EDF
Electricité
de France

THE «WHITE BOOK» FOR PWR NUCLEAR SAFETY

GENERAL PHILOSOPHY

JUNE 1987

A-12

FOREWORD

We have collected in this "White Book" the principles which constitute the EDF's safety policy with respect to PWR nuclear units.

This document has no contractual value and is not intended for a use in our relations with the French Safety Authorities.

Although this work describes accurately the French nuclear safety approach as a whole, it should be noted that the details of the doctrine stated hereafter have not yet been approved by the French Safety Authorities, in particular for some subjects which are currently being discussed as part of the licensing procedure of the 1400 MW - N4 series.

CONTENTS

1 - INTRODUCTION

The implementation of France's major nuclear programme - 54 PWR units in service or under construction - has gone hand in hand with the development of an original philosophy in the field of nuclear safety. This philosophy combines two essential elements which have shaped this nuclear programme 1:

1/ Whilst the French units were originally built under licence from an American manufacturer (Westinghouse for the nuclear steam supply system), the design of these plants has been progressively made French. In terms of nuclear safety, this French influence has led to further development of the deterministic design approach current in the United States to include consideration of a number of additional situations based on a probabilistic approach. This has resulted in a better coherence for safety.

2/ Electricite de France performs the dual role of both operator and industrial architect of its power stations. This has resulted in an active commitment to safety in service, utilizing the feedback of operating experience at a very early stage in the design, and also by improving the design with a view to enhancing operational safety (man-machine interface, operating procedures).

Furthermore, the establishment of emergency plans has enabled the Safety Authorities and the operator to adopt a coherent and logical approach to the severe accidents which may call for the implementation of these plans. With the aim of achieving greater defence in depth, this has resulted in the provision of certain additional measures designed to further reduce the probability and consequences of severe accidents.

Thus, from an initial core of deterministic safety philosophy developed across the Atlantic, and which has been wholly retained and in some instances refined, a range of additions have been made which enhance the overall level of safety of the installations without undue complication.

This document describes the culmination of this work, as exemplified in the new 1 400 MWe plant series currently under construction, of which the essential elements are also incorporated into all previous units, thereby giving them an equivalent level of safety. This now constitutes EDF's safety policy with respect to PWR nuclear units.

2 - DETERMINISTIC DESIGN PHILOSOPHY

2.1 - BASIC PRINCIPLES

2.1.1 - Safety Objectives

EDF's fundamental objective in the design of PWR nuclear units is to ensure that :

- in normal operation, the dose equivalents received by workers and members of the public are as low as possible and, in any event, below the statutory limits,

- in more general terms, the presence of a unit on a site does not involve unacceptable risks for the population.

To this end, comprehensive technical measures are taken so as to be able to maintain or bring the unit into a safe condition at all times, such a condition being assured when the following three fundamental safety objectives are met :

- control of reactivity,

- removal of residual power,

- containment of radioactive substance.

2.1.2 - Design Philosophy

EDF's design philosophy hinges on the two basic principles of prevention and control of accidents. To this end, the philosophy is based on the concept of defence in depth, at three levels :

Level 1 : Every precaution is taken to ensure that the unit is fundamentally safe : quality of design studies (incorporating adequate safety margins), quality of construction and associated testing/inspection so that, in normal operation, including normal operating transients, the installation is not subject to failure. In particular, the specification of control systems is involved at this level.

Level 2 : It is assumed that incidents which can lead the unit out of its normal operating range may occur ; it is therefore necessary to detect and arrest the development of an incident process. This is the basis for the definition of safety systems designed to maintain the unit in a safe condition, together with that part of the protection system enabling these systems to be utilized.

Level 3 : It is further assumed that serious hypothetical accidents liable to compromise the containment of radioactive substances may occur.

In order to guard against these accidents, safeguard systems are designed together with that part of the protection system enabling their use, which operate to limit the consequences of such accidents to an acceptable level.

This concept is a particular feature of each of the three barriers placed between the nuclear fuel, which constitutes the principal source of radioactive substances, and the population :

- fuel cladding,

- main primary circuit,

- containment structure.

In practical terms, this deterministic approach to safety operates on the following principal lines :

a) establishment of as comprehensive a list as possible of events of internal origin liable to occur during the life of the installation, which may be of a hypothetical nature, classified into categories according to their estimated probability of occurence where this can be assessed,

b) selection within each category of so called "envelope" events, having regard to their consequences which should predominate over those of the other events in the same category, also referred to as design operating conditions,

c) design and rating of the various buildings, structures, systems and equipment so as to afford protection against the effects of the various events selected, followed by a study of their consequences using a number of deterministic conventions :

- to safeguard against random mode failure, the single failure criterion is applied to the accident design operating conditions (see definition para. 2.2.2) ; the statutory definition of this criterion is as follows :

"A mechanical system satisfies the single failure criterion, for a given function, if it is capable of performing this function despite a single active failure during the short period, or a single active or passive failure during the long post-accident period ; an electrical system satisfies the single failure criterion, for a given function, if it is capable of performing its function despite the failure of any component in this system".

- to guard against certain common mode failures, adoption of the principle of geographical or physical separation of redundant equipment, and independence of power sources, and of their distribution,

- accident studies conducted using pessimistic assumptions and conservative calculation rules aimed at producing the margins necessary for the deterministic approach to safety. The analysis should demonstrate that the action of the safeguard systems is capable of limiting the consequences for the station and for the environment to within given limits ; it should be performed with conservative assumptions, both with respect to accident scenarios and for assessment of the stability of the containment barriers and the plant as a whole,

d) allowance in the design for the existence of hazards of internal or external origin. It will be seen that for certain of these hazards, of external origin, use is made of probabistic methods in addition to the deterministic approach.

2.2 - EVENTS AND HAZARDS ALLOWED FOR IN THE DESIGN

2.2.1 - Introduction

From the inception of a project, the design of buildings, structures, systems and equipment is performed with due regard for analysis of "events and hazards" in a broad sense, and which must be taken into account in the deterministic approach to safety. These are of three different types :

- design operating conditions,

- hazards of internal origin,

- hazards of external origin.

These aspects are discussed in turn below, describing in each case the way in which they are taken into account and the associated acceptance criteria.

