COMMISSION OF THE EUROPEAN COMMUNITIES

COM (88) 788 final

Brussels, 24 February 1989

COMMUNICATION FROM THE COMMISSION

ASSURANCE OF SAFETY OF NUCLEAR POWER PLANTS

Objectives and methods

TABLE OF CONTENTS

1. INTRODUCTION

The technological problems of safety of nuclear installations are treated by the Commission in the frame of the Council Resolution of 22.07.75. In 1987, in its report COM(87)96 (1) the Commission reviewed the implementation of this Resolution after around twelve years.
The work was carried out mainly in the field of nuclear power plants (NPPs), and particularly for those with Light Water Reactors (LWR) (which generate a dominant part of electricity of nuclear origin in the Community) and those with Liquid Metal Fast Breeder Reactors (LMFBR) (for which development and demonstration works are going on in the Community).
The actions undertaken by the Commission in this field aimed mainly at bringing out a consensus between the safety authorities, the power plants designers and constructors and the electricity producers of the member states on the objectives and methods used to assure and evaluate the safety of LWR and LMFBR power plants at the design stage and during their operation.

A first step in this field was the publication in 1981 (2) of a set of fundamental and general safety principles for LWR power plants which can also be applied to LMFBR.
Since that time, the experience acquired in the design and operation of NPPs has increased as well as the understanding of complex physical phenomena as those occurring in accidental situations. Both technological progress and improved understanding allow the constant improvement of plant safety.

The safety of a nuclear plant like the safety of any complex industrial process depends on many factors throughout its existence and, most particularly during its design and operation stages.
The developments recorded in the last few years have allowed to systematize the analysis methods and to progress in the study of accidents of very low probability but whose consequences could be severe. This allows to assess systematically the safety of NPPs by means of proven methods.

Safety evaluation of NPPs was one of the areas identified in the last chapter of the document COM(81)519 as suitable for further developments.
As a follow up, the present document gives a description of safety objectives and methods used in the Community in the two particularly important areas of design and operation for the LWR and the LMFBR nuclear power plants.

---

1) COM(87)96
"Technological Problems of Nuclear Safety"

2) COM(81)519
"Safety Principles for Light Water Reactor Nuclear Power Plants"

2. SAFETY OBJECTIVES AND METHODS FOR THE DESIGN OF NUCLEAR POWER PLANTS

2.1. GENERALITIES

Nuclear safety is "the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of site personnel, the general public and the environment from undue radiation hazards" (as defined in the safety documents of the IAEA).
Consequently the safety of nuclear power plants is based on a fundamental principle of radiation protection and implemented in technological safety principles.
The link between the technological safety principles and the radiological ones has been recently emphasized by INSAG (3) in its report on "Basic Safety Principles for NPPs".

In order to avoid radiation hazard from operating NPPs and generate electricity with minimum risk, the following three safety functions must be fulfilled in all normal and accidental conditions:

- **the nuclear chain reaction must be controlled**
- **the heat from the core must be removed**
- **the radioactive fission products must be confined in the plant**

In view of the magnitude of the **potential risk** from such installations and hence the stringency of the measures to be taken in order to achieve a satisfactory level of safety, designers are prompted to use "methods" adapted to the status of the projects and to the state of knowledge, such methods being inspired by the basic postulation: the more serious are the **consequences** for the public of an accidental event, the lower must be the **probability** of occurrence of such an event.
Hence the two factors on which the "methods" can have an influence are:

- prevention of an accident, or failing that, reduction in the probability of its occurrence;
- limitation of the consequences of an accident that may occur in spite of preventive measures, in other words **mitigation.**

Three "methods" based on the principles set out above and of complementary nature have been thus developed: the deterministic method, the probabilistic method (those two methods usually closely linked),and the systematic use of operating experience to bring out the weak points of the plants and correct them to reduce the risk. It is important to note that these different methods must always take account of an "ALARP" concept (As Low As Reasonably Practicable) to lay down limits to the safety measures, without which the installations would be impossible to construct and operate, from both the technical and the economical points of view.

