Safety-Related
Innovative Nuclear Reactor Technology Elements

– R&D Network –

EC-funded Concerted Action (FI4I-CT96-0013)

TOPICAL REPORT

WORK PACKAGE 1:
INNOVATIVE REACTOR CONCEPTS/
FUTURE R&D REQUIREMENTS

TASK 1.1
R&D RECOMMENDATIONS DERIVED FROM UTILITY REQUIREMENTS AND LICENSING TRENDS/
PART B – LICENSING TRENDS

INNO-SINTER(99)-D-1.1.2

August 1999

Authors:

This report has been established under a Concerted Action funded by the European Commission. The following SINTER Network Partners acted as main authors:

G.L. Fiorini (CEA)
K. Foskolos (PSI)
I. Tripputi (ENEL SpA)

Please contact them directly in case of check-back.

Acknowledgement:

The report is part of the documentation of a collaborative project with contributions, comments and revisions from all partners:

W. VON LENSA (FZJ-ISR, Juelich) Co-ordinator;
G. L. FIORINI, J. PORTA, P. RAYMOND, (CEA/DRN, St. Paul lez Durance);
M. A. CHIMENO, F. ALOMAR (DTN, Madrid);
H. VAN RIJ (NRG, Petten);
F. VETTRAINO (ENEA, Bologna);
I. TRIPPUTI (ENEL, Roma);
F. SEVINI, L. DEBARBERIS (JRC, Petten);
K. FOSKOLOS (PSI, Villigen);
M. KLEIN (SCK-CEN, Mol);
R. SAIRANEN, B. WAHLSTROEM (VTT, Espoo),
F. SCHMIDT (IKE-Stuttgart) and
J. FOEHL (MPA Stuttgart)

This report and a great deal of additional information is available on the Internet. After having registered, it can be assessed via the SINTER Network Homepage:

http://www-is.ike.uni-stuttgart.de/sinter/

INDEX

1. INTRODUCTION

Opposite to research institutions and nuclear industry, licensing and regulatory authorities are not in the forefront of technological innovation. They generally react to technological developments to the extent these are relevant for the licensing and regulatory process of new as well as existing plants. On the other hand, safety authorities (SA) may respond to public and political pressure regarding the safety of nuclear installations, often adapting safety requirements to the expectations of the public opinion. They, thus, can trigger technological development that would help to respond to more stringent safety requirements.

Beyond technical issues with potential regulatory impact, licensing bodies are also concerned by socio-economic and political issues, organizational, management and human resources issues as well as international issues that could potentially affect regulatory practices. These latter issues are, however, not covered in the following chapters. Neither does this report attempt to extrapolate licensing trends out of today's practices and describe a " regulatory future ". Moreover, it elaborates on current licensing issues and open questions raised to this date, to identify possible necessary R&D activities.

In order to identify current licensing issues and open questions, following documents reflecting the present status and discernible trends in the regulatory environment were taken as basis:

- IPSN-GRS Proposals for the Development of Technical Guidelines for Future PWRs, Vol. 1, Common Report IPSN/GRS No 33, March 1997.
- TSO Study Project on Development of a Common Safety Approach in EC for Large Evolutionary PWRs, RISKAUDIT Report No 92/1, June 1997
- Report on Future Nuclear Regulatory Challenges, Final Draft, OECD/NEA/CNRA, November 1997
- Nuclear Science and Technology - 1995 consensus document on safety of European LWR, European Commission, 1996

Reference to the European Utilities Requirement Document (EURD) is also used to identify significant trends or to support the authors judgements.

The aforementioned documents are all of international, mostly European character. Although additional useful information can be found in national papers, these were deliberately not considered. Achieving international harmonization being one of the main trends identified (see below), not consolidated national positions could be rather source of uncertainty and confusion.

It should be noted that these references have often been elaborated for LWR applications. Nevertheless, on a basis of authors judgements, it is considered that most of them are applicable to all the future nuclear plants.

The approach chosen in this paper was to give an overview of the evolution of regulatory and licensing processes in the past and to focus on the main lines of the present practice, in particular reflecting different opinions. Where consensus among several regulatory bodies was achieved, this is pointed out clearly, as well as fields of still existing discrepancies. The short term evolution, as envisaged by the regulatory bodies themselves should be shortly described, and the mid-term evolution is documented only where clearly discernible.

On this basis, necessary R&D topics are identified. This R&D reflects not only the need to get information on unknown issues, but also the necessity to reduce uncertainties and to achieve international harmonization. The former leads, e.g. to experimental investigations to gather data for the validation of models describing novel systems and features. The latter

would, for instance, necessitate better understanding of certain basic phenomena in order to gain a solid basis and a common understanding prior to accept common rules and target values.

After an overview on general licensing trends, this report is structured around the following main issues:

- Radiological impact assessment
- System design, passive and innovative systems
- Methodologies :
  - General approach for the nuclear plant safety related design and assessment ;
  - safety objectives (radiological consequences) ;
  - use of PSA ;
  - methodologies for the identification of PIE and
  - methodologies for the identification of severe accidents to be addressed in the design
- Severe accident prevention and mitigation
- Ageing
- Decommissioning and waste/spent fuel disposal.

2. GENERAL LICENSING TRENDS

In this chapter a general review of the main streams of Regulatory innovations and trends are identified. In most cases reference is made to papers and documents presented by safety authorities, but in some cases, and in particular in the identification of the long term trends, the author judgements had to be used.

First of all currently it is not easy to identify clear licensing trends that can affect the R&D for advanced reactors and the technological innovation. The combination of a clear slow down of the interest for new reactors order and of the traditional prudence of Safety Authorities in changing the licensing bases is leading to weak signs about the future of licensing bases in the medium-long term.

With a few notable exceptions (mainly the French/German initiative on EPR), the focus of all Safety Authorities (SA) is at the moment the assurance of the highest possible safety levels to the operating plants. Therefore issues, like: life extension, aging, plant backfitting, safety levels of plants designed against previous standards are of foremost importance together with new emerging issues related to plant decommissioning, waste disposal and closure of the fuel cycle.

However the need for a licensing framework for advanced plants is shared also by the SA. It is a great opportunity to review what has been done in the past and rationalize it, possibly simplifying it. The real question is the confrontation of the trend for an international harmonization of the requirements, and therefore the need for compromises, and the responsibility of each SA to assure at the national level the safety of nuclear installations according to the role they have been assigned. In particular in Europe the ”internationalization” of the safety requirements is becoming effective both with the agreement of French and German Safety Authorities about the EPR and with the common review of the EURD requirements. With the implementation of a deeper European integration, also safety requirements may be expected to be further harmonized.

On the bases of what has been said above, some trends could be extrapolated, both in terms of content and applicability, for the future nuclear installations others than large PWR. In general safety requirements are probably going to be more restrictive in the future, in accordance with the general trends with other hazardous industries. It would have been preferable to have first a comparison of the associated risks between different industries and then trying to improve the entire quality of life of the population, but this is difficult at the moment from several points of view.

The challenge to the regulators is to assure the highest possible safety to the public and the environment, consistent with the general society safety levels without explicit consideration of the cost of the kWh. In a world rapidly orienting towards open market of the electricity the utilities shall give much greater attention to the cost control and competitiveness also through R&D. The challenge is that this shall not occur not only complying with the regulations, but providing for future plants even greater safety protection than required.

In general it is not the role of the SA to define, or to give indications in order to define, the suitable design options for future installations. Therefore it cannot be expected to have from them formal elements for a long term strategy. However it is possible to identify a number of actions, that, if extrapolated to the future may give some indication of a potential trend.

The most general trends are:

- a more realistic approach to the ”classical” design basis accidents, once the cumulated experimental evidence has been factored in ;

- the consideration of events always more complex and less probable, in order to reduce the ”residual risk”;
- A tendency to minimize interference to population surrounding NPP’s both in normal operations and in case of accidents.

However only the need to license a new reactor on a real site may realistically urge a SA to fully analyze and solve the above issues.

The need for innovative systems is not generally coming from the SA. It is their responsibility to ask for a minimum acceptable safety level that shall be consistent among new and existing plants to the extent possible.

As a matter of fact the SA generally have difficulties to review and accept innovative systems when these are based on new concepts and new technology and, therefore, lack the experience feedback and reliability demonstration that are one of the basis of a licensing review. Therefore an R&D program to support innovative reactors shall also be conceived and carried out to support a future licensing process from all facets, including the reliability one.

3.1 KEY ISSUE A - RADIOLOGICAL IMPACT ASSESSMENT

Health and safety impacts of normal operation, but much more important of accidents have been and are being assessed with large margins and with simplifications in the licensing arena, so that it can be expected that in real emergencies the actual consequences would be different from the calculated ones. The question treated under this heading is whether it can be expected that public safety and environmental protection would be required to reach higher levels and whether the cumulated knowledge and additional R&D may allow more realistic evaluation of accident consequences. It shall be underlined that, since this paper is mainly oriented to trends in technological advancements, the entire question of the low doses effect assessment, which is of foremost importance, will not be addressed.

Trends for the future can be recognized stemming from two considerations:

- the current level of harmonization between different countries is rather low
- the impact on the population and on the environment of even very improbable accidents has to be reduced to ”acceptable” levels

About the first point, it shall be underlined that wide divergences exist in the source term calculation assumptions among different countries for design basis events. The main reason is the different combination of conservatism included in different phases of the process, so that differences exist also in the evaluation of the same design in different countries. It appears that only a trend towards more realistic assumptions could be the basis for the harmonization.

Some first signs can already be recognized. For example in the USA the NRC has published in 1995 NUREG 1465 with a new source term to be assumed in case of Design Basis Accidents, which is a large step forward in the direction of more realistic assessment. Even in this case, however, NRC has maintained its historical position of assuming a ”core melt” source term to assess the consequences of Design Bases Accidents, in contrast with the position of other Safety Authorities and in contrast with the evidence of no core damage for licensed plants in these conditions.

Difficulties in the direction of more realistic assumptions are related also to the level of uncertainties still existing. For example the lack of precise criteria for the fuel cladding failure assessment in the course of an accident or the lack of knowledge about the formation and transformation of several chemical substances in the course severe accident are important factors to be taken into account.