It will be noted that the majority of arrangements made in the design to guard against hazards of internal or external origin seek to minimise common mode risks. As such, these arrangements supplement those taken in respect of the single failure criterion and are essentially designed to ensure, as a minimum, that the unit is placed and maintained in a safe shut-down condition irrespective of these hazards. Consequently, it is necessary to regard these events as being entirely independant of the operating conditions and of the conservative assumptions, like the single failure criterion, associated with their analysis. They are considered in combination only with certain other aspects, fos reasons of convention, for example with seismic events, to develop conservative assumptions designed to produce design margins in accordance with statutory requirements.

2.2.2 - Design Operating Conditions

The term design operating condition refers to the range of operating and normal transient conditions, incident or accident conditions of the unit which must be taken into account in the design. These operating conditions have been assigned to four categories according to the order of magnitude of their estimated frequency of occurence. In each category a limited number of conventionnal operating conditions has been identified, the consequences of which predominate over those of the other operating conditions which may be considered.

Each of these categories is defined in the Table below, showing the associated acceptance criteria. Note that the criteria relating to radiological consequences specified for category 2, 3 and 4 operating conditions are not subject to a statutory requirement. In respect of categories 3 and 4, these criteria are orders of magnitude of the dose equivalent measured at the site boundary which the safety authorities deem to be acceptable provided that they are not exceeded in calculations performed using conservative assumptions.

CATEGORY	DEFINITION	ORDER OF MAGNITUDE OF ESTIMATED ANNUAL FREQUENCY OF OCCURENCE (f)	RADIOLOGICAL CONSEQUENCES AT SITE BOUNDARY
1	Normal operation	$f > 1$	Authorized releases in normal operation
2	Incidents of moderate frequency	$10^{-2} < f < 1$	Authorized releases in normal operation
3	Accidents of low frequency	$10^{-4} < f < 10^{-2}$	0.005 Sv (whole body dose) 0.015 Sv(Thyroid)
4	Serious hypothetical accidents	$10^{-6} < f < 10^{-4}$	0.15 Sv (whole body dose) 0.45 Sv (Thyroid)

All equipment required in design operating conditions to meet the fundamental safety objectives referred to in para. 2.1.1 are safety classified, which generates a whole range of particular requirements in terms of design, construction and operation.

2.2.3 - Hazards of Internal Origin

The term "hazards of internal origin" embraces all events other than the operating conditions referred to above occuring within the nuclear island buildings or within certain auxiliary buildings and which are liable to compromise nuclear safety by physical "violence". In this context, the following hazards are considered :

* Internal projectiles :

On the basis of design studies, testing and periodic inspections carried out, it has been possible to draw up a list of components or parts of components regarded as potential projectiles, particulary inside the reactor building, against which protection is provided via installation rules based on maintenance of the integrity of containment barriers and operation of the systems required to place and hold the reactor in a safe shut-down condition.

* High energy pipework breach :

In operation, breaches or cracking of pipework may occur. It is necessary to make allowance for the potential risk associated with the presence of pipework carrying a fluid medium in conditions of high temperature ($\geq$ 100 °C) and pressure ($\geq$ 20b abs). In addition to the functional aspect considered in the context of design operating conditions, it is necessary to examine the damage which may be caused outside the pipework either by the fluid or by the piping itself.

To this end, it is necessary to protect not only the components of systems designed to perform necessary safety functions, but also those of support systems required to enable these systems to function and, consequently, all associated mechanical and electrical components necessary to limit the consequences of the breach and to enable a safe shut-down condition to be achieved.

For this purpose, structural arrangements are made both in terms of civil engineering and plant design so as to satisfy the requirement for non-aggravation of the initial accident.

* Internal flooding :

The design of the installation to cater for this risk must ensure fulfilment of the safety functions deriving from the safety objectives defined in para. 2.1.1 despite a postulated internal flooding condition, either as an initiating event or as a passive failure during utilization of safeguard systems following an accident.

For this purpose, it is necessary to :

- protect not only the components of systems designed to perform the required safety functions, but also those of the support systems necessary to ensure their operation to enable a safe shutdown condition to be achieved.

- prevent or limit aggravation of the initiating event : internal flooding resulting from a given operating condition must not exacerbate this condition.

* Fire :

In normal operation, the risk of fire is one of the major hazards with which the operator may be required to deal and against which it is necessary to provide protection. Moreover, a fire - even of limited extent - may have serious consequences if safety functions are compromised (cf fire at Browns Ferry in the U.S.A.).

The fire risk is taken into account at the design stage with reference to the triple aspects of prevention, detection and firefighting :

- prevention : choice of materials and plant layout designed to limit the risk of fire and spread of fire from one safety system to another,

- detection : the outbreak of fire must be detected rapidly and accurately to facilitate the immediate deployment of firefighting facilities,

- firefighting : the provision made at the design stage involves arrangements for evacuation of personnel, access for firefighting crews and extinguishing of the fire using fixed (automatic or otherwise) or mobile firefighting systems.

2.2.4 - Hazards of External Origin

External events of natural origin or due to human activity which are analysed and, where necessary, allowed for in the design of each nuclear unit, are as follows :

- hazards of natural origin : earthquakes, continental and marine flooding, extreme meteorological conditions, swell ;

- hazards related to human activity : aircraft crashes, industrial environment and lines of communication (explosions, fire, toxic gases) ;

- emission of projectiles resulting from failure of a turbo-alternator set.

For design purposes, the basic principle governing the choice of reference level for each of these hazards is the observance of a probabilistic criterion coherent with the criteria implicitly used to define the design operating conditions (see para. 3.1).

An attempt is thus made to bring some coherence into the way in which these various internal or external risks are taken into account. It is important to note that this effort to achieve coherence extends both to occurences of initiating events them-selves and to the consequences which may result therefrom.

In the present state of knowledge, and at the level at which the assessment is required, it appears that natural events are not all amenable to probabilistic treatment, by virtue of their extremely low probability of occurence and because the envelope value to be taken into account is difficult to quantify. The events for which the probabilistic approach is not applicable are then allowed for in the design on a deterministic basis with a sufficient margin (seismic event, external flooding, for which a "safe shutdown level" is defined).