---

3) INSAG: "International Nuclear Safety Advisory Group" to the IAEA Director General

This ALARP concept is implemented in each Member State, by the safety authority in charge of controlling the NPPs at all stages of their life starting with siting and including design, construction, commissioning and operation.

It should also be added that the awareness of the complexity of the physical phenomena which play a role in nuclear plants has always been the motivation of important theoretical and experimental studies which lead to a better knowledge of the **conservative margins** used for prevention, and of the exact nature of physical and radiological consequences of the accidents taken into account.

Finally, the importance of the **human factor** is to be recognized. Control of the quality of design and construction by formal Quality Assurance procedures is required.

2.2. DETERMINISTIC METHOD

2.2.1. Introduction

This method consists in setting up "a priori" a number of defense lines between reactor core and environment and in applying the **"defense in depth" concept** (as defined in COM(81)519) to verify that they are able to cope with the different normal and accident conditions; it is used primarily at the design stage and necessitates the incorporation of safety margins in the structure design and of conservative factors in the calculation of radiological consequences of accidents.
As far as possible structures are designed and necessary material chosen in such a way that safety margins are inherent in the plant.
This method analyses the **barriers** placed between the fuel and the environment and **lists the accident situations** both of internal and external origin to be taken into account in **the design**. A number of barriers is foreseen in accordance to the ALARP principle.
The **barriers** between reactor fuel and environment are the nuclear fuel cladding, the primary pressure boundary containing the core and the coolant, the reactor containment building. Barriers are also installed in associated buildings where radioactive materials may be handled and/or stored.

Design basis accidents covering different scenarios are selected in order to prove the fulfillment of the fundamental safety functions under different accidental situations. They are chosen in such a way as to have an envelope character for a group of fault conditions of similar characteristics.

The "defense in depth" concept copes with such situations as follows:

- designing, constructing and operating the equipment in such a way as to impart intrinsic strength to the installation;

- equipping the installation with control and protection systems capable of restoring it to its normal operating conditions in all cases of anticipated transients and incidents;

- taking into account, despite the preventive measures referred to in the two preceding points, of accidents that are presumed to be possible and designing safety systems capable of mitigating the consequences of such accidents and returning the plant to safe conditions.

2.2.2. The barriers

A large international consensus exists for the establishment of these barriers and their objectives were already defined in the document COM(81)519.

"**The first barrier** comprises the retaining ability of the fuel matrix and the fuel cladding.
It is essential to ensure the integrity of this barrier; therefore reliable cooling of the core and reactivity control must be provided to limit the fuel and cladding temperature during normal operation, anticipated operational occurrences such as transients and in accident conditions.
In addition, reliable means must be provided to remove residual heat after shut down to preserve the integrity of the fuel elements."

"**The second barrier** is the primary pressure boundary: within this barrier the heat production and the heat exchange take place.
This barrier prevents the escape of any radioactive materials which are present in the cooling fluid. Loss of integrity of this barrier leads to a loss of coolant, which in turn might lead to a failure of the fuel cladding. Provisions are therefore necessary to limit the consequences of the failure of the second barrier."

Due to the importance of this barrier the probability of failure must be kept very low and, as a consequence, material, design, fabrication and construction are to be of highest quality, e.g.:

- made following specific validated codes and subject to an extensive programme of quality assurance;
- allowing in-service inspection and non-destructive testing.

A particular attention is to be given to the steam generators (when applicable) to avoid as far as possible tube failure and tube rupture propagation.

"**The third barrier** is constituted by the containment system. Its main function is to mitigate the consequences of an escape of radioactive materials from the primary circuit and to limit the escape of these materials into the environment."

This barrier being the last between radioactive content of the core and the public is designed to withstand a design basis accident. The behaviour of the containment in case of a more severe accident is presently being studied in the Community.
The particular importance of this barrier has led to the need to verify its resistance not only to internal hazards, but also to external hazards as will be seen in the following paragraphs.