But the attention also of the Safety Authorities have been devoted recently to credible assessment of severe accident consequences. Realistic assessment of consequences related to these events in combination with the performances of evolutionary and innovative proposed reactors may lead to substantial changes in the needed data. It shall be underlined for example, that, while in the past the attention has been given mainly to the acute doses, to which the population was subject at the time of containment failure, and these doses were dominated by Noble Gases and iodine, the situation with the new proposed reactors is changed. Once containment failure in the course of a severe accident can be ruled out and therefore the doses are greatly reduced, the importance of stochastic effects and, therefore, of committed doses, is dominating the risk profile. However, in this case the role of noble gases is greatly reduced and other isotopes, like Ru, Rt etc. with their complex chemistry came into play.

The consequences in terms of R&D may be twofold. A possible way is to proceed with current R&D in the field of Source Term, waiting for example the results of the Phoebus FP experiments in order to reduce the uncertainties. The other possibility is to go around the problem and design reactors that would never enter in the conditions subject to uncertainties.

In parallel to the need of a realistic assessment of consequences, the Safety Authority question is the definition of defining the "acceptable" consequences. After TMI accident and much more after the Chernobyl accident the acceptability of rapid evacuation of large segments of the surrounding population has been questioned. Many experts support the thesis that evacuation, relocation and consequential disruption of the social tissue are among the worst consequences, with indirect impacts also on the safety of individuals.. Evacuation itself causes death toll, stresses, illnesses etc. Therefore a safety objective generally shared is that advanced plants shall try to provide the bases to simplify the Emergency Planning and possibly to completely eliminate the need of public evacuation. By the way this is seen also as a stress reduction for the public during the plant life (not being subject to periodic drills) and also a saving for the utility budget.

As a consequence, some SA are setting the elimination of the public evacuation as a target for the advanced plant designs. French and German Authorities have agreed on this as a basis for the acceptability of the EPR design. The maximum allowable potential release of radioactive materials outside the containment system, i.e. the **design release**, *" should be small, so that only limited protective measures are required ".(see also section 3.3.B)*

Differences exist still in the quantitative objectives to achieve this goal. It can be hoped that the IAEA Safety Series 115 can be used also as a target to demonstrate that public evacuation is not needed.

Another important goal in terms of environmental impact is the importance given to land contamination. Even if the public can be demonstrated that can be moved away from the accident site to comply with the dose objective, their permanent relocation and the loss of land is considered unacceptable at least in several European countries densely populated.

Therefore limits in the total release of the most important isotopes for land and crop contamination are being introduced at least in some countries. In this case it is very important the calculation of the total inventory of isotopes that is released from the plant during the entire accident period. Therefore the long term evaluation of the source term and the calculation of atmospheric dispersion for very long releases are becoming more and more important.

As a consequence different and more sophisticated tools will certainly be necessary for realistic calculations of accident consequences.

3.2 KEY ISSUE B - SYSTEM ARCHITECTURE, PASSIVE AND INNOVATIVE SYSTEMS

3.2.A - System Architecture

The construction and the operation of any nuclear power plant must necessarily rely on a deep study clearly showing that the general safety requirements and recommendations, established by the Safety Authorities and the Utilities, are respected. The plant architecture shall be organized to meet the General Nuclear Safety Objective defined by the IAEA Safety Fundamentals publication : *" To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations* ***effective defenses*** *against radiological hazards ".*

So, for a given NPP, the ***effective defenses*** based architecture (i.e. Lines of Defenses, integrating systems, inherent characteristics, procedures ; see appendix 3.2.1 to this section), answers the overall functional requirements for preventing, managing and mitigating accidents. Systems **redundancy**, **independence**, **diversity** and **maintenance provisions** shall be considered defining the architecture.

For existing reactors, the system architecture is based mainly on a deterministic approach which is applied according the following points :

a) Identification of all the plausible initiating events including transients, incidents, and Design Basis Accidents (DBAs), generally grouped into families and categories according to their frequencies (Postulated Initiating Events - PIE).

b) Identification of the systems, inherent characteristics, procedures (i.e. the Lines of Defence - LOD) needed to prevent or manage the PIE and to mitigate their consequences.

c) For the implemented systems, **redundancy** is introduced to answer the single failure criterion (SFC). Although the postulation of a single failure is a common principle, there are various exceptions in the application of the SFC, and different procedures for applying it.

d) Still for the systems, the **independence** is ensured implementing :
⇨ functional isolation to reduce the likelihood of adverse interactions between equipment and components of redundant trains.
⇨ physical separation (by distance or barriers) to prevent common cause failures

e) **Diversity** is considered to cope with the risk for common mode failures but this solution increases maintenance and plant operation complexity.

f) Safe and reliable behavior need **maintenance**. Two different approaches can be adopted concerning maintenance: the first is to do the maintenance activities during a short period allowed by the Technical Specifications; the second is to implement an additional redundancy in all safety systems (n+2) or to implement a back-up system (functional redundancy) to allow more time for maintenance activities.

For future nuclear power plants, the objective of a significant improvement in safety at the design stage, implies to reinforce the defense-in-depth principle in order to reduce the probability of core melt sequences and subsequent radioactive releases. A broad consensus

between the referenced documents is achieved considering that additional efforts are needed to :

- reduce the frequency of PIE ;
- improve the reliability of safety grade systems (increased redundancy and diversity);
- implement design measures to cope with multiple failures and severe accidents.

Moreover the correct implementation of the different levels of defense in depth should aim at guarantee the **gradual defense**[1], the **defense homogeneity**[2] **and exhaustiveness**[3] (see some practical guidelines in appendix 3.2.2 to this section)**.** These characteristics should be confirmed by probabilistic safety assessment (PSA - see also section 3.3.C).

In this context, in addition to the requirements definition for safety grade systems, also the regulatory treatment of non safety systems, and generally speaking for all the implemented LOD, is considered to be a key issue for future reactors.

The improvement of the operational safety and a significant reduction of the core melt probability is possible by implementing an LOD architecture based on the following principles:

a) The LOD based architecture should be organised on the basis of a deterministic approach defined by the list of Design Basis Conditions (DBCs ; formerly Design basis Accidents - DBAs) and the application of the single failure criterion for the implemented systems ;

b) To determine a suitable combination of redundancy and diversity in safety systems, a probabilistic approach should supplement the deterministic approach ;

c) Testing and maintenance have to be taken into account at the design stage. The needed redundancy can be verified by the PSA, but engineering judgement is needed to balance the uncertainties and limitations of the PSA data and models ;

d) The evaluation of the ability of LOD to fulfil their function should include a systematic analysis of the independence of physical and functional redundancies ;

e) The need for additional LOD and the need for improvement of safety grade systems have to be defined from a multiple failure analysis performed by PSA, and from the need to practically eliminate certain severe accidents ;

f) Increasing the number of redundant trains to increase the reliability claimed for a non-diverse system has a common cause failure limit, typically between 10^{-4} and 10^{-5} per demand ; this lead to implement functional redundancy (i.e. complementary LOD) to meet the current probabilistic objectives (see section 3.3.B).

g) Finally, it is considered that safety improvements can be obtained without burdening the present deterministic rules but by using PSA during the design process.

---

1 *the **lack of** graduality means the existence of " short " sequences for which, upstream from the initiator, the failure of a barrier entails a major increase, in terms of consequences, without any possibility of salvaging the situation at an intermediate stage.*

2 *The homogeneity means that no initiator family participates in an excessive manner to the global probability of the major accident. The homogeneity might also be reached within a same PIE family.*

3 *The exhaustiveness for the e identification of the initiating events should be taken as a target.*

3.2.B - Passive and innovative systems

Innovative and already proven passive systems are suggested for implementation in the design of several future concepts to ensure the three basic safety functions: reactivity control, fuel cooling, and confinement of radioactive substances.

Consensus between the different actors (IAEA, GPR/RSK, EURD, TSO, Designers) is achieved on several items :

⇨ The independence from external energy supply is mentioned as the essential advantage of passive systems.

⇨ Lower driving heads in fluid systems and less operational flexibility are mentioned as examples of possible disadvantages.

⇨ Available tools are not yet sufficiently validated to describe their behaviour. Complementary experimental data are requested both for code validation and for the performance effectiveness demonstration.

⇨ Finally it is agreed that the reliability of passive systems shall be assessed considering that there is no experience which can directly form the basis to do this.

IAEA points out that passive safety features are considered as an engineering tool, not as an engineering or regulatory objective. Consequently a fully passive plant may not be desirable, even if it would be achievable. This position is commonly shared by safety authorities and EURD. A similar consensus is achieved considering that the best use of passive systems may be for ultimate protection within defence-in depth. The first LOD is often better served by active, normal operation systems, particularly as a means to recover as quickly as possible to normal operating conditions in the case of mild transient sequences. This approach is consistent with the principle of diversity.

The GPR/RSK requests the deep analysis of advantages and disadvantages of passive systems including the estimation of their reliability. GPR/RSK recommends the use of passive systems, as far as this is possible as one of several means to minimise the possibility of human errors and to make the plant less sensitive to these errors. As an example for the Containment Building Design, the GPR/RSK proposes a substantial improvement of the containment function during Severe Accidents implementing a last-resort heat removal system which should be preferably passive with respect to its components inside the containment.

Within the EURD, as for the GPR/RSK recommendations, the majority of the requirements is not specifically addressed to either passive or active systems. Although it is requested to consider passive features in the process of designing next generation plants, these features are not considered as a safety goal by itself. Most of the requirements apply to any technical solution of new plant concepts, regardless whether these are active or passive. The EURD says that passive features should only be considered for adoption in the design of the plant if it can be demonstrated that they are appropriate, of overall safety benefit and cost-effective. The use of passive safety components and whole passive safety systems shall be sought, when appropriate for the following purposes: reduction of failure sensitivity, reliability, autonomy, functional separation, diversity, and simplicity.

It is generally agreed that plants which maximise the potential of passive safety can have significantly greater autonomy times than the specified minimum values.

From designer side, there is no uniform approach for the next generation reactor plants in the way they consider passive safety features and systems within their concepts :

- **EPR -** During the conceptual phase of the EPR project a methodology to provide decisions about the use of passive safety systems has been elaborated by the designer and applied. Four categories of criteria were defined: safety ; operation ; simplicity ; costs. Some of the studied passive systems have not been retained on the basis of these criteria.

- **AP600 -** The major plant design requirements for the AP-600 have been the following : simplification ; capital cost reduction ; construction schedule reduction ; safety improvement ; one step for licensing ; no need of prototype for the plant ; standard design for US sites ; extended plant-life. In order to achieve the above objectives, the approach used in designing the AP-600 systems was to simplify systems in general, to utilise passive systems as far as possible for the safety functions, and to optimise system design through plant arrangement and modularization.

