TRAINING IN MANAGEMENT AND ANALYSIS OF SEVERE ACCIDENTS

ORGANISED BY FRANCE

IN THE FRAME OF THE
INTERNATIONAL ATOMIC ENERGY AGENCY
TECHNICAL COOPERATION PROGRAM
(HUN/9/013)

BUDAPEST

13 - 24 JANUARY 1992

4 ACCIDENT MANAGEMENT

4.1.1 ACCIDENT MANAGEMENT STRATEGIES MEASURES AND EMERGENCY PROCEDURES

I A E A INTERREGIONAL TRAINING COURSE

ON

ACCIDENT MANAGEMENT IN NUCLEAR POWER PLANTS

22 May - 16 June 1989

Argonne National Laboratory

CHICAGO UNITED - STATES

OPERATING PROCEDURES FOR EMERGENCY SITUATIONS in EDF PWR plants

Gérard DEPOND (EDF SPT FRANCE)

Lucien RESSE (EDF SPT FRANCE)

ELECTRICITE DE FRANCE

Service de la Production Thermique
Département sûreté nucléaire

16 Esplanade Charles de Gaule
CEDEX 57
92 060 PARIS La Défense

FRANCE

INTRODUCTION

Analysis of incidents and accidents occuring at French and foreign power plants - particular the TMI accident - and the commissioning of many units in France, as well as tests o simulators, have all demonstrated that an improvement of safety in nuclear power units depend largely on the improvement of the man-machine interface and particularly of emergenc operating procedures (EOP). EDF has taken numerous actions in this direction, especially sinc 1979. First of all, in improving the classical approach based on event-oriented procedures :

- Rewriting of initial accident operating procedures with regard to their technical conten their form, and the organization of the operating team (procedures I and A).
- Extension of initial procedures into areas at the limits of design basis and beyond the desig basis limits (procedures H).

Nevertheless, this approach is subject to several weaknesses

- dependance on a precise initial diagnosis,
- impossibility to take into account all the conceivable accidental situations,
- discrepancies between the predicted pattern and the reality.

These drawbacks of the event approach have led us to revise the technical conception of th EOPs, and to develop a new approach based on a continuous monitoring of the physical states o the plant and the ability to define a relationship between the physical state of the plant and th operator actions.

Electricité de France (EDF) has applied this new approach in two successive steps :

- First, by improving the existing procedures and introducing procedures based on physica states, but which only act through making up for failures of event-based procedures. This i the first generation of physical state procedures (SPt-U1).
- Secondly, EDF and Framatome (manufacturer of the NSSS) verified that it was possible t completely replace the event-based procedures by a set of physical state procedures. Thi second generation of new-design procedures is called generalized physical state procedures.

More generally, developments for emergency situations can be classified as follow:

1. Event-based procedures
2. State approach with event-procedures
3. Generelized physical state procedures

1. Event-based procedures (I-A)

1.1 General

These procedures deal with design basis incidents (I procedures) and accidents (A procedures).

Different working groups have been set up since 1980, bringing together manufacturers, operators, and method engineers.

It rapidly became necessary to break down procedures into two separate documents :

- Emergency Rule Guidelines call ERGs (theoretical contents).

- Emergency Operating procedures call EOPs (practical contents).

These event-related procedures have been improved in terms of their contents and form. The operating rules are drawn up by the specialists in incident and accident functioning. These rules have three different objectives.:

- They serve as a repository for technical options, chosen on the basis of realistic accident analysis, that enables optimization of action sequence. Actual experience is factored in whenever possible.

- They form a document that can be used as a training aid for learning the instructions.

- They form the basis for drafting the operating procedures.

The operating procedures for immediate use by the operator in the control room are drafted on the basis of the operating rules.

1.2 Improvement in technical contents

The post-accident procedures available to the operator up to 1980 were based on a pessimistic sequential analysis of "envelope" accidents, used for the dimensional calculation of protection and safeguard systems.

The area covered by I and A procedures has been progressively extended to include :

- all initial unit states for each conceivable incident or accident : from full power to cold shutdown,

- all conceivable break sizes and types(primary, secondary breaks , steam generator tube ruptures) which may or may not lead to startup of the safety injection system ,

- situations which take into account a more realistic behavior of the NSSS, and not merely result of conservative envelope studies.

Moreover, the main operating strategies used for all procedures have been standardized and optimized : natural circulation operation according to available systems, operation in case of breaks in the steam generator tubes, etc.