It should be noted that the barrier concept involves not only the "barrier" itself, but also includes procedures and systems which are necessary for the barrier to function satisfactorily. A good example of this is the third barrier which ensures containment: this containment is ensured, not only by the containment building, but also by internal structures as well as ventilation and filtration systems.

2.2.3. The accidental situations

These situations can be classified in three classes:
- design basis conditions
- internal hazards
- external hazards

2.2.3.1. Design basis conditions

These are the set of operational states and anticipated transients of incidental or accidental nature that are taken into account for equipment and structural design; they can be classified according to different criteria.

For the LWR, the document COM(81)519 final classifies those events, according to their frequency:

a) Events (operational occurrences) with moderate frequency, any of which may occur in every nuclear power plant several times during plant life.

Due to the presence of protective means in the plant, these events do not escalate into situations where the prescribed yearly dose limits (operational limits) are exceeded, although during short periods of time the normal exposure levels might be exceeded.

Examples of postulated events are:
- Loss of normal feed water
- Partial loss of core coolant flow
- Total loss of load and/or turbine trip
- Loss of off-site power.

b) Events or fault sequences which may occur during the life time of a particular plant.

Due to the presence of protective means in the plant, these events or fault sequences are not expected to escalate into situations where external countermeasures to protect the public are necessary other than for instance on a precautionary basis a monitoring programme (with respect to foodstuffs), although the prescribed yearly dose limits for normal operation might be exceeded.

An example of postulated events is:
- loss of primary reactor coolant from a small ruptured pipe of such an extent as to prevent normal reactor shut down and cool down, assuming make up is provided by normal make up only.

c) Events or fault sequences not expected to occur during the lifetime of a particular plant, but whose occurrence is nevertheless considered in the design.

Due to the presence of protective means in the plant, these events or fault sequences are not expected to escalate into situations where extensive off-site countermeasures are required to protect the public.
An example of postulated events is: double ended break of a large pipe in the primary pressure boundary.
Such events or fault sequences are used e.g. for the design of the containment.

For LMFBR those events have been classified according to the systems affected and in particular:

a) Core reactivity faults

- Incorrect withdrawal of absorbers
- Ejection of absorbers
- Core loading errors
- Ingress of cold sodium to core
- Addition of moderator
- Voiding by gas
- Variation of core configuration

b) General cooling accidents

- Primary pump failure or loss of power supply
- Failure in operation of valves in primary coolant circuits
- Loss of primary sodium
- Leak in the intermediate heat exchangers
- Failures in the main systems for removal of heat from the primary circuit
- Failure of core coolant supply structures
- Malfunction of decay heat removal

c) Sub-assembly faults

- Incorrect positioning of a sub-assembly
- Inlet and outlet blockages in a sub-assembly
- Local blockage or cooling defects within sub-assemblies
- Fuel pin failure
- Wrapper failure
- Damage propagation within sub-assembly and core

2.2.3.2. Internal hazards

In addition to the above-mentioned design basis conditions, internal hazards which could lead to failure of safety systems (in particular common cause failures) have to be considered in the design of containment building and some nearby auxiliary buildings. In this context, the internal missiles, high energy piping ruptures, internal floods and fires are taken into account.

2.2.3.3. External hazards

The external hazards, both natural and man-made, which are analyzed and, when appropriate, taken into account in the design basis studies for NPPs include:

- events of natural origin: earthquakes, continental and coastal floods, waves, extreme meteorological conditions.
- events caused by man-made activities: aircraft crashes, accidents arising from industrial activities and hazardous materials transport (explosions, fire, toxic gases).
- missile ejections e.g. from possible turbo generator failure.

Such external events are considered in either a deterministic manner, or by probabilistic techniques as appropriate and following the national practices.

Another kind of external hazard is sabotage. Measures are generally taken in the Member States to protect the NPPs but this point is not treated at Community level.