- The **innovative passive concepts** (e.g. PIUS) implement passive systems to a larger extent. No exhaustive and detailed analysis (e.g ; versus all the criteria implemented by the EPR) is available. Difficulties for the operability and lack of competitiveness seems to be the key reasons to explain the lack of success in promoting such a concepts.

Within this context, the basis to imagine the short or mid term evolution is that the criterion for the safety assessor will be that the proposed system fulfils the required safety function with the appropriate reliability duly demonstrated. The competitiveness is a complementary key criterion for the acceptability. This is why the R&D programme on innovative passive systems should be defined integrating the following items which request specific efforts on the following items :

- practical implementation of the principle of defence-in-depth, requirements of redundancy, diversification, single failure criteria, common cause failure ;
- new accident scenarios such as inadvertent operation or interactions with other systems ;
- definition of failure criteria for all accident conditions ;
- protection against internal and external events ;
- limitations of analytical safety demonstration, need of experimental safety demonstration, need of prototype ;
- effects of ageing, e.g. surface oxidation, clogging, radiation ;
- diagnosis of state ;
- inspectability, recurrent testing, in-service testing close to operational mode ;
- sensitivity against human errors ;
- interconnections between passive systems, must be investigated with respect to possible disadvantageous interactions.

Still about the open issues, the advantage of possibly higher reliability values calculated for passive systems, arising from features such as lower number of components and parts, may be diminished or even eliminated by larger uncertainties currently present.

General approaches for the assessment of reliability of passive systems are not yet settled and not yet generally agreed. Reduced impact of known and generally dominant failure modes due to simple concept or stand-alone character may lead to increased and even dominant contribution of usually less important factors such as failure of integrity, reduced testability under incidental conditions and limited thermal hydraulic modelling.

On the other hand it is recognised that the combined use of passive and active systems or components for the same safety function potentially provides a high degree of diversity.

Moreover passive systems may potentially be more robust against extreme accidents. This would favour the use of passive systems for ultimate protection as final LOD. Simultaneously, high energy density in the beginning of accidents may require use of active systems. Frequent events should also be dealt with by active systems, provided this would enable a swifter recovery to normal operational conditions. Accident management may also benefit from the ability to utilise systems that can be controlled by operators[4].

For the final comparative assessment it is essential to consider that the potential advantages of passive systems over active systems are not necessarily applicable to all passive systems. The importance of possible disadvantages may also vary from case to case. They may not apply in total to one particular system.

Referring to the passive systems for DHR, there are specific challenges on thermal-hydraulic codes for the safety demonstration of novel passive systems function : low system pressure, low pressure differences, influence of non-condensable gases, large volume mixing, system interactions between active and passive systems, instabilities, etc.. Model modification and improvement may be necessary.

Complementary R&D is justified to explore the potential of such systems for other safety functions (e.g. reactivity control).

3.2.C - Instrumentation and Control

The detailed analysis made on this key issue by the TSO group is available. Following this analysis, nuclear licensers, designers and users of computer based safety systems have now become well aware of the problems raised by the qualification of software for safety applications. These problems are essentially due to the difficulty of detecting software faults most of which are design faults, to the difficulty of testing with sufficient coverage the large number of distinct behaviors of a discrete system, and thereby to the difficulty of assessing the reliability of these systems. These difficulties are amplified by the possible common cause failure modes that software systems can induce in I&C protection and control systems.

A number of initiatives are currently dealing with software related issues. Basically they follow two kinds of approach. A number of them aim at identifying specific issues, either generic or particular to a given phase of the software development process - and intend to give guidance on how to deal with these issues. Others, emphasize guidance on how to design systems and to collect evidence for the safety case of a software based system.

The GPR/RSK Proposal gives some general recommendations. For instance, it is indicated that the three main principles for designing computers for safety systems are fault avoidance, fault removal and fault tolerance, and that, following GPR/RSK, diversity has to be examined to achieve software fault tolerance.

Utilities (i.e. the EURD document) clearly intends to focus on digital technology. EURD makes little distinction between hardware and software, and, in its present version, pays yet too little attention to the specific aspects of the use of programmable systems for safety critical applications.

Nine specific dependability issues have been identified by TSO : Hardware/software fault-tolerant architectures ; Multi-processing and Communications ; Software reliability targets and assessment ; Defence against common mode failures ; Fault Tolerance Characteristics ; Documentation ; Formal specification and verification methods ; Use of automated development tools. Following the TSO position, it appears that none of the evolutionary PWR designs investigated by the group, presented definitive answers which would have allowed any of these specific issues to be dismissed.

---

[4] *By definition the passive systems cannot be " controlled " by the operators.*

Taking into account the TSO remarks that insufficient information was available to deal in depth with the above nine specific issues, the group position for a future common approach is tentatively based on the following elements:

- Software engineering techniques and good practices are available to ensure high quality software products. The difficulty however is to assess quantitatively - or with at least sufficient precision - the reliability of ultra dependable software systems.

- The potential for common mode failures caused by common design fault is a major issue and a major weakness of software intensive systems important to safety. No design today can rely on a single type of defences. A set of congruent defences must be explored, of which physical isolation, system diversity (different systems performing the same function) and functional diversity (different functions reacting to the same PIE) are the most important ones to take into consideration.

- More attention should be paid to designs which are amenable to dependability demonstration, particularly at the architecture system level. This means also that the different aspects of dependability, the different types of possible demonstrations, and above all the different kinds of evidence (including operational experience) that should be collected must be understood and clarified.

- A major problem of computer based systems is the correct transformation of the safety system requirement's specifications into the software specifications.

Other important problems, only indirectly dealt with in this key issue, should require attention and possibly are in need of an agreement on a common position :

- Different degrees of safety criticality may exist for I&C systems, and a graduation of safety classes and corresponding engineering requirements can be established.

- Licensing methods of digital protection systems : the practices followed in the different countries should be compared and tentatively harmonised.

- Environmental and Dynamic Qualification : criteria and methods of qualification of I&C equipment for EPR should be established, given that differences exist between practices followed in European countries.

- Requirements for additional monitoring instrumentation for severe accident management should be investigated.

- Diagnostic Instrumentation. The safety relevance and requirements of early failure detection and diagnosis instrumentation should be identified. The applicability of advanced knowledge processing techniques (e.g. artificial intelligence) should be clarified.

On the other hand, the TSO analysis does not tackles the human factors issues in relation to plant computerised control. In fact it appears that the trend towards the generalisation of computerised systems in plant control and/or supervision opens wider subjects of concern than the problem of reliability of the computerised functions by themselves.

As far as human operators are supposed to be kept in an active role in the plant operational safety, one must ensure that the computerised systems involved in the plant operation do not prevent them from keeping in the control loop, particularly in complex situations exceeding the design hypothesis of these control functions.

Therefore several topics relating to plant control computerisation seem to deserve a particular attention for future advanced plants :

- Operations of plants with computerised controls (a common experience return of projects already operational (French N4, ABWR...) could help to identify the pros and cons of generalised computerized controls) ;

- conditions of co-operation and tasks allocation between operators and computerised systems enabling optimum performance and plant safety ;

- level of cognitive guidance that should be provided by the computerized decision aids to the operators under disturbance operation ;

- level of plant automation, particularly under disturbed operation.

These questions are related in fact to the problem of " user oriented design " that is totally forgotten, the reflection being restricted to the safe design of technological functions.

Since a large number of safety problems arise from human errors, it is reasonable that some consideration be given to the above topics in the design of the control systems.

Appendix 3.2.1 : The notion of Lines of Defence

As discussed within the key issue on the " methodologies " (see section 3.3), the principle of " defence in depth - DD " shall be maintained and even reinforced ; nevertheless some remarks concern its applicability to the practical design of the future reactors.

⇨ Before considering the systems, design approach should define how **inherent safe behaviour and characteristics** can participate to stable operation (first level of DD : Prevention) and can reduce the risk of severe accident (fourth level of DD : e.g . reduction of important reactivity insertion and of potential source term).

⇨ The complexity of the plants " safety architecture ", the need for the coherency with the defence in depth concept and with the probabilistic objectives currently adopted, lead to suggest the notion of **the Lines of Defence (LOD)**. This notion is already present within the documents taken as reference but it is not systematically developed.

⇨ The " Line of defence is an effective defence[5]. This term is used for :

- any inherent characteristic, equipment, system, etc., implemented into the safety related plant architecture,
- any procedure foreseen coherently with the General Rules for Plant Operation (e.g. human actions : preventive, protective, etc.)

the objective of which is to accomplish a given safety function ".

The implemented LODs shall fulfill the missions requested to prevent abnormal situations or to bring back the plant from the Plausible Plant Condition into a controlled safe condition and to maintain it in a safe state. That is these LODs, coherently with the defence-in-depth principle and depending on their rule, shall permit to the plant to meet the safety objectives : preventing, or managing, or limiting the possible PPC consequences.

The idea on which the proposed concept is based is that, following a PIE, the passage from the normal plant condition to the degraded condition results from the failure of one or more LODs[6]

⇨ It is suggested to introduce the Lines of Defence (LOD) concept as a practical mean to apply the DD principle at least for the **preliminary design phase**.

According to the concept of **defence in depth**, the **safety design** leads to practically implement these **lines of defence** organising the global architecture and their interactions. The plant **safety assessment**, both for normal and abnormal plant conditions, leads to identify and count these lines, verifying they are able to fulfil the requested missions (performances) with the needed reliability. Such a method is close to the Probabilistic Safety Assessment (PSA) even if it is not as rigorous, in particular from a quantification point of view. Nevertheless, if it is conducted " systematically ", it can allow the identification, by comparison with the probabilistic objectives duly defined, of the main **weak points** of the

---

[5] cf. the General Nuclear Safety Objective in the IAEA Safety Fundamentals publication : *" To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations **effective defences** against radiological hazards "*

[6] A detailed analysis shows that even the "inherent characteristics" are characterised by a given "reliability". Generally speaking, this reliability, is defined as the probability to fail the requested mission to achieve a generic safety function. This reliability depends on environmental, physical, nuclear or chemical phenomena, and passive component reliability.

concept under examination (i.e. : insufficient or exaggerated number of lines ; inhomogeneous treatment inside a same family of initiators ; existence of " short " sequences for which, upstream from the initiator, the failure of a line entails a major increase, in terms of consequences, without any possibilities of salvaging the situation at an intermediate stage). This type of information can first lead to the motivated hierarchisation of additional and/or support studies, necessary to complete the real safety analysis. As well, they can help in conducting the real PSA which would allow, downstream, to confirm and quantify the results.