Procedures for Loss of ELectrical Supply

A special working group, set up in 1980, defined the procedures to be applied in the various cases of electrical control source and power supply losses - particularly the procedures to be used to reach the safest shutdown state according to the remaining available systems. This group has also been designated to perform minor modifications to improve nuclear safety in these situations and have been continuously improving the procedures taking into account experience feedback.

Entry to the Emergency Operating Procedures

The initial diagnosis of the event that occurs after safety injection actuation is effected by using the special AO procedure.
Confirmation of the diagnosis is requested at the beginning of each EOP.

Studies were carried out in 1984-1985 to define a logic of diagnosis (analogous to AO) to cover all accident procedures, on the basis of about 70 important alarmes specifically indicated in the control room. This new procedure (called DEC) provides two major improvements in the diagnosis :

- It allows for a specific order of procedures according to the degree of damage in the specific situation.

- When a large number of alarms appears (which is frequent after an emergency shutdown, for example), it helps the operator not to forget any of the important alarms that allow for accident diagnosis. Consequently, the risk of errors in diagnosis is greatly reduced.

1.3 Improvements in the form and organization of operating procedures

The operating procedures should always be as clear and direct as possible to avoid any confusion or ambiguous interpretations, and they should be written in the operator's own language. The final document is a product of numerous sessions on the simulators to test the effectiveness of several possible forms.

These test series, performed in 1981, also helped define the form and writing (vocabulary, typography) of the instructions, as well as the organization of the operating team.

In the event of an accident, the application of an EOP requires the following in the control room :

- a control room operator who mainly operated the primary system and associated safeguard systems,

- a control room operator who operates the SG and, more generally, the secondary system of the power unit,

- a shift supervisor who coordinates these different operations and monitors the key points.

Each participant has his own instruction sheet.

1.4 Extension of event-based procedures to complementary conditions:

Within the framework of improvement in general safety level, additional devices and procedures have been defined to perfect the area of design bases.

EDF and its partners have established a complementary field of operation, historically called "beyond design", providing when necessary additional means of mitigating an accident which escapes the mesh of the single failure criterion. Suitable operating procedures and complementary means have been worked out to cover such accidents.

The so-called H Procedures basically represent situations related either to short term loss of frequently used redundant safety systems or to the medium and long term loss of safegard systems involved in accident sequences initiated by a LOCA.

H1 procedures cover total loss of heat sink or of the systems ensuring heat transfer to it. In this situation heat removal is ensured by the steam generators (with AFW system) if primary circuit is closed, or by primary boiling and compensation for evaporated water (with CVC system) if primary circuit is open.

H2 procedure covers total loss of steam generator feedwater. It consists of feed and bleed configuration when low level in steam generators and high core exit temperature criteria have been reached.

H3 procedures covers total loss of emergency power supply. When primary circuit is closed : residual heat removal is ensured by steam generators feeded by auxiliary turbine driven pumps, and a complementary turboalternator group (LLS system feeded by steam generators) supplies power to the sensors and indicating devices required for operation and to the test pump of CVCS . When primary circuit is open , residual heat removal is ensured by primary boiling compensated by a gravity feed then by a complementary thermal motor driven pump from RWST.

H4 procedure covers total loss of LPSI or CSS during a LOCA in the long term. The principle is to arrange the two safeguard circuits in such a way the pump of the available circuit injects into the primary circuit the water from the containment sump, making use of mobile connections installed at the latest three days after the start of the accident.

The possibility of a deterioration of the situation described above has led to a study being made of scenarios extending as far as the total loss of LPSI and containment spray exchangers. Provision is to be made in this case for the installation of a mobile pump and a mobile exchanger (U3 procedure).

2. State approach with event-procedures:

This domain involves all situations not included in the accident configurations covered by the I, A and H procedures. This area is covered by procedures SPI, SPU and U1, based on the physical state approach. These procedures are designed to implement all means available - before the appearance of damage to the fuel - to avoid the most extreme damage.

To remedy the relative stalemate posed by the event-based approach EDF, in liaison with the French Safety Authorities, have developed a new operating approach since 1981, based on the physical states of the nuclear steam supply system.

Studies carried out in this area enabled the following :

- identification of all possible states of the nuclear steam supply system that are limited in number (contrary to event combinations).

- establishment of a diagnosis for the states, valid for each instant during the accident.