2.2.4. Safety systems

Reactor safety systems which initiate actions to prevent safety limits being exceeded are designed by applying the **single failure criterion**. They are hence **redundant** and capable of performing their function under the various operating conditions considered for the design, account being taken of one single failure.

During reactor operation, situations do, however, arise in which redundancy can be reduced or lost, and measures should be taken to cope with them from the safety standpoint.

These situations are:

- **non-availability of equipment** because of maintenance or repair work, resulting in situations in which redundancy is reduced
- **common cause/common mode failures**, which can result in the simultaneous loss of supposedly independent systems, including the
- **total loss of a redundant system**, no matter what the redundancy may be.

2.2.4.1. Non-availability of equipment

Non-availability of equipment may be either planned (maintenance) or the result of a breakdown. There are several ways of coping with situations of this type by measures taken at the design stage or during operation:

a) At the design stage, the system's degree of redundancy can be increased so as to allow necessary repair work to be carried out during operation without loosing the required redundancy.

Increasing a safety system's redundancy, i.e. adding, in parallel, components capable of performing the same function (pumps, valves, etc...), decreases the probability of failure of that system. No international consensus has yet been reached, however, on the advantage gained, in the case of a given system, by increasing redundancy of the systems.
Indeed, the limited advantages gained from such an increase can be offset by the increasing complexity of the installation.

Other methods are hence sometimes applied in order to increase the reliability of such systems:

- equipment diversification and physical separation to avoid common mode failures.
- mutual assistance between several existing systems.

These methods, of course, also have their drawbacks e.g. less independence between systems in the second example.

b) Adequate operating rules can be laid down such that, in the event of non-availability of safety equipment, the safety level is not significantly reduced in comparison with the case of full equipment availability. Such rules could include the requirement to return to a safe shutdown state within a limited period of time.

In coping with non-availability of equipment, a choice can thus be made from an economic standpoint between design measures and operating restrictions. As regards safety, it is necessary to ensure that the same level is ultimately attained in both cases; an overall comparison of safety must not be limited to the design aspects, but should also take account of the rules laid down for reactor operation and the assurance that can be obtained that operators will comply with them.

2.2.4.2. Common cause and common mode failures

Taking account of the impact of external and internal events on safety systems is an indispensable adjunct to redundancy; single failures or equipment outages can also be coped with by a redundant design.
Redundancy, however, does not always help to overcome common mode failures in identical subsystems or failures due to common causes like external or internal impacts. Indeed, fire, floods, earthquakes, frost and other such hazards are potentially capable of causing total system losses. Prevention of such losses is done by means of physical or geographical separation of systems, diversification, earthquake-proof design, independence of electrical power sources, etc.

2.2.4.3. Total system loss

In addition to the above mentioned precautions, a requirement is more and more often introduced: to study the effects of total loss of certain vital systems, such as heat sink, steam generator feedwater system, electricity supply systems, etc., and reduce their consequences by means of procedures or structural measures as far as is reasonably practicable.

2.2.5. Conclusion

The adoption of consistent sets of design and operating conditions is of utmost importance to ensure safety and this has been achieved in all Member States.

The deterministic method is used in all the Member States to design the NPPs with the same basic hypothesis and concepts and with some differences stemming from their implementation (in particular as concerns the "ALARP" concept) and from different technological practices. This has led to differences in some areas : containment systems and protection against external hazards, and methods applied to design the safety systems (redundancy, diversification, physical separation, mitigation of common cause failures).

One should also note that the analysis of the consequences of the total loss of safety systems or other technical supports (electrical power supplies for example) lead to differing positions which would benefit from further in depth comparison in the future.

It is likely that more attention will have to be given to beyond design basis measures. Therefore, it would be appropriate to study in depth the following areas:

- safety margins allowing structures and systems (and more particularly the containment) to survive beyond design basis accidents.

- measures available to assist operators in accidental situations.