Appendix 3.2.2 : The implementation of the *defence in depth* for the design option selection

The different levels of *defence in depth* shall be systematically applied :

1st level : Prevention : Quality in design and achievement, prevention of nonconformity

- Facility with an excellent inherent resistance so as to reduce risks of failures or internal hazards
- In-depth study of all the predictable plant conditions both normal and off-normal ;
- Appropriate and clearly defined safety criteria ;
- Facility with a reduced potential for consequences following off normal sequences;
- Use of well established and qualified rules and codes which provide, at all times, sufficient margins related to the limits defined to ensure the proper behaviour of the facility ;
- Margins in order to avoid constantly using the systems designed in case of off-normal operating conditions ;
- Choice of materials and fabrication controls in compliance with the design and construction rules;
- Compliance to the existing quality assurance rules ;
- Integration of the safety culture in the design team and in the operating team.

2nd level : Surveillance, detection and control : Quality of operation, keeping the facility within authorised limits

- Measures anticipating failure : periodic surveillance program which recognises the off-normal evolution of the most important material, which could, in the long run, lead to failures (periodic controls and tests). The maintenance policy will therefore be based on:
  - a preventive programme (periodic controls)
  - an on line control of the operating parameters
  - a predictive programme for the equipment whose reliability is of vital importance and for which experience feedback does not allow to determine systematic replacement times.
- Regulation, control and protection systems which are sufficiently reliable, in order to detect a nonconformity or a failure as soon as it occurs, and to stop an off-normal evolution before the materials are solicited beyond the foreseen conditions.

3rd level : Safety systems and Protection systems design : Postulate of all plausible incidents and accidents and implementation of means to limit the effects of these accidents to acceptable levels.

- Postulate of all plausible incidents and accidents.
- Implementation of means (inherent characteristics, engineered safety features and protective systems, procedures) to limit the effects of these accidents to acceptable levels.
- The choice of postulated incidents and accidents shall be done at the beginning of the project, with the aim to integrate perfectly the needed systems to the whole facility.

4th level : Accident management and containment protection, limitation of consequences : Prevention of deterioration of accidental conditions and limitation of severe accident consequences.

- Integration of multiple failures (e.g. postulate of loss of redundant safety systems).
- Implementation of additional measures (inherent features, adapted materials, procedures) to be able to face operating conditions which have not been treated by the first three levels but are likely to lead to significant releases, and to limit the consequences of severe accidents.

Nota bene : the notion of multiple failures leading to highly hypothetical sequences is not systematically integrated by the designers. To take into account these sequences is essential to achieve a correct severe accident prevention. Moreover the principle for the implementation of additional dedicated measures to cope with such a sequences is essential.

5th level : Response outside the site : Limitation of radiological consequences for populations in case of significant releases.

3.3 KEY ISSUE C - METHODOLOGIES

3.3.A. General approach for the nuclear plant safety related design and assessment

All the Plausible Plant Conditions (PPC), intended as operating conditions or incident/accident events, needed to design the safety related plant architecture and to design its components, should be grouped into two main families : the Design Basis Conditions and the Design Extension Conditions.

3.3.A.1 - Design Basis Conditions

Referring to the European Utility Requirements (EURD) document (Vol. 1, Appendix B), the definition of Design Basis Condition (DBC) is : *" normal condition, incident and accident conditions of internal origin for which the plant is designed according to established design criteria and conservative methodology "*.

The conventional DBC - formerly called Design Basis Accident (DBA) - is characterised by a Postulated Initiating Event (PIE), which occurs when the facility is in a given initial state. All the initial states characteristic of the plant (steady states and operational transients) shall be clearly defined by the designers. For each DBCs, the safety related plant architecture response has to be analysed to verify that the acceptance criteria, set forward for each of them, are respected. Indeed a traceable safety review requires that - for each DBC - the relevant acceptance criteria are clearly identified. In this respect, the TSOs " *encourages a clear identification, where an unambiguous cross-reference DBAs* (i.e. the DBCs ; NDR) *versus acceptance criteria' is established* ".

Each PIE shall be classified by category, based on their estimated occurrence frequency (i.e. in terms of frequency (f): events / reactor · year). Therefore, by analogy with the PIEs, a similar categorisation is chosen for the DBCs. The plant safety assessment is structured through the analysis of these DBCs. As an example, the Table 1 summarises the categorisation used in France.

DEC Category	Definition	Occurrence frequency (events / reactor · year)	Qualitative acceptance criteria
I	**Normal Operation conditions**	list of operational events to be defined explicitly	Plant conditions within the limits of the technical specifications and defined in the general operating rules
II	**Incident conditions**	$10^{-2} \sim < f$	Consequences must remain extremely limited
III	**Accident conditions**	$10^{-4} < f < 10^{-2}$	Consequences must remain sufficiently limited
IV	**Hypothetical accident conditions**	$f < 10^{-4}$	Consequences must remain acceptable

Table 1 - Conventional design basis conditions categorisation.

3.3.A.2 - The Design Extension Conditions

To complete the deterministic approach, the compliance with the 4th level of *defence in depth* (see appendix 3.2.2) imposes, on one hand, the integration of a possible lack of exhaustiveness in the deterministic assessment and, on the other hand, the demonstration of the potential of the facility for the prevention, control and limitation of the consequences of "severe accidents"[7].

The TSO elaborated a set of recommendations for the treatment of severe accidents for future PWRs. Coherently with the principles evoked in the introduction, it is considered that they are broadly applicable to the future nuclear installations :

" (...) For future designs, accidents beyond the "classical" deterministic design basis have to be considered at an early stage of the design to obtain a significant reduction of the probability of occurrence of severe accidents. Accident situations which would lead to large early releases have to be "practically eliminated". For the remaining accident situations (...), the potential release of radioactive materials outside the containment system should be small, so that only limited protective measures are required.

The accident scenarios to be considered early in the design process should be all those accidents, even of very low probability, that can be judged as physically plausible. (...)

Severe accident sequences should be either "practically eliminated" if sufficient preventive design and operation provisions are taken, or "dealt with" (...).

TSO point out that the "practical elimination" of such accident sequences " *shall be matter of judgement and each type of accident sequences has to be assessed separately. Due to the limited knowledge on some physical phenomena and due to the large variety of these types of accident sequences, the safety authority considers that their "practical elimination" cannot be demonstrated by the compliance with a general " cut-off " probabilistic value.* "

Therefore *" There is a need to develop adequate guidance to clearly establish when "sufficient design and operation provisions" have been taken to practically eliminate a severe accident sequence. "*

Finally *" Evaluation of severe accidents should be performed using a "best-estimate" approach together with a quantification of the uncertainties to determine, for representative scenarios, a spectrum of the possible outcomes. Systems and components provided only for severe accidents, should not require the same conservative analysis and requirements that are necessary for those developed to cope with "classical" design basis accidents;(...). There should be a high confidence that necessary equipment will survive severe accident conditions for the period that it is needed to perform its intended function ".*

In order to answer these requirements, the conventional DBCs should be completed by the integration of accidental situations generated by multiple failures (e.g. : the total loss of the redundant systems) or the severe accidents. These situations studied for the prevention, the control and the limitation of consequences are qualified as Design Extension Conditions

---

[7] Considering the needs for taking into account the different reactors specificity (e.g. no core melting (?) for the gas cooled reactors core) the following definition is suggested to be applicable for future nuclear installations **:** *Severe accidents are sequences with an estimated frequency lower than the Design Basis Conditions. In these accident conditions, the plant suffers damage. The potential for the release, outside the containment, of a significant radiological source term greater than the design release (i.e. unacceptable for the environment) exists.*

(DECs)[8]. Referring to the EURD (Vol. 1, Appendix B), the definition of DEC is : *" A specific set of accident sequences that go beyond Design Basis Accidents (DBA), to be selected on deterministic and probabilistic basis and including : (1) Complex Sequences, and (2) Severe Accidents. Appropriate design rules and criteria are set for DEC, in general different from those for DBA "*.

Two types of accidents shall be considered :

- the *Complex Sequences* for the prevention of severe accident configurations (i.e. core meltdown for fission reactors). The analysis of these sequences can lead to design additional systems and/or to adapt existing systems to guarantee that the corresponding safety objectives are verified. For these situations, additional failures will not be taken into account, and the conservative margins will be smaller compared to the DBC ones. >From the safety point of view, the designer should aim at meeting the conventional design basis targets (4th category of Table 1).

- the *Severe Accidents* for the prevention of releases greater than the **design release**. Specific objectives are established : the consequences *" should be small, so that only limited protective measures are required "*. As for the situations above, additional failures will not be taken into account, and the conservative margins can be smaller. The " *quantification of the uncertainties to determine, for representative scenarios, a spectrum of the possible outcomes* " is also an essential step.

For each of these families, a limited number of operating situations shall be identified and examined. These two classes (DBCs and DECs) of conditions compose the plant **Design Basis** (i.e. the complete set of PPCs used to design the " effective defences ").

Other accidental situations *" which would lead to large early releases"*, i.e. the release of which is estimated as greater than the design release, " *have to be practically eliminated ", i.e.* it is necessary to demonstrate that they are either excluded by design, or that their occurrence frequency allows them to be rejected in the Residual Risk (RR ; i.e. practically excluded). These situations will not be analysed. This part of the approach meets the recommendation for the exclusion of any " cliff edge effect " [9] leading to an early release of a non-admissible source term.

Referring to the authors judgements, a nuclear installation which inventory is greater than the one " unacceptable for the environment " should answer the requirements evoked above.

3.3.A.3 - The Global Approach

The global approach for the nuclear safety assessment is summarised in the Fig. 1 where all the notions discussed above are structured and presented.

---

[8] Design Extension Conditions (DECs) is the terminology suggested in the European Utility Requirements document. The same concepts are grouped within the Risk Reduction Categories (RRC) of the European Pressurised Reactor (EPR).

[9] This risk corresponds to the mobilisation of a potentially unacceptable source term - severe accident - with the simultaneous loss of the containment (releases much higher than those which are acceptable).