2.3 - LIMITATIONS OF THE DETERMINISTIC APPROACH

The design of equipment and systems according to the deterministic method described above (selection of a limited number of design operating conditions, consideration of envelope values for physical parameters, application of the single failure criterion, redundancy of safeguard systems, application of aggravating assumptions) has made it possible to design and construct a given product which satisfies a set of envelope hypotheses. In addition, with a view to ensuring the coherence of the studies thus carried out, EDF undertakes critical examinations of the design of the entire system or major subsystems. These examinations take the form of project reviews and design reviews.

However, although providing appreciable margins for the envelope cases treated, the studies thus carried out cannot make claim to complete coherence embracing all operating conditions which can be envisaged. It therefore became clear that the deterministic method, whilst highly effective for design purposes, has the basic flaw of being restrictive, which poses a number of questions relating to safety analysis :

- is the list of operating conditions defined at any given moment sufficient and truly all embracing ?

- is it acceptable to lose safety systems designed according to this methodology ?

- does this philosophy actually result in a coherent design of the unit in terms of safety ?

The answer to these questions may be found first and foremost in the utilization of probabilistic studies (see Section 3) which have made an undeniable contribution as an aid to the design and verification of coherency of safety. These studies have also contributed to the identification of complementary operating conditions (see Section 4) and to the establishment of coherent technical specifications to cater for conditions of deliberate or inadvertent unavailability of important safety related equipment.

It was then found that the deterministic design philosophy gave rise to an event-related approach to plant operation based on operating conditions, the limitations of which were amply demonstrated by the TMI 2 accident. EDF has therefore developed a policy of prevention of severe accidents based on the so called "physical states" approach to plant operation (see Section 5).

Furthermore, no matter how small the probability of occurence of such accidents may be in the light of the preventive measures adopted, the consequences and actions to be taken in the event of a severe accident occuring have been studied (see par. 6).

Finally, this philosophy would be entirely worthless were it not validated by experience and complemented by a uniform policy of safety in service (see Section 7).

3 - CONTRIBUTION OF THE PROBABILISTIC TOOL TO DESIGN

3.1 - EXTERNAL EVENTS

Intially, the probabilistic tool was used to study external hazards due to human activity (aircraft crashes, industrial environment), which are considered on the basis of a probabilistic assessment of risk, because the statistical data are sufficiently representative and the events considered are sufficiently well known. This does not rule out the incorporation of conservative margins both in terms of calculation assumptions and definition of the event involved.

For this type of event, fundamental safety rules have been established to define probabilistic safety objectives, and which set the upper limit of probability of an unacceptable release of radioactive substances at the site boundary at approximately 10^{-7} per year, per unit, per safety function and per group of events. A risk of probability below this limit will be referred to as "residual risk". The basic principle for protection of power station against this type of event thus involves the adoption of structural arrangements (protection of the systems involved by buildings, physical or geographical separation of redundant systems, ...) designed to reduce the risk to this residual level.

3.2 - DESIGN AID

In parallel with this, and from the inception of its nuclear programme, EDF set up a programme of work for methods development and data acquisition to facilitate a detailed reliability analysis of the safety systems of a power station. These studies yielded immediate and practical results, thereby making an important contribution, as illustrated by the following examples :

- identification of reliability gains obtained by improving the layout of the safety injection system for the 900 and 1300 MW series units.

- establishment of the importance of the problems of common mode failure, showing the limited gain obtained in terms of overall system reliability in changing from a "two line" configuration to a "three line" configuration, and the importance of diversification of systems to attain a high level of reliability.

These two examples show the substantial benefit brought to the designer by the probabilistic tool, which essentially involves lending support to the deterministic choices made. This is also true in the case of maintenance which is taken into account at the design stage, and more generally in the technical operating specifications. These limit the time permitted to continue operation of a unit when part of the equipment on a safety system is unavailable. Rather than systematically increasing the redundancy of equipment to cater for chance unavailability or maintenance, the maximum possible unavailability time is calculated such that the additional risk remains extremely small (of the order of 10^{-7} per unavailability and per year).

In cases where the time obtained is too limited, EDF has increased the redundancy of certain active equipment belonging to safety systems which are frequently activated (Essential Service water system pumps for example).

3.3 - VERIFICATION OF DESIGN COHERENCE

For the 1300 MW plant series, EDF has studied the reliability of the main safety related systems. These studies have facilitated an assessment of the uniformity of reliability of these various systems and validation of their design.

However, in essentially qualitative terms, these analyses have revealed a number of potential common mode failures. In addition, the probabilities of failure obtained, whilst satisfactory, have not made it possible to entirely exclude an allowance for simultaneous failure of two redundant lines within the same function.

It was therefore felt necessary to seek further measures to ensure a uniform approach to safety design for the unit. To this end, it is necessary to verify that accident sequences which are not envisaged in the design are consistent (in terms of probabilities and associated radiological consequences) with the design operating conditions.

In this respect, it is first necessary to recall (see para. 2.2.2) that the limits of the domain which served as the basis for the unit design correspond to Category 4 accidents (order of magnitude of probability of occurence : 10^{-4} to 10^{-6} per year).

These accidents should not have unacceptable radiological consequences (0.15 Sv whole body dose, and 0.45 Sv to the thyroid at the site boundary), when the calculations are performed using a number of pessimistic deterministic assumptions which it would be theoretically possible to translate into probibalistic terms (application of the single failure criterion, systematic pessimism of physical parameters considered, cumulative loss of external electrical sources, etc ..).

In the case of accident sequences not envisaged in the design, and which may have unacceptable radiological consequences, it is therefore necessary to verify that the probability of such consequences arising is sufficiently low. In practical terms, it has been choosen that, for the sequences studied using realistic assumptions and data, in particular actual probabilities of equipment failure, the probability of unacceptable consequences should be less than 10^{-7} per reactor and per year. In addition, the unacceptable consequences have been defined as being a prolonged uncovering of the core, which generally introduces an additional margin relative to the target radiological consequences given in the Table in para. 2.2.2. Note the coherence of this practical criterion with that used for external events (see para. 3.1).

