C. R. Physique 3 (2002) 1059–1065

Physique appliquée/*Applied physics*

DOSSIER

DU COMBUSTIBLE NUCLÉAIRE AUX DÉCHETS : RECHERCHES ACTUELLES

FROM NUCLEAR FUELS TO WASTE: CURRENT RESEARCH

International views on nuclear safety

Adolf Birkhofer

Technical University Munich, Chair for Reactor Dynamics and Reactor Safety, Walther-Meissner-Strasse 2, 85748 Garching, Germany

Received 3 May 2002; accepted 6 May 2002

Note presented by Édouard Brézin.

Abstract Safety has always been an important objective in nuclear technology. Starting with a set of sound physical principles and prudent design approaches, safety concepts have gradually been refined and cover now a wide range of provisions related to design, quality and operation. Research, the evaluation of operating experiences and probabilistic risk assessments constitute an essential basis and international co-operation plays a significant role in that context. Concerning future developments a major objective for new reactor concepts, such as the EPR, is to practically exclude a severe core damage accident with large scale consequences outside the plant. ***To cite this article: A. Birkhofer, C. R. Physique 3 (2002) 1059–1065.***

nuclear safety / defence-in-depth / operational experience / severe accidents / nuclear safety research / probabilistic risk analysis / future developments

Un regard international sur la sécurité nucléaire

Résumé La sécurité a toujours été un objectif important dans la technologie nucléaire. Partant d'un jeu de principes physiques solides et de conceptions prudentes, les concepts de sécurité ont graduellement été perfectionnés et couvrent à présent un large domaine de prestations relatives au *design*, à la qualité et au fonctionnement. La recherche, le retour d'expérience et les évaluations probabilistes des risques en constituent la base essentielle, tandis que la coopération internationale joue un rôle majeur dans ce contexte. Concernant les futurs développements, un objectif majeur pour les nouveaux concepts de réacteurs, comme l'EPR, consiste à exclure pratiquement tout endommagement accidentel sévère du cœur, avec des conséquences à grande échelle à l'extérieur de la centrale. ***Pour citer cet article : A. Birkhofer, C. R. Physique 3 (2002) 1059–1065.***

sécurité nucléaire / endommagement sévère / recherche nucléaire / futurs développements

E-mail address: birkhofer@iisar.de (A. Birkhofer).

S1631-0705(02)01356-7/FLA

1. Introduction

Precaution and protection have always been two principles guiding the safety development of nuclear reactors. They were already applied when the first chain reaction took place. On 2 December 1942 when the first atomic reactor was brought to criticality, Enrico Fermi had made safety to an important part of the experiment. In addition to a shutoff rod, other emergency procedures for shutting down the pile were prepared in advance. Fermi also considered the safety aspects of reactor operation. Shortly before the reactor was expected to reach criticality, Fermi noted the mounting tension of the crew. To make sure that the operation was carried out in a calm and considered manner, he directed that the experiment be shut down and that all adjourn for lunch.

2. Safety concept

The basic safety concepts for light water reactors – the worldwide predominant design among nuclear power reactors – are going back to solutions developed together with that technology about five decades ago. Already at that time it was well known that the potential for nuclear power excursions and the radioactive fission products in the reactor constituted significant risks.

Therefore it was necessary to develop a deep understanding of the basic physical phenomena and of possible failure mechanisms in order to prevent failures and their propagation into accidents. Moreover, design had to use significant safety margins to compensate partially incomplete knowledge, and methods had to be developed to avert consequences of failures and accidents if their prevention would not be fully successful.

The implementation of these features within multiple levels of safety provisions has become a fundamental safety concept termed ‘defence in depth’ (Fig. 1).

Defence in depth means a succession of physical barriers to contain the radioactive materials and a hierarchical deployment of different echelons of equipment and procedures in order to protect these barriers during normal operation, anticipated events, and accidents in the facility. At each echelon, priority is given to those measures which prevent the plant status from proceeding to the next echelon. Those measures are supplemented by mitigation as far as is required to assure that even an accidental release would remain sufficiently below intolerable levels.