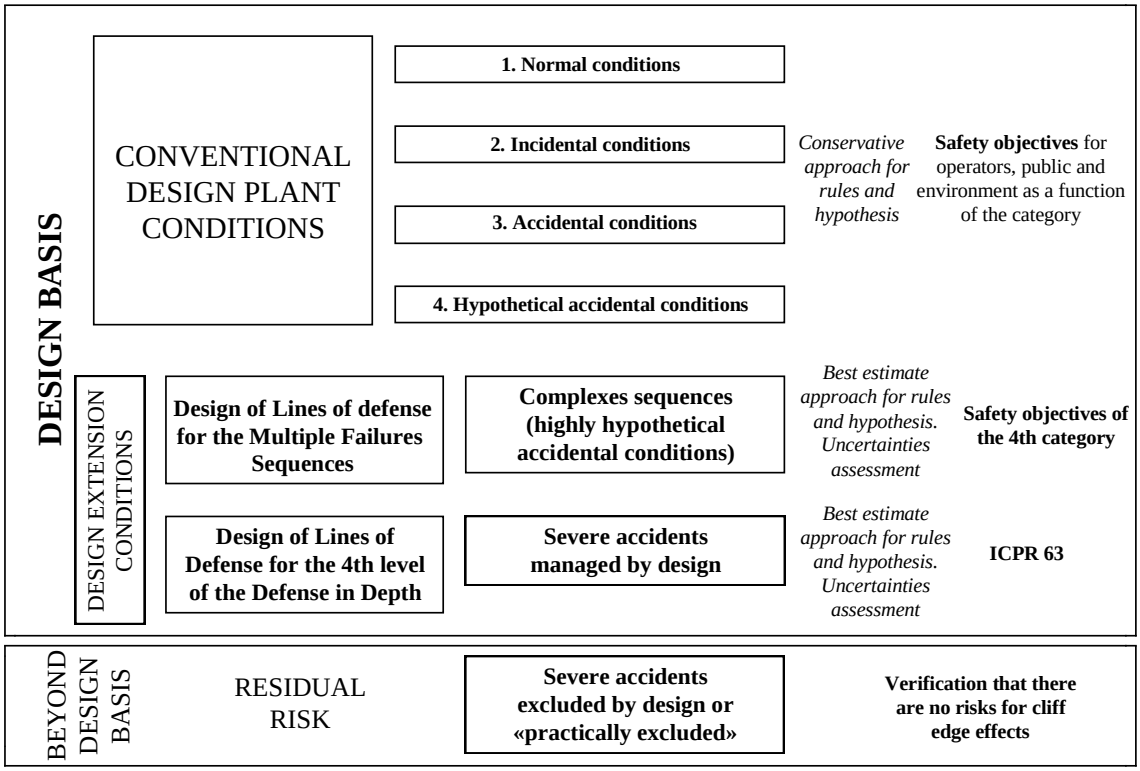

Figure. 1 - Safety Approach for Plant Design and Assessment

Finally, within the frame of the methodology in terms of still open issues there are needs for :

- a clear identification of unambiguous cross-reference DBCs versus acceptance criteria should be established ;
- to develop adequate guidance to clearly establish when "*sufficient design and operation provisions*" have been taken to practically eliminate a severe accident sequence ;
- to define the rules for the “best-estimate” approach applicable to the evaluation of severe accidents and
- to define the rules for the quantification of the uncertainties to determine, for representative scenarios, the ”*spectrum of the possible outcomes*”.

3.3.B. Safety objectives

3.3.B.1 - Allowable Radiological consequences

The General Safety Objectives define the allowable radiological consequences for the personnel, the public and the environment, during normal, incidental or accidental conditions. The retained limits shall be coherent with the ICRP recommendations, or the IAEA Safety series 115. Targets (i.e. challenging objectives below the limits) can be defined coherently with the adoption of the As Low As Reasonably Achievable (ALARA) principle.

For future plants important requirements are already available.

For example, for future large fission reactors the TSO proposal mentions that "*For accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant (no evacuation, no sheltering) (…)*". This objective should be applicable to all nuclear installations for the DBCs and for the Complex Sequences (see Fig.1).

Still referring to the Safety Authorities recommendations, for the severe accident situations the potential release of radioactive materials outside the containment system, i.e. the **design release**, *" should be small, so that only limited protective measures are required ; accident situations which would lead to large early releases have to be practically eliminated ".*

3.3.B.2 - Use of probabilistic studies

There is a broad consensus to considers that probabilistic safety assessments are an analysis tool supplementing the deterministic studies and that the results of these probabilistic assessments should be considered as indicators (see also section 3.3.C). For the future and innovative concepts, the main difficulty could come from the lack of reliable data. On the other hand, the implementation of probabilistic approach needs the definition of clearly understandable probabilistic objectives (i.e. technical safety objectives).

3.3.B.3 - Technical safety objectives

For future fission plants the reduction of the probability of core meltdown (Core melt frequency - CMF) from that for present reactors should be a target in itself. A design target of 10^{-6}/ reactor · year should be set for internal events ; this target should be compatible with those set internationally, in particular by INSAG 75-3 (10^{-5} / reactor · year, with all types of failures and events taken into account). This target should be applicable to the future nuclear installations for the " severe accidents ".

On the other hand, a global probabilistic target for the **design release** of 10^{-6} / reactor · year, for all initiating events is retained for fission plants. Referring to the GPR/RSK :*" Such a target makes it possible to direct the choice of provisions with the intention either of eliminating certain families of events of internal origin for which the containment has not been designed, or of defining families of external events to be retained in the design basis. This does not preclude the need, for certain families of events, for example those with highly significant consequences, from making specific arrangements even if they have an extremely low probability of occurring ".*

It is interesting to point out that equivalent objectives are retained in the EUR document :

- *Core damage cumulative frequency shall be lower than 10^{-5} / reactor · year ;*

- *Cumulative frequency of exceeding the Limiting Release* (i.e. the design release ; NDR) *shall be lower than 10^{-6} / reactor · year ;*

Moreover EURD recommend that :

- *Sequences involving very large releases shall have a cumulative frequency well below the previous target of 10^{-6} / reactor · year.*
  Nota Bene : The acceptability/applicability of this last requirement should be verified taking as reference the TSO position on " practical exclusion " as showed on section 3.3.A.2.

In summary, referring to the authors judgements, these objectives could be generalised to future nuclear installations saying that

- the cumulative frequency for the **severe accident**, i.e. mobilisation of a potentially unacceptable source term inside the last barrier, should be lower than 10^{-5} / reactor · year ;

- the frequency of 10^{-6} /reactor · year is applicable to the **design release** that will ask only for limited protective measures.

3.3.B.4 - The allowable risk domain

As discussed above, PPCs are categorised according to the corresponding estimated frequency; higher radiological consequences can be deemed tolerable for categories of lower estimated frequency. For the different reference incidents and accidents with radiological significance, appropriate technical criteria have to be respected. For these incidents and accidents, assuming the corresponding technical criteria are respected, it has to be verified that, radiological consequences are tolerable.

Finally, some events are rejected into the Residual Risk category 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 situations.

Figure 2 summarise the allowable/non allowable risk domain. A tentative qualitative comparison with the INES Scale classification is presented.

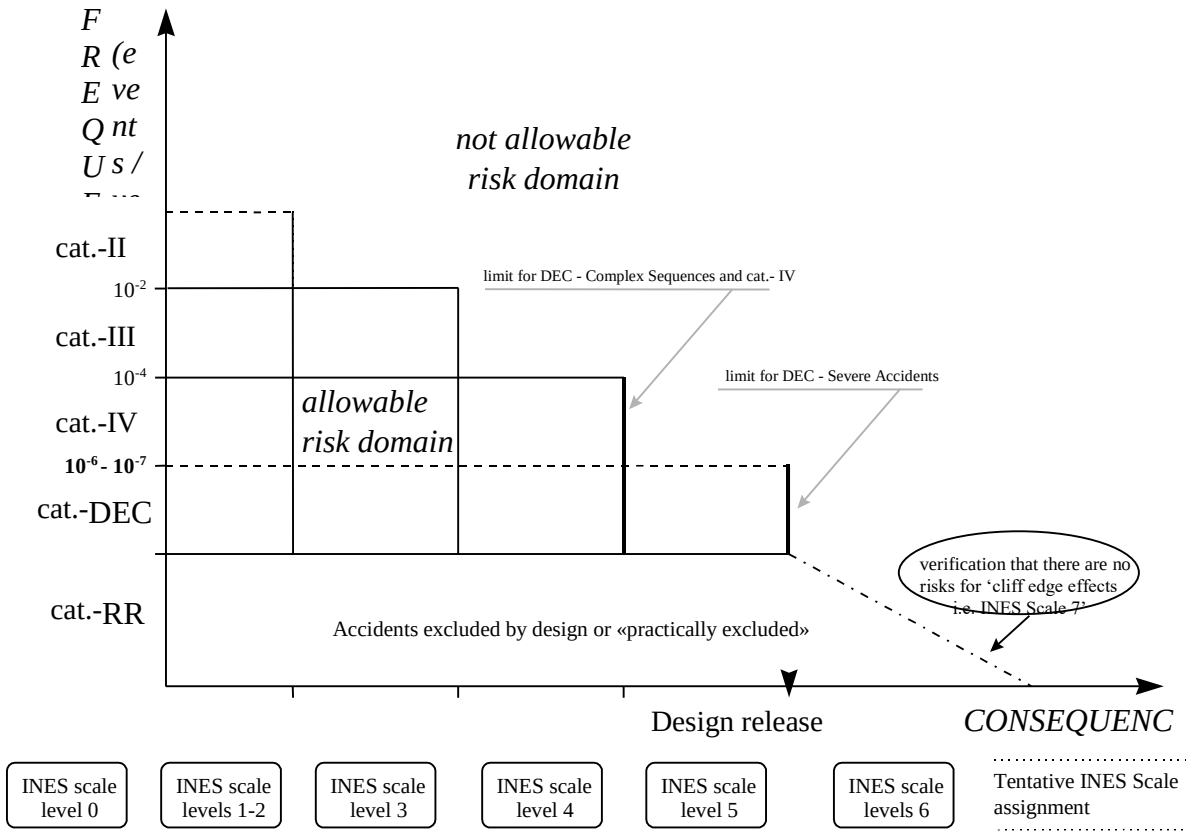

Figure 2 Allowable/non allowable risk domain

3.3.C. Use of PSA

All policies agree that the principle of defence-in-depth should be maintained and even reinforced. To achieve this, the design should be made on deterministic bases, supplemented by the use of probabilistic methods. The reinforcement of the defence-in-depth of the plants will, however, imply a more extensive consideration of the possibilities of multiple failures and the implementation of diversified means to fulfil the three basic safety functions whatever the state of the plant could be.