These conditions prompted EDF and the Safety Authorities to define a set of so called complementary operating conditions, described in Section 4 below. These conditions basically involve accident sequences which override the single failure criterion (total loss of redundant safety systems) for which compliance with the probabilistic objective defined above, and hence rejection of unacceptable consequences in the area of residual risk, has been achieved by the definition of adapted operating procedures and, where necessary, by the introduction of additional equipment.

3.4 - PROBABILISTIC SAFETY STUDY

The successful completion of the studies referred to above has yielded an important body of experience both in terms of the methods of assessment and probabilistic evaluation of accident sequences, and in terms of the problems raised by these studies (quantification of common mode faults, human factors, ...) ; in addition, a range of related software and a body of reliability data specific to French equipment have been developed. This will enable EDF to make a further step forward in its understanding of the reliability of its installations on the basis of a probabilistic safety study applied to a 1300 MW power station. Apart from further confirming the high level of safety of French units, this study should provide the designer with an even more complete aid to design tool, not forgetting the operational benefits referred to in Section 7. It should be noted that a similar study has been undertaken by the Institute of Nuclear Protection and Safety with reference to the 900 MW plant series.

3.5 - LIMITATION OF THE PROBABILISTIC TOOL

Just as the deterministic approach has its limitations, probabilistic reliability studies have their own particular limitations. Without going into detail, suffice it to say that these limitations stem in particular from the difficulty of determining all possible undesirable scenarios and of precisely quantifying all necessary data in terms of human factors, common mode faults or sudden failure of major components. Whilst fully aware of the importance of the probabilistic tool and pursuing its development, EDF is thus reluctant to speak of a probabilistic approach to safety in design, which remains fundamentally deterministic.

4 - COMPLEMENTARY OPERATING CONDITIONS

This complementary operating range, historically referred to as the "beyond design" range, embraces a number of complementary events and combinations of events related either to short term loss of frequently used redundant safety systems or to the medium and long term loss of safeguard systems involved in accident sequences initiated by a loss of primary coolant.

This area thus supplements the area covered by design operating conditions.

4.1 - SHORT TERM LOSS OF FREQUENTLY USED REDUNDANT SYSTEMS

Initially, EDF focussed its attention specifically on the consequences of short term loss of redundant safety systems which are frequently used in normal operation of the unit or in Category 2 operating conditions (see para. 2.2.2).

It was felt appropriate to check whether in the event of activation of the systems the failure to fulfil their function could lead to unacceptable consequences from the safety stand point, defined as being in excess of those accepted for Category 4 operating conditions.

The following complementary operating conditions have been considered : total loss of heat sink, total loss of steam generator feed-water and total loss of power supplies.

The results of the studies undertaken, based on the reliability of these systems, showed that for the complementary operating conditions referred to above, unacceptable consequences could arise in the event of failure. For this reason, EDF undertook a study of the measures necessary to prevent these events and reduce the probability of sequences leading to such consequences (prolonged uncovering of the core, see para. 3.3).

Special procedures were thus put into effect. These procedures are characterized by a high degree of flexibility and attempt to derive maximum benefit from existing systems. In certain cases, this approach called for the introduction of additional equipment and systems, but preference was given in all cases to functional redundancy and diversification rather than increasing redundancy within existing systems designed on deterministic lines. This approach essentially made it possible to reduce common mode risks whose contribution is poorly understood and cannot always be satisfactorily treated in probabilistic studies.

Procedures relating to the loss of frequently activated redundant systems, historically referred to as "beyond design procedures" include the following :

H1 : total loss of heat sink,

H2 : total loss of steam generator feedwater,

H3 : total loss of power supplies.

Although not covered by a procedure, it should be noted that provision has been made to cater for certain anticipated transients without scram (ATWS). Indeed, this type of accident was under investigation even before the incident at SALEM in 1983 in the United States involving a precursor incident of common mode failure on the emergency shutdown control system. It was concluded that the problem could be resolved by a diversification of the signals controlling main turbine trip and starting of the steam generator emergency feed pumps.

It is noteworthy that the equipment used in the short term in these procedures and which is not classified in relation to design operating conditions, is covered by a specific safety classification.

4.2 - LONG TERM LOSS OFF SAFEGUARD SYSTEMS

The next phase of the study focussed attention on the medium and long term loss of redundant safeguard systems utilized following a primary loss of coolant accident. These systems are required to remove residual power from the reactor and to operate for several months following a primary loss of coolant accident.

These include the EAS system (containment spray system) and ISBP system (low pressure safety injection) for which the long term failure of these pumping facilities is examined.

By applying the principles referred to in para. 4.1, it has thus been possible to achieve mutual backup between the low pressure safety injection system and containment spray system, initially by incorporating mobile inter-connections between the two circuits (procedure H4).

At a later stage, after about a fortnight, it is possible to provide emergency backup for certain failed equipment which may be difficult to repair notably in view of the radioactive environment, by means of mobile equipment (pump and heatexchanger) fitted at the same time as the mobile connections. This procedure, which is a natural extension to H4, was initially regarded as an ultimate procedure (see Section 6) and designated U3. In fact, procedures H4 - U3, which both relate to prevention of core meltdown, should be considered as a whole.

It will be noted that every effort has been made to exclude the possibility of a false manoeuvre during "normal" operation of these systems.

Equipment utilized solely on the basis of these procedures is designated as "important for safety - non-classified" and is covered by particular requirements specified in each individual case in order to ensure good availability.

4.3 - CHECKING THE GOOD HOMOGENEITY

It is important that the designer who has the above procedures at his disposal is able to verify that the complementary operating conditions thus defined are consistent in relation to design operating conditions. For this purpose, use is made of a probabilistic approach designed to verify that, in the event of occurence of one of these complementary conditions, the probability of unacceptable consequences arising remains within the area of residual risk (see para. 3.3).

Furthermore, in order to preserve the role of the deterministic approach in design, it was decided to set a ceiling on the gains anticipated from procedure H and from the complementary equipment where appropriate. This is achieved by imposing the requirement that the gain on the probability of exposure of the core remains below a factor of the order of 100. This means that every sequence leading to unacceptable consequences with a probability greater than 10^{-5} per unit per year must entail a re-examination of the basic design and may not be treated using this complementary approach.