- establishment of a direct relation between each state and the required actions.

The first application of the physical state approach is introduced into the I, A and H procedures to make the criteria for action for the main systems (particularly the safety injection system) independent from the sequences of events and, consequently, from the initial diagnosis and from EOP chosen.

SPI, SPU and U1 procedures :

The purpose of the post-incident permanent monitoring procedures (SPI) is to detect at any moment and for whatever the causes, whether the EOP I, A or H being applied is no longer effective. This consists of a permanent diagnosis.

- either to follow up and, where necessary, to confirm to the operator the main actions already called for in EOP I, A or H in progress (if the initially diagnosed configuration follows its course normally),

- or, to ask the operator for limited complementary actions, but without abandoning the procedures in progress, in the case of some cumulative faults,

- or, in very degraded situations, to order the operator to abandon the EOP in progress and to apply the U1 procedure.

In the latter case, the U1 procedures directly defines, on the basis of the physical states of the NSSS and with the means available, the actions required on the main systems to prevent, limit, or delay damage to the core and its radiological consequences, depending on the severity of the situation. In conjunction with the operating team using the U1 procedure, the safety engineer carries out the ultimate permanent surveillance (SPU) to provide a human redundancy.
SPI, SPU, U1 procedures have been operational in all EDF PWR plant since 1985 - 1986.

3. Generelized physical state procedures (called APE procedures)

The organization of the above-decribed I, A, H, SPI-U1 procedures permits, at any moment and under any circumstances, to ensure maximum safeguard of the core without calling into question event-based operations.

Nonetheless, this organization has several weaknesses : SPI and U1 actions are sometimes not well optimized for unit equipment, when core safety is not directly in jeopardy, the SPI procedure does not always provide the aid expected by the operator, who cannot simply apply his own procedure (in case of multiple events).

The generalized state approach can solve these problems. Procedures ECP1 to 7 for primary system operation, in conjunction with the ECS procedures for secondary system operation, provide exhaustive coverage of all NSSS states.

Figure 1 shows in a severity / complexity diagramm, how both generations of operating procedures cope with accidental situations

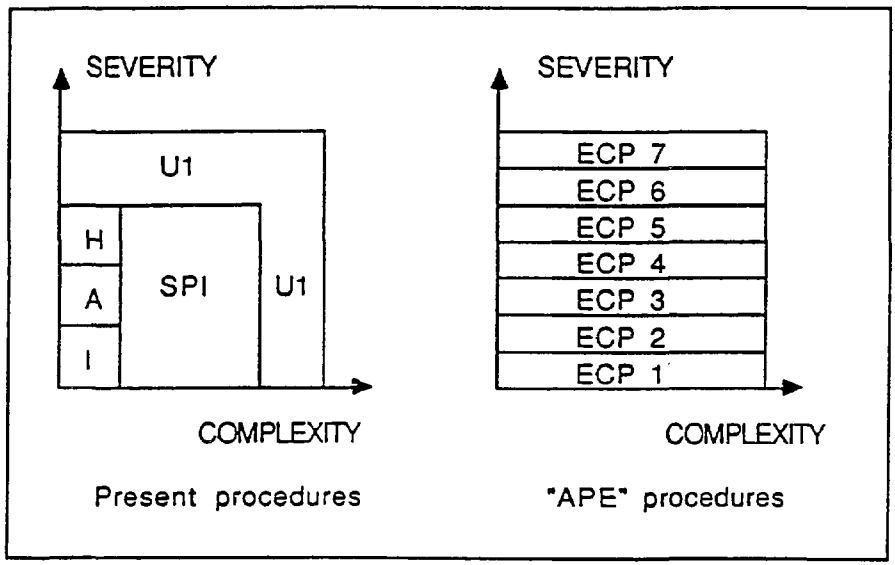

Figure 1 - HOW EOPs COVER ACCIDENTAL SITUATIONS

3.1 Objectives and method of "APE" procedures

This new approach was investigated with the following objectives :

- definition, at any time, of a direct relationship between the physical states of the plant and the operator actions.
- possibility to account for a modification of the diagnosis during the accident (permanent diagnosis).
- possibility to manage all possible situations, including multiple failures.

Theoritical studies carried out by EDF and FRAMATOME from 1980 on, in close collaboration with the Safety Division of CEA since 1982, led to the definition of the successive steps which permitted to implement the method :

- definition of the informations required to characterize the physical states of the primary, secondary, containment and the safeguard systems availability.