The concept applied to most currently operating plants initially included 3 levels:

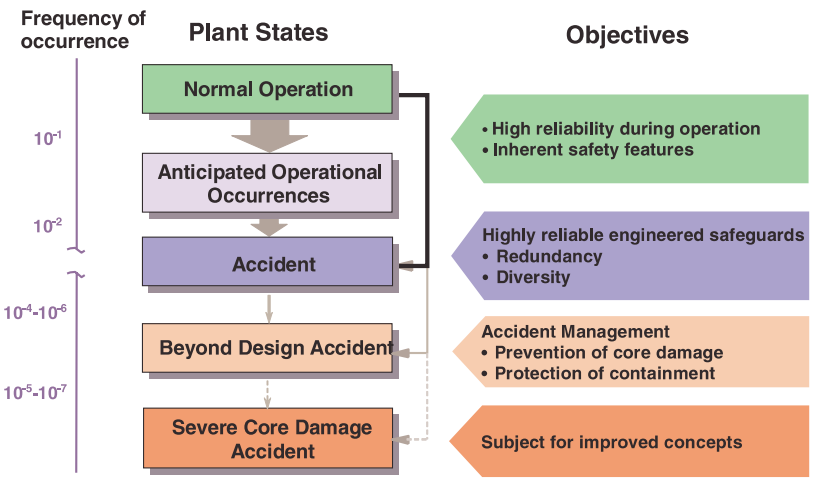

Figure 1.
Defence-in-depth.

- a combination of conservative design, providing margins between the foreseen operating conditions and the failure conditions of equipment, surveillance activities and operating rules that strengthen each of the successive barriers to prevent or to mitigate the release of radioactive materials;
- control of operation, including response to abnormal operation or to any indication of system failure by protective and limiting systems to prevent the evolution of such occurrences into accidents;
- engineered safety features to control incidents and accidents in order to prevent them from progressing into plant conditions where severe fuel damage could occur and to mitigate the consequences of such events to levels considered acceptable in relation with their estimated probability.

As a result of this concept, severe accidents are of a very low probability of occurrence. Nevertheless, there cannot be an absolute guarantee that severe accidents will not occur. Therefore, accident management was introduced as a further level of defence aimed at the control of the course of such accidents and at the mitigation of their consequences.

Accident management includes all actions which can be taken in a nuclear power plant in order to detect the emergence of a degraded state, to prevent its progression to a severe accident, to control and to terminate such an accident or at least to mitigate its consequences. Actions focus on the very vital safety objectives such as shut-down of the plant, cooling of the core, integrity of the containment and limitation of radioactive releases. Safety and operational systems and external equipment may be used for that purpose in a flexible way, even outside their design specification.

Several specific concepts have been developed and are already implemented in a number of plants in several countries. In French plants for instance, special procedures are implemented for secondary and primary bleed and feed in order to provide core cooling even in the extreme situation where all equipment provided in the design has failed. If such measures did not succeed in the event of a beyond-design accident, accident management would focus on the protection of the last barrier, the containment, and on the long-term control of the plant.

In Europe, the approach to the mitigation of severe accident consequences had to consider relatively high population densities. Thus the integrity of the containment in the event of a pressure increase after a core melt is being considered as a matter of prime importance. Accident management measures are considered to preserve the containment function, even if that seems not necessary according to a mere probabilistic assessment. Some measures, such as filtered containment venting, have already been specified and implemented in most European countries. Other measures are still under development.

3. Safety research

Research has been an essential prerequisite for the development of the basic safety features and for their gradual optimization within the concept of defence-in-depth. Knowledge on basic phenomena had to be acquired. Possible safety-relevant problems needed to be anticipated. Phenomena relevant for potential accidents and for the design of engineered safeguards are never observed in a real plant so that knowledge from experiments is required. Accidents which are prevented and eventually controlled by the safety systems need to be simulated by computer models.

