steps needed to reach a common approach for those points which at this stage do not present still a full convergence.