2.3. PROBABILISTIC METHOD

2.3.1. Introduction

The probabilistic approach has been increasingly used over the last 10 years as a complementary tool for designing and licensing, so that nowadays all countries carry out some studies in all the headings (i) to (v).

This method is used in its more general form as **"probabilistic safety assessment"**, to verify overall safety consistency and calculate the overall risk, occasionally by comparing it with that of other industrial activities.
It is also applied in certain countries to validate measures intended to reduce the effects of certain failures (for example, total failure of redundant systems) and assign reliability objectives to some components important to safety.
This method is also used as a design procedure in order to take care of certain hazards external to the installations (aircraft crashes, explosions, etc...): consequences of those hazards are evaluated together with their probability of occurrence and, if necessary, extra protection means are incorporated. If the probability of such an event is sufficiently low this event is not taken into account in the design.

With the application of the probabilistic method, qualitative and/or quantitative probabilistic safety objectives have been introduced by some Member States authorities in addition to the existing deterministic safety requirements. Setting such objectives is another example of application of the ALARP principle cited above. However, because of some specific limitations of the probabilistic method (e.g. data uncertainties, difficulty in quantifying the human operator's role in accidents, the magnitude of common-mode failures that could be caused by fire or flooding, etc...), these safety objectives have generally not been made mandatory.

The use of probabilistic studies can be subdivided into several interrelated headings:

(i) Reliability analyses - including effects of redundancy, diversity, segregation, common mode failures, and human factors;

(ii) Consistency of overall design - including common cause effects and systems interaction; and

(iii) External hazards.

(iv) Feedback of operating data

(v) Risk analysis.

2.3.2. Reliability analyses

Most countries use reliability analyses to confirm the grounds used by the designer for choosing certain deterministic targets. In this respect the reliability technique has proved to be a substantial help to the designer in providing

- the proof of a sufficiently low probability of failure of a safety system;

- the evidence of possible weak points in the safety system;

and allowing

- the systematic examination of the safety measures for coping with individual accident sequences;

- the determination of check intervals and admissible repair times of components of the safety systems.

2.3.3. Consistency of overall design

Research into the reliability of all the important safety systems of a NPP allows the designer to appreciate the internal consistency of the different safety systems and to justify their design. It is one of the ways to identify potential sources of common mode failures, as well as undesirable systems interactions which may degrade the overall safety of the plant.

2.3.4. External hazards

In many countries probabilistic analyses are used to assist in quantifying the effects of external hazards on the design. The treatment of external hazards of human origin (e.g. aircraft crashes, industrial environment) is more straightforward than the treatment of natural external hazards (e.g. earthquakes, high winds). In the former case there is usually some representative historical data and the possible consequences are known, although the calculations may not be very accurate. However, in the latter case there is often little representative historical evidence and the likely consequences of very improbable events may be difficult to predict. This often leads to the inclusion of conservative margins in the probabilistic estimate.

2.3.5. Feedback of operating data

For the application of probabilistic techniques, data based on operational experience (e.g. component failure rates) are necessary. This is an area of increasing importance where co-operation of utilities and designers is vital in order to provide as large a data base as possible.

2.3.6. Risk analysis

The major use of probabilistic techniques is in probabilistic risk assessments (PRA) carried out during the preparation, and subsequent confirmation, of the safety case for a NPP. It is usual to divide PRA into three levels: level 1 is the identification of all the ways in which the plant can malfunction in such a manner as to lead to potential releases of radioactive products from the core together with estimates of the frequency of those fault sequences; level 2 is the categorization of those emissions in terms of size and frequency taking account of containment performance; level 3 is the calculation of the consequences in terms of population exposure and related consequences.

Although the impetus to use PRA arose from the general desire to evaluate the overall risk from the plant (e.g. in terms of cumulative probability distributions of late cancer deaths), the main benefits to safety come from the application of level 1 PRAs. The progression of level 2 and level 3 PRAs is encumbered by calculational uncertainties and difficulties of interpreting the significance of the results.
Although progress has been made in understanding the sources of uncertainty in PRAs, some problems persist e.g. the impossibility of finding all possible fault sequences and the associated phenomena with a valid verified approach, the handling of common mode failures, external hazards and human factors.