In conclusion, all H procedures were thus analysed using probabilistic risk studies. The target of 10^{-7} per reactor and per year for core exposure was achieved for each of them, bu the use of procedures and, where necessary, additional facilities the need for which did not clearly emerge from the deterministic design approach.

5 - "NON-EVENT-RELATED" APPROACH TO PLANT OPERATION

Consistent with a philosophy which puts prevention before utilization, albeit necessary, of facilities designed to deal with the consequences of an event, EDF has developed an original approach to plant operation aimed at optimising prevention of core meltdown : the "physical states related approach".

The power station as designed, with due allowance for design and complementary operating conditions, must be capable of providing satisfactory core cooling in all circumstances, thereby avoiding any possibility of core meltdown, provided that the operators are effectively capable of events, perhaps not very serious when taken individually, which may be compounded by simultaneous or staged equipment or human failure. Therefore, it is not possible for event-related operating procedures to cater for all possible eventualities and, moreover, it is not possible to entirely rule out the possibility of a diagnostic error on which the choice of procedure is made.

EDF therefore developped a procedure referred to as "U1" based on an approach related to the states of cooling of the nuclear steam supply system (NSSS), whereby operator action is based not on a reconstruction of events occuring previously, but on identification of the physical state of the NSSS and facilities available to cool the core. This procedure is based on the measurement of a number of physical parameters representing these cooling states, of which the most significant is the difference in hot water temperature vis-a-vis the saturation temperature (boiling margin).

The physical states related approach is currently being developed as standard practice, and involves the elimination of event-related accident procedures and their replacment by a set of physical states related procedures facilitating post-accident operation adapted to the actual status of the reactor. These new procedures will be operational when the first units of the N4 plant series are scheduled for commissioning.

Introduction of this new method of operation clearly shows that, given the diversity of design features provided for core cooling and optimum management of these facilities using the physical states related approach, a core meltdown accident is not within the realm of the "plausible". Beyond this, one enters the realm of the severe hypothetical accidents described below.

6 - SEVERE HYPOTHETICAL ACCIDENTS

Application of the prevention philosophy described in the preceding sections has reduced the probability of severe hypothetical accidents to the area of residual risk. However, in line with the concept of defence in depth, it was felt necessary to supplement this safety approach by making allowance for these events even though they are not considered plausible. Studies were conducted and, where appropriate, measures taken to reduce the effects of such accidents and to hold the consequences at levels compatible with the implementation of emergency plans which define the arrangements to be made to protect the population and environment.

In this scenario, which assumes that core meltdown has occured, the principal concern is to safeguard the containment structure which constitutes the ultimate barrier between the radioactive products and the environment. The integrity of this structure must be maintained for a period compatible with implementation of the emergency plans prepared by the authorities. In order to keep the situation on a manageable footing, French emergency plans provide for the confinement of populations within a radius of 10 km and evacuation of populations within a radius of 5 km. Studies carried out have indicated that the source term (TS) representing accidents leading to environmental releases under 1 % of the core inventory excluding rare gases, is compatible with implementation of these emergency plans. Measures must therefore be taken to ensure that TS is the most serious source term which can arise.

Five possible failure modes of the containment structure have been identified and investigated (see Rasmussen WASH 1400 report) :

6.1 - STEAM EXPLOSION

This phenomenon involves a failure of the containment structure resulting from violent interaction between molten fuel and water contained at the bottom of the reactor vessel or at the bottom of the reactor pit in the event of rupture of the vessel bottom. The studies carried out show that, even with a pessimistic evaluation of the energy released following such an interaction within the vessel, the generation of massive missiles liable to compromise the containment integrity is not plausible.

This is basically due to the fact that no reactivity accident is likely to induce a damaging power excursion. Moreover, it appears that in the majority of accident sequences the reactor pit is dry when the vessel ruptures, and there are no processes taking place which could lead to the creation of large missiles. Finally, the pressure peak resulting from these phenomena is not sufficient to threaten the containment integrity. On this basis, it is possible to conclude that this mode of failure of the containment is not likely and need not be taken into account.

6.2 - PENETRATION FAILURE

To deal with the random failure of a containment penetration following a severe hypothetical accident in the reactor building, or of a safeguard circuit carrying highly contaminated water outside the containment, a special procedure designated U2 has been developed with the aim of pinpointing and sealing off the leak, and subsequently to provide for re-injection where necessary of the contaminated water recovered back towards the reactors building.

6.3 - HYDROGEN EXPLOSION

This risk involves loss of containment following an explosion of hydrogen released in large quantities essentially by the zircalloy-water reaction, secondarily and in the medium term by radiolysis of water in the sump chambers and decomposition of concrete despite the use of the mobile hydrogen recombiner provided for this purpose.

This problem is indeed of some concern in the case of containments having a small free internal volume (ice condenser containments for example) or those which are designed for low pressure peaks (pressure suppression containments for boiling water reactors), but is much less significant in the case of large dry containments designed to withstand high accident pressures.

EDF has participated in an international research programme on this topic coordinated by the EPRI in the United States. The latest findings indicate that containment structures for French PWR units do not present any risk of failure due to a hydrogen explosion, and that no particular provision need therefore be made to cater for this phenomenon.

6.4 - FOUNDATION RAFT LEAKTIGHTNESS FAILURE

Following an uncontrolled severe hypothetical accident, a situation can be envisaged whereby the corium (mixture of melted core and structures) comes into direct contact with the foundation raft of the reactor building. Design features incorporated into the 1400 MW-N4 series (no drains in the middle portion of the reactor building raft) will prevent early contact between the corium and the outside. Should the raft be penetrated, after approximately six days, and allowing for radioactive decay and the ground retention factor, the immediate radiological consequences would remain small having regard to the probability of occurence of this event and the measures which have been taken to implement internal (PUI) or external (PPI) emergency plans (see Section 7).

Studies carried out show that atmospheric discharges in the short term would be of the order of one hundredth of TS.

In the longer term, apart from any mesures taken to prevent the transfer of contamination from the water table to areas outside the site, the transfer time via the water table would permit conservative measures to be taken in terms of water usage (emergency plans).

6.5 - CONTAINEMENT OVERPRESSURE

This phenomenon would involve delayed loss of containment integrity due to a rise in pressure in excess of the design pressure.