Referring to TSO (cf. also §3.3.A.2), as a design goal for future plants, accident situations which would lead to large early releases have to be " practically eliminated " when they cannot be considered as physically impossible, design provisions will have to be taken to design them out. Practical elimination of such accidents is a matter of judgement : due to the limited knowledge of some physical phenomena and due to the large variety of these types of accident sequences, their practical elimination cannot be demonstrated by the compliance with a general " cut-off " probabilistic value.

Probabilistic safety assessments and quantitative probabilistic targets are considered as important tools and guidelines at the design stage to gain an in-depth understanding of the relative weaknesses of plants and to deal with complex situations involving multiple equipment failures and/or human errors. A PSA at the design stage of the PWR should be performed with the objective to support the choice of design options, to include redundancy and diversity of the safety systems within a well-balanced safety concept and to appreciate the improved safety level as compared to existing plants. It should be an iterative process, considering the actual stage of the project in each iteration.

The design stage PSA should cover sequences up to core melt (Level 1) and include a probabilistic assessment of the containment performance for core damage situations (partial

Level 2).The designer would have to consider a list as complete as possible of initiating events, without omitting such events as loss of heat sink, interfacing loss of coolant accidents, steam line breaks, accidents during shutdown states, etc. For those internal and external hazards the probabilities of which cannot be realistically determined, provisions have to be implemented by the designer to obtain a consistent design. However, the application of PSA at an early stage of design will have to be handled cautiously because the final results will be dependent on the real choice of components, system techniques and operational procedures.

Evaluation of PSA results against quantitative probabilistic targets (see section 3.3.B.3) 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.

Reduction of the frequency of occurrence of accidents can be obtained by reducing the frequency of initiating events and by further improving the availability of safety systems. The aim of reducing the frequency of initiating events implies to increase, as far as possible, the reliability of operational systems and components. In particular :

- High pressure core melt sequences must be prevented by design provisions for the secondary side safety systems and if necessary for... the primary feed and bleed systems.
- The reliability of the shutdown function has to be high enough to contribute to “practically eliminate” high pressure core melt sequences.
- The residual heat removal function must be ensured with a high reliability.
- Accident sequences involving containment bypassing have to be “practically eliminated” by design provisions aimed at assuring reliable isolation and also preventing failures.
- In PWR, reactivity accidents resulting from fast introduction of cold or deborated water must be prevented by design provision so that they can be excluded.

The above tendencies indicate following possible fields of necessary R&D activities :

- Methods for obtaining reliability data for new components and passive systems.
- Detailed analysis of operating experience.
- Definition of a coherent and harmonized methodology and acceptance criteria for the use of PSA, especially for common mode failures.
- Development of a common approach for PSA application during the licensing process.
- Sensibility studies to deal with uncertainties associated to the treatment of common cause failures.
- Validated data for the treatment of human interventions.

3.3.D. PIE-Identification

Possible incidents and accidents within the plant have to be considered to demonstrate that the required safety level is achieved. The accident scenarios to be considered early in the design process should be all those accidents, that can be judged as physically plausible. The process of selection of these scenarios should be based primarily on deterministic analyses, probabilistic considerations, and engineering judgement. The incident/accident analysis comprises the identification of reference accidents and accidents which could have radiological significance. It seems appropriate to categorise these reference incidents and accidents according to the estimated frequency of the corresponding postulated initiating events (PIE ; see section 3.3.A.1).

Analysis of the operating experience of current reactors can contribute in a valuable way to establish the list of PIEs to be considered in the deterministic design of future reactors. The existing deterministic requirements for protection against external events and hazards should be maintained during the design phase, supplemented by probabilistic requirements. Using a probabilistic approach in addition to any deterministic one might be of most benefit for more innovative or novel designs, especially where there is less certainty of correctly identifying and categorising the PIEs from experience from previous reactors. The Safety Analysis Report of future reactor designs should document the reasons for each PIE categorisation.

Complementarily to single initiating events, the safety demonstration has to analyse multiple failure situations as well as internal and external hazards. Particular attention should be paid to minimising the possibilities of common mode failures. The principle of physical and spatial separation should be applied as far as possible, as well as an effective defence against fires and flooding. The “defence-in-depth” principle has to be fully applied to the protection against internal hazards so as to limit the likelihood and the consequences of such hazards by the implementation of prevention, control and mitigation provisions.

For LWR, providing adequate leak before break measures, the loads to be considered for the design of the internal structures of the reactor vessel and for the design of the structures in the containment building can be limited to those resulting from a break equivalent to the complete guillotine rupture of the largest pipe connected to the main coolant line (surge line). Larger LOCA are considered for the design of the emergency core cooling system (ECCS) and the containment.

To minimise the possibilities of common mode failures, it is recommended to install the parts of the safety system trains which are located outside the containment building in divisional areas designed to that event the complete loss of one divisional area due to a specific internal hazard would not prevent the fulfillment of the three basic safety functions. Also, the design and layout of pipes, vessels, tanks, pumps and valves shall base as far as possible on the principle of physical or spatial separation.

The occurrence of internal hazards during shutdown states has to be considered at an early stage of the design. Particular attention has to be devoted to assess the completeness of the potential causes of such hazards.

Potentially necessary R&D can be envisaged in the following fields :

- Harmonisation in the definition and the application of the single failure criterion and in the distinction between active and passive failures.
- Extension of the grace period
- Treatment of uncertainties in analyses using best estimate models and codes and more realistic hypotheses and input parameters.
- Analyses of existing practices (as applied by regulators for operating plants or by vendors) to evaluate whether there is a need for further harmonization.
- Analyses to show compliance with European criteria for radiological consequences of nuclear accidents.

3.3.E. Identification of the Design Extension Conditions (formerly Beyond Design Basis Accidents - DEC)

For future designs, accidents beyond the "classical" deterministic design basis will have to be considered at an early stage of the design to obtain a significant reduction of the probability of occurrence of core melt accidents (see section 3.3.A.2). Accident situations which would lead to large early releases have to be "practically eliminated". For the remaining accident

situations involving core melt, the potential release of radioactive materials outside the containment system should be small, so that only limited protective measures are required.

As pointed out, the accident scenarios to be considered early in the design process should be all those accidents, that can be judged as physically plausible. However, there is no widely accepted methodology to identify those DECs to be considered in the design. PSA should be used for that purpose, but work remains to be done to agree on a common methodology and decision criteria.

Many of the identified DECs are related to multiple failure situations. Some situations are studied using a deterministic approach, some others are studied by PSA. For the deterministic approach, the use of best estimate analyses for DECs is an acceptable practice. In those cases where the probabilistic approach is used, the main objective should be to show that the DECs do not contribute significantly to the overall risk of the plant.

The analysis of potential severe accidents has been incorporated into the regulatory process. Severe accident studies are being performed in all countries even though they are not required in most countries by the regulations; it is commonly accepted that severe accident studies should be best estimates taking into account the related uncertainties.

Among the main lessons learned from the TMI accident (and to a lesser extent from the Chernobyl) was the need for a more detailed understanding of severe accident phenomena and how to prepare mitigation for them. More recently, it became evident that it is necessary to review systematically the analyses of accident initiators at zero and low power to confirm the adequacy of designs in this area.

Most uncertainties relate to the detailed description of the progression and timing of core melt or the likelihood of containment failure. However, though of interest for the design of new plants, reduction of most uncertainties would not change the most important severe accident management decisions. There is now a general consensus that, for LWR designs, the following plausible phenomena could occur in some or all of the sequences with core degradation :

- In vessels debris cooling.
- Core concrete interaction and ex-vessel debris cooling.
- High pressure core melt with containment failure due to the combination of pressure and heat.
- Steam explosion in containment due to water being in the cavity.
- Late containment failure due to overpressure caused by steam build-up or direct heating from uncovered corium pool.
- Hydrogen burning or detonation causing damage of the containment.

The two first shall be assessed within the context of severe accidents scenarios and their analysis can lead to design additional LOD and/or to adapt existing LOD to guarantee that the corresponding safety objectives are met.

All the other shall be excluded by design or " *practically eliminated "* implementing *" sufficient preventive design and operation provisions "*. As already stressed, these situations will not be analysed. This part of the approach meets the recommendation for the exclusion of any " cliff edge effect " leading to an early release of a non-admissible source term.

Concerning the fission product retention in containment there are significant mechanisms mitigating the release to the environment, including chemical reactions with water and

surfaces . There is little evidence of accident management measures being introduced to enhance this natural retention capability.

Appropriate preventive and mitigative countermeasures for the above phenomena are considered:

- Controlled RCS depressurisation,
- improved hydrogen concentration control,
- containment venting[10],
- devices to limit corium-concrete interaction,
- provisions for corium cooling in the containment,
- development of symptom-based procedures.

In the light of the above considerations, R&D seems to be necessary in the following areas:

- Accurate information on phenomena related to core-concrete interaction (effects of different outpouring and spreading conditions, timing of water addition, debris size, effect of crusts, size of spreading area);
- Validation of models describing containment leak-tightness and failure modes;
- Reduction of uncertainties in calculated hydrogen generation;
- Reduction of uncertainties regarding in-vessel steam explosions;
- Implementation of natural aerosol retention capabilities of water and surfaces into accident management measures.
- Demonstration of the reliability of novel passive features.

[10] *In fact, referring the TSO, the use of a filtered venting system is not desirable, as this is considered not to be in line with the general goal of maintaining the primary containment as leak tight as possible to meet the radiological safety objectives. (see also section 3.4.D.1)*

3.4 KEY ISSUE E - SEVERE ACCIDENTS

3.4.A - State of knowledge

After the TMI accident, the international severe accident research programmes have been mainly aimed at reducing the remaining uncertainties on key phenomena, at identifying plant states for which the containment integrity (and operability) could be threatened and, at investigating design improvements and innovative strategies for prevention or mitigation purposes.

Current theoretical research and experimental tests continue to provide the basic knowledge needed by severe accident issues resolution and closure.