Examples for safety relevant research are:

- experiments regarding the basic features of the nuclear chain reaction leading to an understanding of reliable means by which good reactor design can avoid power excursions with a potential damage to the core;
- experiments and analytical investigations into the physical phenomena governing the course of accidents with loss of coolant from the reactor system and the effectiveness of emergency core cooling systems (ECCS);
- research on the properties of materials used for fuel elements and reactor vessel and other large components;
- investigations into the human behaviour and the suitability of man–machine interfaces;

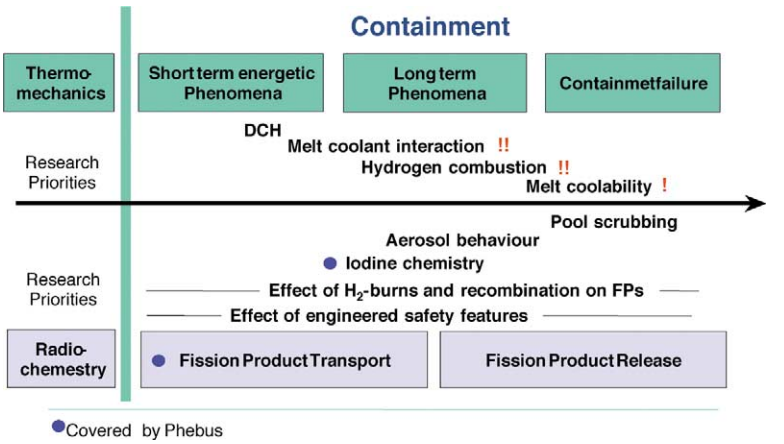

Figure 2. Progression of a severe accident and key phenomena – containment.

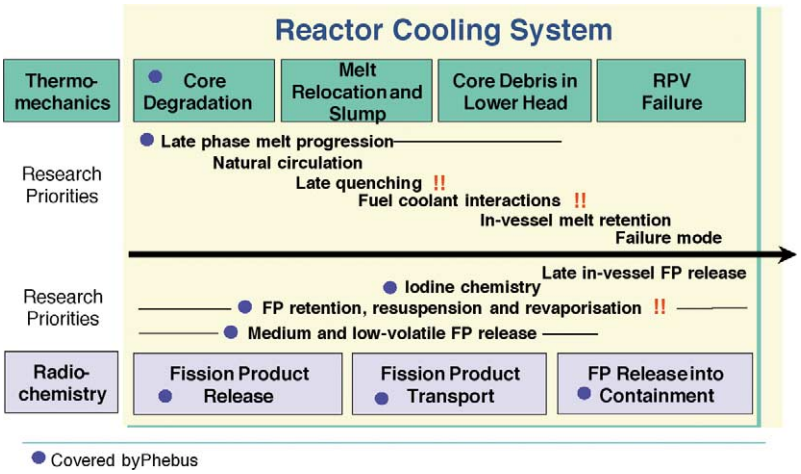

Figure 3. Progression of a severe accident and key phenomena – the reactor cooling system.

- investigations into the risk of severe accidents and into new possibilities to further reducing that risk;
- development/improvement of computer codes capable to simulate transients, accidents and specific phenomena, as realistically as possible, including the qualification of such codes against experiments.

Further intensive experimental and analytical research has been made on the progression of severe accidents (Figs. 2 and 3): If sufficient cooling to the reactor core is no longer possible, fuel temperature will increase strongly, eventually resulting in partial or complete melting of the core. This can affect the integrity of the reactor pressure vessel, leading to a release of core debris and other radioactive material (i.e. iodine) into the containment. With this the complexity of phenomena increases considerably and the linkage between them is getting more and more complex. While for anticipated disturbances and design base accidents plant simulation can essentially be based on neutron physics and thermal-hydraulic phenomena, severe accidents require further knowledge about thermo mechanics, physico-chemical processes, aerosol physics, radio-chemistry, steam explosion and hydrogen generation and burn or detonations. Research on this wide variety of phenomena is necessary and is being performed in international cooperation. It is concentrated on the main uncertainties which have major impact on the consequences of accident progression and the possible radioactive pollution of the environment (source term). Key phenomena (Figs. 2 and 3, marked by !!) are the hydrogen generation during late quenching and the energy release under high pressure, which could both lead to a containment failure due to hydrogen detonation and fuel coolant interaction. For containment

by-pass sequences, the source term is dominated by fission product release, transport and retention and in particular by the iodine behaviour.