Pressure rise within the containement is related to the formation of incondensables (essentially CO - CO2) resulting from decomposition of the raft concrete by the corium (mixture of molten fuel and structures) accompanied by more or less extensive vaporization of water depending on the scenario envisaged. The time to loss of containment integrity due to its mechanical characteristics being exceeded therefore varies from one to several days depending on the asumptions made.

This process gives the operator time to take action to prevent containment failure with the best control of radioactive releases.

This action, formalized in a procedure designated U5, involves limiting the pressure in the containment to a level equal to the containment design pressure. To do this, the pressure within the containment is reduced via a sand bed filter caisson, this system being connected downstream to the effluents discharge stack. The use of the U5 procédure after 24 hours with the use of the sand filter ensures that discharges are below the source term TS defined above, and event TS/10 after several days, depending of the assumptions made.

6.6 - CONCLUSION

It is thus seen that, in the area of severe hypothetical accidents, EDF has instituted a range of simple measures (in addition to its prevention policy) which facilitate implementation of emergency plans within the timescales imposed and with the radiological consequences involved.

7 - NUCLEAR SAFETY IN SERVICE

The purpose of Nuclear Safety in Service is to :

- maintain and if nessary improve the level of safety defined at the design stage for the installation,

- manage incident or accident situations and, in particular, crisis situations.

7.1 - MAINTENANCE OF SAFETY LEVEL

In order to maintain the level of Safety, it is first of all necessary to observe the operating limits provided for in the design. These limits are set out in a document entitled "Technical Operating Specifications" witch itself forms part of the General Operating Rules contained in the "Operation" volume of the Safety Report.

The Technical Operating Specifictions indicate :

- limit thresholds to be applied to normal operating or transient parameters,

- availability of equipment required to move from one state to another,

- permitted periods for continued operation in the event of unplanned unavailability of essential equipment.

Having defined and monitored the availability of equipment, it is necessary to ensure that this equipment retains the servicability and performance provided for in the design : this is the role of in-service periodic testing.

An exhaustive analysis is carried out on systems important for safety (IPS) to identify which equipment is required to undergo periodic testing and to justify which items do not require testing (normal operation is sufficient proof of good working order). For each system, a "test procedure" document specifies the operating procedure for each test and sets out the acceptability criteria adopted and the test intervals required. These instructions are used as the basis for preparing "test schedules" used by the operators.

In the case of component replacements, and particularly in the case of system or component modifications, the job specification stipulates the type of "re-qualificatin test" required, which may often merely consist of a simple periodic test.

In addition, by legislative order of 26 February 1974, the Government gave statutory force to monitoring programmes for the main primary system and to the conditions and requirements for intervention on this system. EDF's Thermal Generation Division has extended the spirit of this order to include all IPS equipment :

- by defining the concept of "specialized activities" which require prior approval by the Administration, acceptance by the organizations involved and an independent inspection procedure ;

- and by drawing up "basic preventive maintenance programmes" for all IPS equipment. These basic programmes are used by the power stations as guides to good maintenance practice, and are used as the basis for developing specific programmes to suit local conditions.

7.2 - IMPROVEMENT OF SAFETY

With a view to improving Safety, all incidents, including the most minor, occuring during operation are analysed to ensure that they are not "precursors" of more serious accidents. The results obtained from this analysis may give rise to improvements on the equipment or systems(this constitutes feedback of experience to the design), on documentation or on staff training.

7.2.1 - Feedback of operating Experience to Design

The policy of standardization adopted by EDF (one main PWR system including a limited number of individual plant series - 900 MW and 1300 MW - preceding the inception of the 1400 MW-N4 advanced PWR series) justifies the major commitment by EDF to maximise the value of operating experience by placing particular emphasis on the analysis of precursor incidents. This work has a dual purpose :

- to reduce the frequency of incidents liable to cause unavailability of generation, even where they have no direct bearing on safety,

- to reduce the frequency of more serious incidents liable to have consequences for safety ; the design principles for nuclear units based on defence in depth and the presence of barriers are such that serious accidents could only result in practice from a simultaneous combination of independent and more probable incidents.

In terms of nuclear safety, the principal objectives of experience feedback are as follows :

- to identify precursor incidents of more serious accidents in order to define and implement any corrective measures required before these accidents occur,

- to take advantage of the standardization of units (generic aspect of incidents, maximum benefit derived from modification studies, etc ...),

- to ensure, in cases where modifications are necessary, that these do not have any adverse secondary effects before they are standardized on the entire plant series,

- to utilize data gathered during actual operation of the installations in order to harmonise their level of safety, if required, especially in the case of new plant series.

The guidelines on which EDF has developed its system of operating experience feedback are as follows :

- to systematically gather maximum data and circulate these data very widely, particularly within EDF (see para. 7.4.2 below),

- to bring together as far as possible designers, operators, manufacturers and safety authorities in analysis of the data gathered,

- to learn from the experience gained to the benefit not only of units planned or under construction but also of units in service ; for example, the design of the new 1400 MW-N4 series takes full account of operating experience on the units in the 900 MW and 1300 MW plant series as well as the TMI2 accident.

By way of illustration, on the basis of the TMI2 accident, 46 separate actions were defined and implemented on the 900 MW series which was then at the commissioning stage. These actions gave rise to over 3000 interventions on the units. The 1300 series, which was then under construction, immediately incorporated many of these features, and today, on the 1400 MW-N4 series, we can confirm that all of the lessons learnt from this accident are routinely incorporated into the design studies.

In more general terms, since the introduction of the experience feedback programme in EDF, nearly 300 modifications of a generic nature, of which around 60 % relate to safety, have been implemented on all units in the 900 MW series, following an analysis by EDF groups of experts responsible for the experience feedback programme.

Clearly, there is always room for improvement, and it is not impossible that the daily analysis of events as part of the experience feedback process will reveal new ways of making improvements. It may be said, however, that in the main the present design is validated by experience and provides a satisfactory level of safety for the projects. Progress has been made in improving the reliability of certain components (valves, etc), and the steam generator which is undoubtedly a weak point in terms of service life of equipments and therefore in the operation of the power stations. The design of the steam generator and choice of materials are of primary concern, together with monitoring of its condition and effecive controle of any leaks, and the establishment of effective operator procedures to deal with primary/secondary leaks.