TSO analysis tackled with PWR reactors but the identified open issues can, to a large extent, be considered as generic (i.e. applicable to almost all the future concept) :

- Molten fuel - coolant interaction (covering both violent (steam explosion)and mild interactions) ;
- In -vessel debris coolability and retention (e. g. through RPV external cooling) ;
- Ex-vessel debris coolability and retention (e. g. through melt spreading over a concrete base mat (MCCI) or over a refractory/sacrificial substrate and quenching ; through an ex-vessel core catcher device, etc.) ;
- Hydrogen risk exclusion through H_2 concentration control (exclusion of any possible global detonation and mitigation of mild burning processes) ;
- Fission product behaviour (more demanding retention capability inside the containment is actually required).

3.4.B - Safety approach (see also section 3.3.A.2)

For future NPP designs, the main safety objective is to significantly reduce Core Melt Frequency (CMF) and the potential release of radioactive materials so that the risk will be as low as reasonably achievable (ALARA).

Utilities and safety authorities agreed that, to meet this objective, severe accident situations which would lead to large early releases have to be ”practically eliminated” that is, when they cannot considered as physically impossible, design provisions have to be taken to design them out. Other severe accidents (e.g. low pressure core melt) have to be ”dealt with”, so that the associated maximum conceivable release would necessitate only very limited protective measures in plant neighbouring area and in time. PSA approach (Level 1 and Level 2) is intended to be used extensively to verify the compliance of plant design with the probabilistic targets.

The designers proposals show that, for all the innovative NPP designs and despite some differences in the approaches, accidents beyond the ”classical” deterministic design basis have effectively been considered.

3.4.C - Development of a common approach for future R&D

It is considered that a common safety approach for future NPP is essential to motivate a coherent R&D effort. The consensus could be achieved integrating the following recommendations :

- For future designs, accidents beyond the ”classical” deterministic design basis have to be considered at an early stage of the design to obtain a significant reduction of CMF. Accident situations which would lead to large early releases have to be “ practically eliminated ” and protective measures are required, for the others. This means that for the future concepts, provisions (when applicable) have to be implemented for :

- The mitigation of Low Pressure Core Melt & Vessel Melt-through
- The practical elimination of events that could lead to large early release through early containment failure ;
- the Practical Elimination of Core Melt with Containment Bypass
- the Practical Elimination of High Pressure Core Melt
- the Practical Elimination of Core Melt in shut down states with open containment.

For all these items TSO identified, for future PWR, points of consensus and specific unresolved issues that can be used to motivate complementary R&D effort. Once more the majority of these issues are applicable to the future concepts. This is why they are succinctly recalled in section 3.4.D

- The accident scenarios to be considered for these demonstrations should be all those that can be judged as physically plausible. The process of selection of these scenarios should be based primarily on deterministic analyses, supported, where needed, by probabilistic considerations, and engineering judgement.
- The accident sequences should be considered as “ practically eliminated ” if sufficient preventive design and operation provisions are taken. Nevertheless it is recognised that there is a need to develop more detailed guidance to clearly establish when sufficient design and operation provisions have been taken to practically eliminate an accident sequence.
- Evaluation of severe accidents should be performed using a “ best-estimate ” approach together with a quantification of the uncertainties to determine, for representative scenarios, a spectrum of the possible outcomes.
- Systems and components provided only for severe accidents, should not require the same conservative analysis and requirements that are necessary for those developed to cope with ”classical” design basis accidents; nevertheless, their performance should be evaluated and documented along with suitable testing strategies and possible failure modes. There should be a high confidence that necessary equipment will survive severe accident conditions for the period that it is needed to perform its intended function.
- Good design practices that have proven positive effects on severe accident evolution (mitigation or exclusion of phenomena) should be always given due consideration for any new design.

3.4.D - Point of consensus and unresolved issues

3.4.D.1 The mitigation of Low Pressure Core Melt & Vessel Melt-through

Low pressure sequences must be dealt with at the design stage, with due consideration given to the impact of vessel failure on containment integrity and on the adequacy of the containment design for ex-vessel core loads. To meet this goal, the containment should be designed to include: (i) in-vessel and/or ex-vessel cooling, to prevent, as far as possible, vessel melt-through; (ii) protective systems to mitigate the consequences of vessel failure and, (iii) inherent safety features such as the basemat surface area and containment free volume exceeding the critical levels.

A general consensus has been achieved, between TSO, on the following points:

- future plants should attempt to avoid vessel failure ;
- where applicable ex-vessel cooling to prevent vessel failure is a viable accident management option, but its application and the degree of confidence that the debris would be retained in-vessel are plant specific ;
- mitigation by enhanced containment design should be encouraged ;
- to manage the Hydrogen, permanent inerting of the containment is not recommended, as this would deny free access to the containment;
- sufficient conventional and specific new instruments should be provided to overcome shortcomings in the information available to manage a severe accident ;

Considerable work is still on-going and further appropriate R&D remains a necessity on the following unresolved issues:

- core melt retention, coolability and melt segregation are still open issues; evaluation of results from on-going experimental programmes should contribute to the improved understanding and substantiating of possible design solutions ;
- none of the core catcher or melt spreading concepts has so far been implemented or verified;
- the use of a filtered venting system is not desirable, as this is considered not to be in line with the general goal of maintaining the primary containment as leak tight as possible to meet the radiological safety objectives ; if a vent system is envisaged, it should be considered as the last resort in the defence-in-depth strategy, with due consideration given to the system reliability and to the potential radiological releases in case of maloperation or leakages of the system.

3.4.D.2 The practical elimination of events that could lead to large early release through early containment failure

Practical elimination of hypothetical severe accident sequences which could lead to large early releases means that sufficient design and operation provisions have been taken so that these sequences can be considered as extremely unlikely with a high degree of confidence. The demonstration would be provided through deterministic and / or probabilistic means.

For LWR, three hazards are explicitly identified and discussed below : the hydrogen detonation, the steam explosion and the high pressure core melt

Hydrogen

Uncertainties still exist concerning the production of hydrogen during severe accident sequences. These uncertainties should be taken into account for the design and layout of the hydrogen mitigation means and the containment design. The advantages and drawbacks of the different mitigation means are still under discussion and continuation of the R&D effort in this area should be encouraged.

In order to eliminate the risks of detonation, the efficiency of the mitigation means has to be such that with a hydrogen production corresponding at least to 100 % fuel clad metal-water reaction coupled with an appropriate kinetics of release, the local concentration of hydrogen in the containment should be lower than 10% (per volume).

It must be verified in addition, that once the criteria of non occurrence of detonation are satisfied, a global deflagration of a total amount of hydrogen corresponding to these criteria does not endanger the containment integrity. Design provisions to prevent, as far as achievable, the possibilities of local high level hydrogen accumulation should be encouraged.

The leaktightness of the containment in the most representative accident sequences should be ensured with sufficient margins to take into account severe dynamic phenomena like a fast local deflagration.

Steam explosion

State of the art indicates that the likelihood of in-vessel steam explosion threatening the containment integrity is very low. Nevertheless, due to large uncertainties and the lack of knowledge on the understanding of the mechanisms of steam explosions, complementary research in this area seems necessary.

The pressurisation of the cavity due to a ex-vessel steam explosion should be minimised by providing enough adequate design options. Moreover, the structures should be designed to accommodate the dynamic loads of energetic steam explosion and to avoid excessive motions of the components which can ultimately cause failure of containment penetrations.

High Pressure Core Melt

During high pressure core melt situations the principal concern is high pressure melt ejection at vessel failure. Such an event would pose a potential early threat to containment integrity, due to direct containment heating (DCH).

The overall safety approach of the GPR/RSK proposal is to reinforce the ”defence-in-depth” by diverse secondary side safety systems and if necessary by primary feed and bleed systems. It must be a design objective to transfer high pressure core melt sequences to low pressure sequences (in the range 15 - 20 bar, at vessel rupture) with high reliability.

For EURD the measures to prevent high-pressure core melt are basically threefold: highly reliable secondary side heat removal including feed-and-bleed operation, primary feed-and-bleed and finally direct depressurisation of the primary circuit.

The design provisions should include: (i) diverse secondary side heat removal systems to depressurise the primary in a controlled and reliable way; (ii) sufficient primary feed and bleed capability in the event that secondary systems are lost and (iii) adequately sized pressuriser

relief devices or a specific dedicated system for direct primary depressurisation (last line of defence).

General consensus have been reached by TSO on the following specific points:

i. even if the RPV should fail and HPME occurs, the probability of containment failure by DCH is acceptably low ; DCH is design specific and is substantially limited by the containment compartmentalisation;

ii. primary depressurisation can be correctly demanded by operators, using observable plant indicators; it is recognised that a manually actuated, ac-independent system provides a simple and reliable design for the station blackout sequence, while reducing the potential for inadvertent operation ;

iii. the discharge capacity and the reliability of the depressurisation system would have to be demonstrated for severe accident conditions.

The timing of direct primary depressurisation and its impact on accident progression is still an open issue.

The TSOs agree that there is a substantial defence-in-depth approach to the practical elimination of high pressure core melt ; the relatively few unresolved issues are:

i. how to demonstrate ”practical elimination”?

ii. should the primary depressurisation system be safety classified and should the requirements for the system be based on probabilistic considerations alone or are other additional considerations needed?

iii. the timing of direct primary depressurisation and its impact on accident progression is still an open issue, so the state of knowledge should be improved in this area.

3.4.D.3 Practical Elimination of Core Melt with Containment Bypass

These severe accident sequences cannot be considered as physically impossible. Sufficient design and operation provisions have to be taken so that they can be considered as extremely unlikely with a high degree of confidence. As already stressed, generally agreed probabilistic criteria are not existing to define “ practical elimination ” in a more quantitative manner.

Reducing the number of containment penetrations and reinforcing the design pressure of the penetrating piping connected to the primary circuit seems to be one of the very effective means to lower the probability of containment bypass sequences.

Passive systems installed inside the containment may have advantages to reduce the number of containment penetrations. However the disadvantages of passive systems have also to be considered.

3.4.D.4 Practical Elimination of Core Melt in shut down sates with open containment.

The issue arose from PSA results. They notably show that the core melt frequency during shutdown is directly related to plant configuration during shutdown.

General recommendation (i.e. applicable to all future concepts) are specified by TSO in the form of main technical safety options ; they concern :

- The operating conditions during shutdown states which have to be specified ;
- The residual heat removal function which must be ensured with a high reliability ;
- Ractivity accidents have to be "*practically eliminated*" ;
- Internal hazards : Special attention has to be paid on the fire and internal flooding possibilities in shutdown states, taking into account the maintenance activities ;
- Containment Integrity : an initially open containment should be reliably closed within acceptable delays.