The most important international project to contribute to the solution of open issues in this context is the Phebus Fission Product (short Phebus FP) project, conducted at the Phebus experimental facility in France. The program examines the release of fission products after a thermal failure of the fuel elements and their subsequent transport and retention in the primary circuit and the containment. An overview over numerous phenomena covered by Phebus provide Figs. 2 and 3 (marked by •). Important aspects with respect to the use of the results are the reduction of uncertainties in the prediction of the source term and the verification existing computer codes [1].

4. Refinements and further developments

Operating experience shows that the concept of defence-in-depth was highly successful where it has been applied according to these principles. Nevertheless, the operating experience also provides important information about potential safety challenges and possibilities for improvements. Again, failures and phenomena with a potential to impair several levels of defence simultaneously are significant: reactivity incidents, human errors, internal and external hazards, common cause effects with a potential to result in a simultaneous loss of several redundancies, accidents during situations with a reduced number of effective barriers (e.g. low power states), and loss of coolant accidents with a containment bypass.

Since some time ago there has been a continuous process of learning from those experiments. It has resulted in a steady evolution of the defence-in-depth approach. Two general developments are particularly interesting:

- the measures taken at the second level of defence have been extended in many countries and rendered more independent from other levels by extending and systematizing the automation of the control of anticipated operational occurrences;
- accident management was developed to be a new level of defence aimed at the systematical use of safety margins for the prevention of core damage or mitigation of consequences in the event of an accident exceeding the design basis.

Concerning future developments, an important part of this strategy is improving accident prevention. Technical possibilities are:

- a simplification and functional separation of the safety systems;
- an improved physical and divisional separation of systems and the implementation of diverse systems for safety functions to decrease the vulnerability with regard to common mode failures;
- an increase of grace periods for operator actions by designing components, e.g. pressurizer and steam generators, with larger water inventories to smoothen transients;
- a reduction of the sensitivity to human errors by an optimized man-machine interface using the possibilities of digital instrumentation and control systems and status-oriented information supplied by modern operator information systems.

However, strengthening defence-in-depth for future plants should also have a strong mitigative component and the confinement function plays a key role in that regard.

Such optimization can be best achieved with new designs where is much freedom for changes combining sensible new features with efficient use of resources and simplification of plant technology where appropriate. The joint French–German development of a European Pressurized Water Reactor (EPR) is a major project with that objective:

- a considerable proportion of the EPR development deals with a further strengthening of accident prevention through optimization of defence-in-depth. Particular objectives are the improvement of plant behaviour during transients, particularly by increasing thermal inertia and the grace periods for interventions by the control room personnel, the reduction of the possibility of common cause failures,

a further improvement of the man–machine interface, the simplification of the systems configuration, and the use of advanced information technology;
- regarding severe accidents, the EPR aims at preventing large, early releases of radioactive material requiring massive measures outside the confined grounds of the plant. As far as accident scenarios can not be regarded as physically impossible, they are considered in the design with the objective to exclude them or to control them according to appropriate criteria.

Such objectives are demanding regarding the technical realization and the scientific methods needed for their verification. A successful solution requires further efforts in research and development, especially with regard to the phenomena occurring during core melt scenarios and concerning the integrity of the confinement system.

5. Probabilistic risk analysis

The safety concept for nuclear power plants is based on a deterministic approach, which does not explicitly consider probabilities. It renders severe accidents very unlikely but cannot completely exclude their possibility. The following questions have been posed in that regard:
- what is the probability of a severe accident with core damage after a complete loss of vital safety functions?
- what could be the consequences of such an event?
- what would be the course of a severe accident and would it be possible to control it or to mitigate its consequences?

Due to the high quality of safety precautions there is almost no direct experience about severe accidents with light water reactors. On the contrary, most incidents are far away from any direct safety significance. In order to use the operating experience for systematic safety assessments, this gap to safety significance has to be bridged by analytical extrapolation. Probabilistic risk analysis (PRA) constitutes a systematic approach to perform that task.

The first large applications of the probabilistic methodology to nuclear safety were the risk analyses performed in the seventies in the USA, Sweden, France and the FRG. In particular the US analysis, Wash-1400, and the German investigation, the phase A of the German risk study, were aimed at the calculation of individual and population risks from the operation of nuclear power plants and at the comparison with other natural and industrial risks. On the whole, the risk from the operation of nuclear power plants was found to be rather small compared to other non-nuclear risks.