7.2.2 - Operation in Incident & Accident Conditions

Accident operation was reviewed following the Three Mile Island Accident ; this was one of the major measures taken of the 46 actions decided upon, and is based on :

- incident and accident procedures ;

- a control room adapted to suit operation in incident and accident conditions ;

- the presence in the control room of a safety engineer (so-called ISR).

7.2.2.1 - Incident & Accident Procedures

These comprise :

- procedure guidelines, support documentation and training documentation ;

- operating procedures used by the control room operators.

The procedure guidelines are drawn up by the designers and specialists in incident and accident operations.

The operating procedures are written in a style and format suited to the operator's needs. The format was developed on the basis of extensive studies carried out on a training simulator.

Implementation of accident operating procedures requires the following personnel in the control room :

- an operator mainly responsible for the primary system and associated safeguard systems ;

- an operator responsible for the steam generators and, more generally, the secondary system of the unit ;

- a shift engineer to co-ordinate these activities and to monitor the key aspects.

In addition, auxiliary operators may be required to carry out operations directy on the plant. Each participant has his own operating instructions.

In the 1400 MW-N4 series, the area of post-accident operation will be covered by a set of "physical states related" processus as embodied in the physical states related philosophy discussed in Section 5, and which include separate diagnostic and operating documents designed to provide human redundancy (see para. 7.2.2.3).

7.2.2.2 - Man-Machine Interface Improvement

The first step was taken on the 900 MW series with the introduction of an additional aid to operation in disturbed conditions, in the form of safety panels in the control room.

These panels provide for computer-aided diagnosis and application of accident procedures.

One panel in the control room associated with the main unit is provided for use by the operations staff.

A second panel in the control room is provided for use by the safety engineer (ISR).

A third panel located in the crisis technical room is provided for use by the backup operations crew working in this room in the event of a crisis on the unit. An interface is provided to facilitate data interchange with the "National crisis Centres".

Control room design subsequently developed towards the integration of post-accident operation with normal operation. Already partially implemented in the 1 300 MW series, the culmination of these developments begun in 1981 is the 1 400 MWe - N4 control room which can be used to operate the unit in all operating situations from computerized workstations.

7.2.2.3 - Safety Engineer

Each site is now provided with its own safety engineer (ISR). This engineer, who is called to the control room in the event of an emergency shutdown or safety injection, is required to assume responsibility for the plant in incident or accident situations or for any event not covered by the procedures. For this purpose, the ISR undergoes specialized and extensive training.

The ISR performs a continuous monitoring and diagnostic function in any accident situation.

The ISR, shift engineer and control room staff are required to strictly observe the allocation of tasks as defined in the procedures, which ensures the necessary independence for analysis of events.

"Human redundancy" is thereby assured in post-accident operation.

7.3 - MANAGEMENT OF CRISIS SITUATIONS

Eah nuclear site has an internal emergency plan (PUI) which is implemented at the site manager's discretion in the event of a major accident (non-radiological accident - level 1, accident having or liable to have radiological consquences, either within the site - level 2, or outside the site - level 3).

The purpose of the plan is to define and organise the necessary means to aid the operations staff to bring the plant to a safe condition and to minimize the consequences of the accident.

In the event of a level 2 or 3 accident, the site manager will implement the national crisis organisation. This procedure may also be initiated by EDF Management or Head of the Central Department for Safety of Nuclear Installations (safety authorities). This brings together the tree key participants (power station, EDF Paris and Safety Authorities) and the crisis operating teams responsible for advising them.

It should be noted that the individual emergency plans (PPI) organized by the public authorities outside the site are fully compatible and complementary with the PUI emergency plans. The three levels defined in the PUI in fact correspond to the three alert conditions specified in the PPI plans.

7.4 - THE MEANS FOR SAFETY IN SERVICE

Safety in service can only be provided by well trained people. To aid the analysis of operating experience feedback, the Thermal Generation Division has set up a number of organizations charged with gathering and storing data on computer file. Furthermore, safety could not be guaranteed without the work being organized and without this organization being of the highest quality.

7.4.1 - Training of Personnel

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 event outside the power station. In this respect, the events at TMI and Chernobyl provide ample demonstration of this fact without the need for further explanation. What is less widely known is that when one considers only incidents which have occured or only 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 geared towards the situations encountered would have enable these incidents to be avoided. Thus, for us, this training is of the utmost priority.

Nuclear power stations are complex installations, and one can only expect satisfactory performance from the people responsible for their operation to the extent that they have in depth knowledge of how these installations function. 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 power station.

From the outset, EDF has provided a highly systematic training structure for its staff, covering managers, supervisory staff and shopfloor workers alike, combining traditional forms of training with practical experience in situ. This structure has been extended to cope with the considerable task facing EDF : to train operating staff for several tens of units in a few years. The training structure has been tailored to cater for the specific nature of nuclear power.

We have learnt two important lessons from our experience :

- the necessity for continuous refresher training, to ensure that staff do not forget the technical principles of the installation in the course of their daily work at the station. To this end, the system of computer-aided teaching (CAT) which has been in operation for several years at all power stations, has proved to be a highly effective tool.

- the necessity for specialized simulator training, which is in many respects regarded as being more profitable than training on the plant itself. The simultaor enables the trainee to cope with disturbed situations which he would encounter only rarely in actual operation, if only during start-up testing.

The training centre at Bugey was the first to be equipped with one then several simulators. Subsequently, new training centres were set up at Paluel and Caen. In terms of safety, the use of simulators was a further step forward in as much as they are not confined to operator training but can also be used to ensure compatibility between the operating procedures and the personnel responsible for applying them.

This is indeed an important lesson. Whilst the operating instructions must be based on the results of project studies, the form in which they are presented to the operators must be adapted to the reality of their behaviour in the power station. The simulator constitues an essentiel tool in verifying this compatibility and for making any corrections which may be necessary.

The most difficult problem which we have encountered is that of training operators to deal with severe accidents. These accidents have a low probability of occurence, by reason of the safety measures incorporated into the design, but they can nevertheless occur and the behaviour of the power station will then depend directly on the action taken by the operators. In order to provide this training, the simulators must be capable of representing the behaviour of the plant realistically in very serious situations. A major commitment has been made in France to the development of such simulators.