Most Member States recognise the importance of PRA and continue to develop it; few of them incorporate it in the formal licensing procedures.

2.3.7. The use of PRA techniques in setting quantified safety objectives

The task of quantifying safety objectives is difficult for various reasons, the most important of which is the uncertainty of the data

used in the PRA calculations.

Nevertheless in some countries great emphasis is placed on the development of safety objectives for the individual and for the society as part of the process by which regulatory authorities and electrical utilities could provide a consistent basis for decision making on safety.

2.3.8. Conclusion

The development and use of the probabilistic approach is becoming important within Member States, mainly as a complementary tool to the traditional deterministic approach.

The Commission is promoting the sharing between Members States of experience gained from its use in plant design, safety reviews and risk analysis (and in the associated field of safety objectives). Intercomparison exercises are also organized.

2.4. SYSTEMATIC USE OF OPERATING EXPERIENCE

2.4.1. Introduction

The deterministic and probabilistic methods are constantly being improved as knowledge is continuously expanded through reporting and analysis of the failures and incidents that occur in the hundreds of reactors in operation throughout the world. The systematic nature of the "corrections" made in the wake of these events and the increasing international exchange of information in this area constitute the most important factor in the unremitting drive to improve safety.

There is now a wealth of world-wide experience available from roughly 4000 reactor.years of operation over a 30-year period and from the Research and Development programmes set up in order to better understand the observed and anticipated phenomena. Individual plants and research facilities become sources of valuable information for many other plants in various countries. At the same time, all parties involved in the protection of public health and safety - plant operating organisations, vendors and safety regulators benefit from the accumulated scientific and technological knowledge.

Moreover the lessons learned from the analysis of severe accidents i.e. TMI and Chernobyl are taken into consideration for present and future plants.

2.4.2. Reporting and analysis of potential accident precursors

Systematic reporting and analysis of all operating incidents -even the minor ones - is a common practice, based on the awareness that such events can be directly or indirectly significant for safety e.g., common cause scram unavailabilities, power grid outages, steam generator tube failures and feedwater pipe problems in PWRs, relief pipe and pressure - suppression pool problems in BWRs.

There is also a general consensus on large-scale and timely dissemination of information on abnormal occurrences as a contribution to accident prevention.

2.4.3. Analysis of severe accidents

The conclusions reached after the TMI accident, which were recently confirmed through the analysis of the Chernobyl accident, show that, no matter how well a reactor is designed and operated, a severe accident can never be totally ruled out. In this situation the ultimate reactor containment may even be submitted to loadings greater than the design value.
That enhances even more the research work currently under way on the ultimate behaviour of containment systems, the cooling of molten cores and the definition of source terms. The aim of this research is to achieve a still better understanding of the phenomena associated with severe accidents so that measures can be taken to protect the public in such extreme conditions.

These measures concern:

- the protection of the integrity of the containment by additional systems and,
- the direct protection of the public by specific emergency plans and procedures.

TMI and CHERNOBYL severe accidents have underlined the importance of the containment as the ultimate barrier between the radioactive inventory of the core and the environment, the necessity for improving the interface between man-machine (instrumentation, operating procedures, ergonomy) and for allowing the operators to play their essential role in post-accidental management, avoiding diagnosis errors leading to worse plant conditions, and the importance of the "mitigation" of accidents consequences (e.g. safety actions to safeguard the containment).
On the other hand, highlights have been placed by those accidents on the benefits to be gained from emergency planning organization and training for operating personnel to gain a "safety culture" enabling them to drastically decrease the probability of severe accidents.