3.5 KEY ISSUE F-Ageing

Surprisingly, there is relatively little debate in the documents used as a basis for this report on ageing effects, probably, because, in the eyes of the licensing authorities, there is sufficient margin built-in through the monitoring, inspection and surveillance programmes already implemented to early detect any serious, safety relevant material deterioration.

With regard to existing plants, weight is put on the importance of periodic inspection programmes and of the feedback of operating experience, both nationally and internationally. It is pointed out, that the information gleaned by these programmes should be reflected in the reliability data used in PSA studies. The most concrete statements are found in the EC-document, where it is stated, that the evaluation and the management of physical ageing and the resulting degradation of plant components, systems and structures need the implementation of data collection and record keeping systems in order to provide relevant information for the following activities:

- Predictions of future performance (i.e. the functional capability and remaining service life) of components which are required for safe and reliable plant operation.
- Decisions on the type and timing of preventive maintenance actions.
- Identification and evaluation of degradation, failures and malfunctions of components (root cause analysis).
- Optimisation of operating conditions and practices
- Identification of new emerging ageing effects

Where ageing is detected, corrective actions should be taken in order to maintain the level of safety defined in the plant's safety case. If quick repair or replacement can not be done, increasing the defence in depth and mitigating the possible consequences may provide temporary solutions. In particular, procedures can be used to reverse the effects of ageing. For plant life extensions, analysis must show that the plant will continue to operate within design basis.

With regard to future plants, the current practice is implicitly continued, while some more stringent criteria are applied. In the IPSN/GRS document, for instance, it is stated that the designer should propose provisions to detect, at least locally, smaller leak rates, depending on the specific design of the plants. Further, that he has to assume that any pipe connected to a main coolant line might separate from its connecting nozzle and to apply 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. Finally that he should implement provisions which would allow access for a 100% volumetric inspection of all the welds of the line and of the parts of the pipes with the highest fatigue usage factors.

From the above, one can deduce that technological developments to respond to these trends should on the one hand focus on improved monitoring, surveillance and NDT-techniques, in-service inspection, and procedures for risk- and safety-based maintenance and repair. On the other hand, innovative technologies for components life prediction should be introduced. This implies, for instance, that R&D is necessary to replace continuum fracture mechanics

modelling by models based on a better understanding of the degradation processes, in particular the interaction of corrosion, fatigue and irradiation.

In the OECD document it is finally stated, that beyond the physical ageing of components and structures, attention should also be paid to the

- ageing of analytical techniques and documentation,
- ageing of rules and standards and
- ageing of technology.

However, these aspects will not be dealt with in detail here. It is only worthwhile noting that these issues may necessitate innovative approaches in the domain of ”soft sciences” making extensive use of novel communication and information techniques.

3.6 KEY ISSUE G -DECOMMISSIONING AND WASTE/FUEL DISPOSAL

During the design phase of the currently operating plants little attention has been paid to technological issues related to their decommissioning both at the design stage and at the operation stage. This was justified because at that time the costs associated with the decommissioning were considered relatively low; i.e. in most cases rather easy and relatively inexpensive actions would have reduced costs, occupational doses and amount of generated wastes. .

Safety Authorities has recognized only recently the importance of addressing decommissioning since the design and construction stage. Utility requirements (in particular EURD) have also addressed this issue for future plants, concluding that most of the requirements for decommissioning would also improve plant operations and maintenance, having therefore a very high cost-benefit ratio. Examples are improved room accessibility, elimination of Cobalt based , improved shielding of highly radioactive components, improvement of clean-up systems to reduce the coolant activity, etc.

Safety Authorities consolidation of current decommissioning requirements would also improve the standardization of decommissioning techniques. This is of particular importance when, in cases where a SAFESTOR (maintaining the plant in safe condition for some decades before dismantling it) approach is adopted, there is the need to anticipate techniques and costs several decades in advance. Attention is also needed to provide the necessary information, in the proper form and quantity, to people responsible of final dismantling at that time; technologies to maintain adequate level of information for decades is currently an issue.

Development of proper decontamination techniques is another important area, where technical improvements may be of relevant importance.

Waste treatment and waste volume reduction with the use of high temperature incinerators and furnaces is an area where a potential for reduction of the environmental impacts and costs is a possible goal. An international consensus on the final form of different types of wastes could also improve the likelihood that wastes will be available for different disposal sites in the future, at the end of the dismantling process.

4. CONCLUSIONS

Using as reference a set of internationally recognised documents, the paper give an overview of the currently underway evolution of regulatory and licensing processes. The short term evolution, as envisaged by the regulatory bodies themselves is shortly described, and the mid-term evolution is documented where clearly discernible.

On this basis, necessary R&D topics are tentatively identified. This R&D reflects not only the need to get information on unknown issues, but also the necessity to reduce uncertainties and to achieve international harmonisation.

The analysis shows that the most general trend are:

- a more realistic approach to the ”classical” accidents, once the experimental evidence has been factored in ;
- the exploration of events always more complex and less probable, in order to leave less to the unknown ;
- a tendency to reduce the risks to the population.

The report is structured through a series of “ key issue ” used as guidelines to identify the fields and subjects that motivate complementary R&D effort.

Concerning the **Radiological impact assessment**, trends for the future generate the R&D needs : the improvement of the level of harmonization between different countries ; the reduction of the impact on the population in order to simplify the Emergency Planning and possibly to completely eliminate the need of public evacuation

For the **Plants architecture**, the objective of a significant improvement in safety at the design stage, implies to reinforce the defence-in-depth principle : i.e. reduce the frequency of PIE ; improve the reliability of safety grade systems ; implement design measures to cope with multiple failures and severe accidents

The R&D programme on **Innovative passive systems** should be defined integrating the following items which request specific efforts : practical implementation of the principle of defence-in-depth, requirements of redundancy, diversification, single failure criteria, common cause failure ; new accident scenarios such as inadvertent operation or interactions with other systems ; definition of failure criteria for all accident conditions ; protection against internal and external events ; limitations of analytical safety demonstration, need of experimental safety demonstration, need of prototype ; effects of ageing, e.g. surface oxidation, clogging, radiation ; diagnosis of state ; inspectability, recurrent testing, in-service testing close to operational mode ; sensitivity against human errors ; interconnections between passive systems must be investigated with respect to possible disadvantageous interactions ; methodologies for the assessment of the reliability of passive systems ; research for passive systems able to achieve safety functions other than the DHR.

Referring the **Instrumentation and Control**, nine specific dependability issues have been identified by TSO : Hardware/software fault-tolerant architectures ; Multi-processing and Communications ; Software reliability targets and assessment ; Defence against common

mode failures ; Fault Tolerance Characteristics ; Documentation ; Formal specification and verification methods ; Use of automated development tools.

Some open issues are identified for the " **Safety approach - methodology** ": a clear identification of unambiguous cross-reference DBCs versus acceptance criteria should be established ; the development of adequate guidance to clearly establish when "sufficient design and operation provisions" have been taken to practically eliminate a severe accident sequence ; the definition of the rules for the "best-estimate" approach applicable to the evaluation of severe accidents and the definition of the the rules for the quantification of the uncertainties to determine, for representative scenarios, a spectrum of the possible outcomes.

The following possible fields of necessary R&D activities on **PSA** has been identified : methods for obtaining reliability data for new components and passive systems ; detailed analysis of operating experience ; definition of a coherent and harmonized methodology and acceptance criteria for the use of PSA, especially for common mode failures ; development of a common approach for PSA application during the licensing process ; sensibility studies to deal with uncertainties associated to the treatment of common cause failures ; validated data for the treatment of human interventions.

Potentially necessary R&D for **PIE-Identification** can be envisaged in the following fields : harmonisation in the definition and the application of the single failure criterion and in the distinction between active and passive failures ; extension of the grace period ; treatment of uncertainties in analyses using best estimate models and codes and more realistic hypotheses and input parameters ; analyses of existing practices (as applied by regulators for operating plants or by vendors) to evaluate whether there is a need for further harmonisation ; analyses to show compliance with European criteria for radiological consequences of nuclear accidents.

To help the **Design Extension Conditions identification**, R&D seems necessary in the following areas: accurate information on phenomena related to core-concrete interaction ; validation of models describing containment leak-tightness and failure modes ; reduction of uncertainties in calculated hydrogen generation ; reduction of uncertainties regarding in-vessel steam explosions ; implementation of natural aerosol retention capabilities of water and surfaces into accident management measures ; demonstration of the reliability of novel passive features.

Concerning more specifically the **physics of Severe accidents** unresolved issues generate R&D needs to meet the following objectives :

- The mitigation of Low Pressure Core Melt & Vessel Melt-through : i.e. core melt retention, coolability and melt segregation are still open issues ; evaluation of results from on-going experimental programmes should contribute to the improved understanding and substantiating of possible design solutions ; none of the core catcher or melt spreading concepts has so far been implemented or verified ; the use of a filtered venting system is not desirable ; if a vent system is envisaged, due consideration shall be given to the system reliability and to the potential radiological releases in case of misoperation or leakage of the system.

- The practical elimination of events that could lead to large early release through early containment failure. Three hazards are explicitly identified and discussed : the hydrogen detonation, the steam explosion and the high pressure core melt.
- The Practical Elimination of Core Melt with Containment Bypass.
- The Practical Elimination of Core Melt in shut down sates with open containment.

Within the frame of **Ageing** relevant information are expected on the following activities : predictions of future performance (i.e. the functional capability and remaining service life) of components which are required for safe and reliable plant operation ; decisions on the type and timing of preventive maintenance actions ; identification and evaluation of degradation, failures and malfunctions of components ; optimisation of operating conditions and practices ; identification of new emerging ageing effects. 100% volumetric inspection of all the welds of the line and of the parts of the pipes with the highest fatigue usage factors is another essential objective. Attention should also be paid to the : ageing of analytical techniques and documentation ; ageing of rules and standards and ageing of technology.

For **Decommissioning and waste /fuel disposal** in most cases rather easy and relatively inexpensive actions would reduce costs, occupational doses and amount of generated wastes. Technologies to maintain adequate level of information for decades is currently an issue. Development of proper decontamination techniques is another important area. Waste treatment and waste volume reduction where a potential for reduction of the environmental impacts and costs is a possible goal. An international consensus on the final form of different types of wastes could also improve the likelihood that wastes will be available for different disposal sites in the future, at the end of the dismantling process.