These analyses also provided important new insights into strengths and weaknesses of the design and the operation of the plants under investigation. WASH-1400 and the German study as well as the French analyses, for instance, demonstrated the important role of small breaks. As an immediate consequence of these findings several important technical improvements have been made.

By now, more than 200 such assessments have been conducted. Their results show that expected core damage frequencies are currently between 10^{-4} and 10^{-7} per reactor-year. The predicted frequency of large radioactive release is lower by about one order of magnitude. Fig. 4 shows the results of several PRA studies for different LWR plants in the USA (red) and Germany (green) in comparison to the direct experience in Harrisburg.

It should be recognised, however, that the findings and the accuracy of a PRA depend on many conditions including subjective elements in the various steps of the analysis and on the incorporation of the man–machine interface. For instance PRA should be based on plant specific data from operating experience and on accident analysis with reviewed qualified computer models based on qualified research. However, there are practical limitations. Data from experiements are not always available, and the answers to many questions rely on expert judgment. For instance, expert judgment is often the only way to provide the probability of a specific phenomenon when no statistical evidence is available.

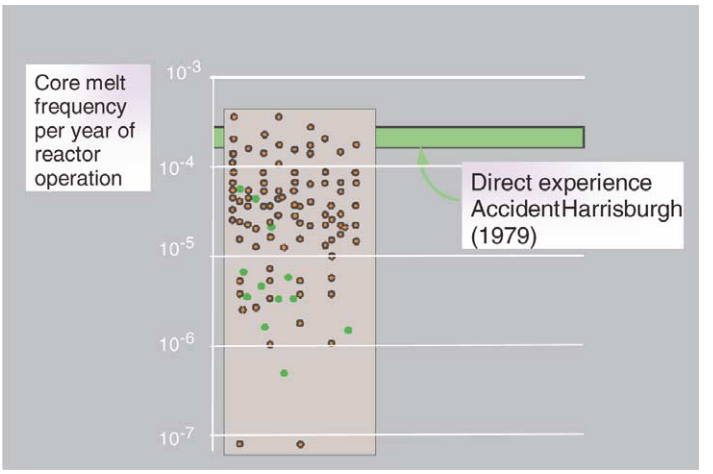

Figure 4. Probabilistic risk analysis.

On the other hand the PRA method permits that uncertainties are quantified and propagated in a transparent way through the steps of an analysis, leading to probability distributions of the calculated results. According to the PRAs of current reactor designs, the uncertainties (90% confidence interval) of core damage probability predictions cover a range of roughly one order of magnitude. For the probabilities of radioactive releases the uncertainties are much larger, because of the difficulties in modelling containment loads and containment failure mechanisms associated with severe accidents.

6. Conclusions

Nuclear safety is not only based on plant design; it is rather the result of the dynamic interaction of several key elements: Besides the design, which of course is of high importance, the safety of a nuclear power plant depends strongly – similarly to other technologies – on the quality of operational management and appropriate quality assurance measures. Moreover, the evaluation and feedback of operational experience, the results of nuclear safety research and the update of safety standards are important contributors to a continuous improvement of nuclear safety.

References

[1] IPSN, Phebus PF, Final Report FPT-1, 01.12.2000.

Discussion

Question from C. Fairhurst

After the accident of Chernobyl, M. Sakharov suggested the underground location of nuclear power plants. Several studies in USA and in Sweden indicated this was feasible. This has the advantage that direct release of radio nuclides to the atmosphere, and their rapid transport in the air, beyond national boundaries, can be avoided. Has this been considered in recent studies?

Reply from A. Birkhoffer

In the 1980s also in Germany feasibility studies for nuclear ground siting have been performed. The reason was to evaluate possible gains for further strengthening of the containment and then limiting further fission product release after severe accidents with core melt down. The results indicated that, because of unavoidable pathways to the atmosphere, the reduction of the source term was less than one might expect.

It is evident however that additional protection of the containment against external impacts can be achieved.