2.4.4. Backfitting of operating plants and design improvements for new plants as a result of operating experience

Backfitting means a modification to plant design according to or required by:

- discrepancy between designed and real plant, due for instance to abnormal aging of components, or
- evolution in safety requirements, which can lead either to additional features, e.g. for protection against external common cause events, or to a simpler design with higher quality materials, as is the case for the reactor coolant circuit supporting system, or
- operating incidents or accidents, new findings or developments, which reveal that additional precautions against damage are needed for keeping the operational risk at a reasonably low level.

In addition to the continuing supervision of safety performance by both the plant owner and the authorities as well as plant reexaminations following a major accident like TMI, there is a legal basis in most Member States for performing periodic safety reassessments of operating plants. This consists in a systematic comparison of plant design with the existing safety requirements, which may differ from the original design base.
To what extent the identified non-conformities have to be corrected is a practical problem for which pragmatic solutions are sought, mostly on a case-by-case basis, taking account of such factors as:

- experience with incidents and difficulties;
- cost/benefit considerations, which lead to a ranking of the envisaged modifications according to their relative merit for safety;
- possible adaptation of test and maintenance procedures;
- new operating procedures to cope with incidents;
- significance of the envisaged modifications in reducing the overall nuclear risk.

Examples of backfitting resulting from operating experience are numerous. They mostly concern the residual heat removal systems and their electrical supplies, the reactor coolant system integrity, post-accident qualification of equipment and containment survival in case of severe accidents.

It is generally agreed that improvements to the safety of old plants have to be applied in such a way as to take account of both the increased safety and the extra costs of modifications and production losses.

Moreover, there should be no undesirable consequences of modifications, e.g. increased system complexity or important exposure of plant personnel to radiation.

Should it turn out however that backfitting of a specific plant is necessary, as opposed to desirable, but at the same time is considered too costly, then there is no alternative left but to shut this plant down.

2.4.5. Conclusion

The systematic use of experience gained from daily operation and from the in-depth analysis of incidents and accidents is an important contribution to the safety of NPPs, allowing improvements in design of new plants as well as in systems and operation of existing plants.

3. SAFETY OBJECTIVES AND METHOD IN NPPs OPERATION

3.1. INTRODUCTION

Management of operation is very important to assuring nuclear safety.
The lessons learned from analysis of past incidents and accidents have increased the consciousness of the importance of the following factors: early detection of faults, man-machine interface, man-man comprehension, ergonomy, personnel training and safety culture.
These various subjects are to be addressed both for normal operation conditions - from cold shut down to full power, including transients programmed or due to incidents - for design basis accidents situations and for situations leading up to severe accidents.

As far as the general safety rules are concerned, safety is treated, from the operation point of view, in a similar way, in the Member States.

3.2. GENERAL OPERATING RULES

The general operating rules, which require the approval of the national safety authorities, include in particular:

- technical operating specifications,
- general matters relating to operating procedures,
- the measures to be taken in the event of incidents or accidents,
- periodical test programmes for systems of safety significance.

3.3. TECHNICAL OPERATING SPECIFICATIONS

Technical operating specifications define the technical rules to be complied with during different states of normal operation of the plant.

They: - specify the safety limits of the parameters taken into consideration at the design stage, which may not be exceeded.

- impose the protection thresholds of essential protection systems, which trigger an automatic response so as to ensure that the safety limits are not overridden.

- specify the functional limits for start-up, power operation and shut-down of a power plant.

- lay down the measures to be taken in the event of non-availability of one or more equipments or systems or in the case of abnormal changes in a parameter of safety significance, for example time limit for a unit to remain in a given state before returning to what is deemed to be the safest state.

Technical specifications are drawn up on the basis of deterministic criteria and with the assistance of probabilistic assessments, making use of the available reliability data for main components.
These documents are very detailed and necessarily differ from one plant to another

3.4. ORGANIZATION OF OPERATING EXPERIENCE FEEDBACK

The aim in organizing operating experience feedback is to reduce the frequency of incidents in order to reduce the safety implications and to avoid unnecessary shut downs. The main objective is the identification of incidents, precursors of more serious accidents, in order to define and apply the necessary corrective measures before these accidents occur.
The events are collected in databases, in each country, and selected events are submitted for incorporation in international databases and at JRC Ispra in order to allow sharing of information and in depth analysis of these events for the benefit of all participants.