It should also be noted that whilst training invariably involves an individual aspect, with each member of the operations team being prepared for this particular task within that team, it is also desirable to have training exercises in which the team as a whole is required to demonstrate its capacity to operate the plant, even in extreme situations.

These "simulated situation" exercises are now being provided in EDF. They provide a valuable insight into the behaviour of operations teams, and in particular have confirmed the very positive contribution made by the principle of "human redundancy" provided by the presence of the safety engineer (ISR) in the control room during an accident.

Although the incidents analysis does rarely make bring out a human factor from maintenance, it is obvious that we must not neglect it. As for operators, an important training programme has been set up for maintenance staff. This training consists of a first part related to the general operation of the plant, taking into account the fundamental safety policy (technical specifications) and of a second part of technical training or improvement, general or specific for each job and for various equipments and systems.

7.4.2 - Experience Feedback Files

In order to analyse incidents occuring in service, it is essential to be able to compare similar incidents and to this end the EDF Thermal Generation Division sets up an "events file" from the start of plant operation. This file is used at the power station to store the following information in partially coded form to facilitate sorting and data processing :

- Significant incidents : these are events for which the selection criteria have been agreed with the Safety Authorities. These events are brought to the attention of EDF management and Safety Authorities within 48 hours by telex.

- Safety related events : the selection criteria, which are broader than the above, are specified by EDF.

This file also facilitates monitoring of the progress of studies and the implementation of modifications.

Section 3 discusses the use of probabilistics methods in safety, but in order to apply these methods it is necessary to have "reliability data" on the equipment and if possible on human factor. EDF Thermal Generation Division has set up a system for collection of reliability data (SRDF).

This system monitors the principal items of equipment which may influence the reliability of systems, and also availability (approximately 600 plant items monitored). For each monitored item, the file contains the following data :

- annual record of operation giving the number of operating hours and/or the number of operations,

- a record describing each failure.

However, the requirements for collection and processing of "human reliability" data are much less clear-cut : failures are extremely difficult to identify and the number of situations in which these failures may be committed is very difficult to determine. Nevertheless, a human reliability data bank has recently been set up. This data bank contains information on failures reported during normal operation and particulary during simulator testing during which it is also possible to evaluate the occurence of situations.

7.4.3 - Organization of Quality

The inservice quality organization is applied to all "monitored quality" activities or equipment (important for safety or availability). These activities are carried out by "qualified" personnel based on written documents prepared in advance, and are reported in writing. The activities are checked by personnel different from the personnel performing these activities, with reference to the technical aspect (quality control) and management aspect (quality surveillance).

The organization of quality is consistent with the legislative order of 10 August 1984 (so-called Quality Order), with the recommendations of the IAEA Code 50-C-QA and with the Fundamental Safety Rule V.2.a.

The principles of quality organization are laid down at national level in the "Basic Rules" and the "National Manual of Quality Organization". Each central services unit, nuclear generation centre or nuclear power station within Thermal Generation Division adapts and amplifies the national documents in their own Quality Organization Manual supplemented by organization notes.

The scope of these activities includes : management of documentation ; operation, inspection, monitoring and maintenance of systems and equipment ; treatment and discharge of effluents and waste ; procurement, reception and storage of equipment ; treatment and discharge of effluents and waste ; procurement, reception and storage of equipment ; recruitment, training and qualification of personnel ; fuel, and the treatment of incidents and anomalies.

7.4.4 - Safety Monitoring

The structures, methods and facilities described above should provide a guarantee of Safety, but it will still be necessary to ensure that these arrangements remain effective and do not deteriorate over time. To this end, monitoring activities are carried out at various levels :

- In addition to his primary role as manager of the plant in the event of an incident (see para. 7.2.2.3) the Safety Engineer is permanently present on site. He has a duty to monitor observance of all safety requirements, and also performs the important task of educating and training operators.

- The nuclear inspection department of Thermal Generation Division carries out detailed surveys on all aspects related to safety. The information gathered is presented to the plant management and to the Thermal Generation Management.

- Also, the Safety Authorities (Central Department of Nuclear Installations Safety under the Minister for Industry, aided by the CEA Institute of Nuclear Protection and Safety) also carry out periodic inspections on our installations. In addition, they receive all incident reports from each power station.

8 - CONCLUSION

In the foregoing we have attempted to describe the experience acquired in France in the area of nuclear safety of pressurized water reactors. Over the last fifteen years we have developed an approach to safety which is particular to us, but which remains within the context of general objectives which we feel enjoy a broad consensus at international level.

In conclusion, we propose to summarize the principal lessons which we have learnt from the Chernobyl accident.

After Three Mile Island, we embarked upon a programme of action which yielded a substantial improvement in the safety of our power stations. The cornerstone of this programme was prevention of severe hypothetical accidents, with particular emphasis on reinforcement of the containment of radioactive material, and consideration of the human factor, with the accent on training of personnel, observance of procedures, organization of operation and improvement of the man-machine interface.

In addition, with the structures established, the feedback of operational experience still plays a vital role and should enable the safety of all French nuclear power stations to be maintained at the highest level. The principal results of our activities in this sphere are presented in this document.

Analysis of the Chernobyl accident confirms the correctness of this philosophy. Of course, this does not mean that the Chernobyl experience has no lessons for all nuclear operators, who feel challenged by the most serious accident which has ever occurred at a civil nuclear installation , but the lessons are of a different order. Firstly, Chernobyl provides a dramatic reminder that nuclear energy involves serious potential risks ; accidents, albeit less serious than that affecting the Ukranian reactor, may happen at our power stations : if we wish to prevent these accidents effectively, we must all be fully aware of them.

Chernobyl has also provided some extremely important information on the problems encountered in the management of major radioactive accidents ; all nuclear operators and the public authorities alike are involved here, and would want the Soviet Union to provide as much relevant information as possible.

Indeed, the major impact of Chernobyl is probably not of a technical nature, but rather lies in the shock felt by public opinion in the majority of countries.

We cannot ignore this, and nuclear operators have a role to play in the task of restoring necessary public confidence in the safety of our installations.