3.5. OPERATION UNDER NORMAL CONDITIONS

The situation is nearly the same in the Member States. At present, there is a tendency to relieve operating staff from manual, routine control functions by the provision of operator aids like highly automated systems. In particular the importance of the man-machine interface is stressed (control room organization, alarms management...).

3.6. OPERATION UNDER INCIDENT AND ACCIDENT CONDITIONS

It is of utmost importance to have suitable procedures dealing with incidents and accidents. One important point is the control room arrangements: currently no operator action for instance is foreseen during the first period of time after a design basis accident (about 20 to 30 minutes, on average, according to the different designs), and a computerised information system presenting concise information regarding plant safety conditions is foreseen.
Another point is to take appropriate measures to mitigate the consequences of severe accidents: the prime objective being to ensure containment integrity.
Containment venting and filtering is being studied and for some countries implemented. The hardware measures are supplemented by appropriate procedures and training programmes.

3.7. EMERGENCY PLANS

Each nuclear site ought to have an emergency plan, in which the pre-planned actions of the utility are described. The main goals of these actions are:

1. to alert the authorities in the event of a nuclear accident to allow them to implement the external emergency plan including information to the public and the local and national emergency centres (as appropriate).

2. to set up the utility emergency organization in order to:
   - help the control room staff in the management of the accident
   - implement on-site and off-site radiological measurements
   - inform the authorities on the development of the accident.

3. to ensure the protection of workers.

3.8. PERSONNEL TRAINING

The operator role is essential for a safe operation of the plants. Very high qualification must be assured and maintained continuously and precautions are to be taken against lowering of attention during long operating periods without an incident.

Consequently, the operator training both for normal operation and operation under fault conditions is of great safety significance and systematic training programmes using simulators are very important.

Indeed, past experience has shown that a serious accident invariably has a "human factor" component, even if its origin lies in an equipment failure or an external event. The events at TMI and Chernobyl provide ample demonstration of this fact. Moreover when one considers not accidents but only incidents or even production losses, the human factor has a major involvement, varying from 30 to 60% depending on the type of event in question.
In the great majority of cases, appropriate staff training oriented towards the situations encountered would have enabled these incidents to be avoided. Training is therefore of utmost importance and priority.

Nuclear power stations are complex installations, and one can expect satisfactory performance from the people responsible for their operation only if they have in depth knowledge of how these installations are functioning. The training of personnel therefore necessarily involves the acquisition of basic knowledge, followed by practical experience and familiarization with the various mechanisms governing operation of the plant. Regular retraining is also needed to maintain and update the operator qualifications.

Specialized simulator training is necessary, being regarded in many respects as more profitable than training on the plant itself. The simulator enables the trainees to cope with disturbed situations they would encounter only rarely in actual operation, for instance after start-up testing.

3.9. CONCLUSION

Safe operation of NPPs requires compliance with well defined and approved technical operating specification, existence of operating procedures for normal and accidental conditions, organization of operating experience feedback and first of all, qualified and adequately trained operators having always safety in the fore-front of their planning for action.

4. GENERAL CONCLUSION

The safety of NPPs is assured by methods allowing to fulfill safety objectives. Three basic methods were described for safe design and the importance of a correct management of operation was stressed.

These objectives and methods are at present the subject of a consensus between the actors - authorities, manufacturers, utilities - in all Member Countries. In the implementation of the ALARP concept and in the importance given to probabilistic assessments differences exist, mainly due to the speed at which new technologies are adopted in the different countries.

Finally, the safety of NPPs cannot be considered as something that is acquired once and for all following acceptance of a given design. Rather, safety is a living concept whose maintenance requires perpetual vigilance and exploitation of experience taking account of technological progress and research results.