In particular, it was shown that the physical states of primary system could be described by using the Reactor Vessel Level Instrumentation (RVLI) and the subcooling margin (difference between the maximum core outlet temperature and the saturation temperature).

The influence of different situations (primary pumps on or off for instance) and environment conditions (containment temperature for instance) taking the precision of the necessary informations into account was studied.

- definition of the functional objectives (primary coolant inventory control, residual power transfer control, subcriticality control for the primary side for instance) and selection of priorities between these objectives in correlation with the states of the plant, thus giving to the operator the necessary indications to start the adequate actions in the right priority.

- identification of physical states of plant requiring the same types of actions, if any, in order to define limits for the actuation or termination of different components and systems and thus to gather all the plant states into a limited number of configurations.

3.2 Organization of physical state ERG's documents

The physical state approach gets organized around :

- one guideline for verification of the proper operation of the automatisms (called EV).

- one guideline for continuous monitoring of all state parameters in order to carry on state diagnosis leading to the choice of the guidelines for the primary and secondary sides.

- 7 guidelines for primary side (ECPI 7)

- 2 guidelines for secondary side (ECS1-2)

- 1 guideline for containment ECE

- 1 guideline for system monitoring ESS

and a permanent monitoring post incident APE guideline (SPE) allowing the Safety and Radioprotection Engineer to confirm the main safety actions dictated by the APE procedure used by the operators, to survey state-parameters and to decide the necessity to abandon the current procedure for a higher level one (these procedure ECPi are ranked in order of increasing plant degradation). Distribution in control room of these procedures is given in figure 2.

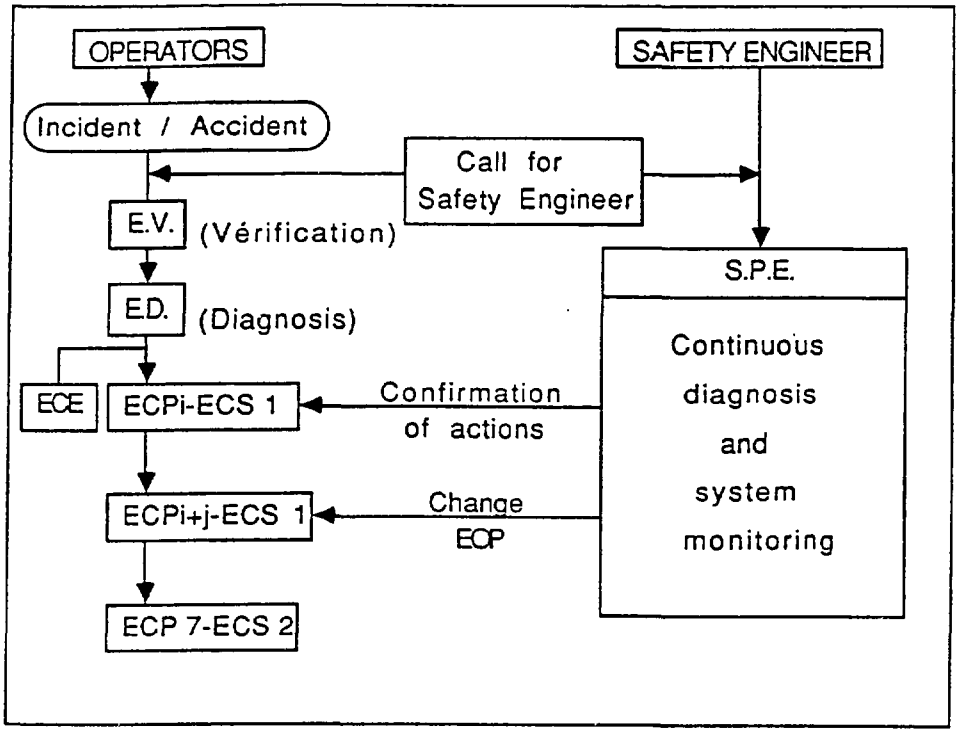

Figure 2 - ORGANIZATION OF "APE" EOPs

3.3 Structure of physical state ERG's documents

These documents are self-carrying and allow the operator to reach a stable and safe reactor state without changing of procedures, if no more plant degradation occurs.

They are structured in the following way :

- immediate actions
- orientation criteria towards different operating sequences
- operating sequences : each can be composed of several phases

Figure 3 shows an example of this structure.

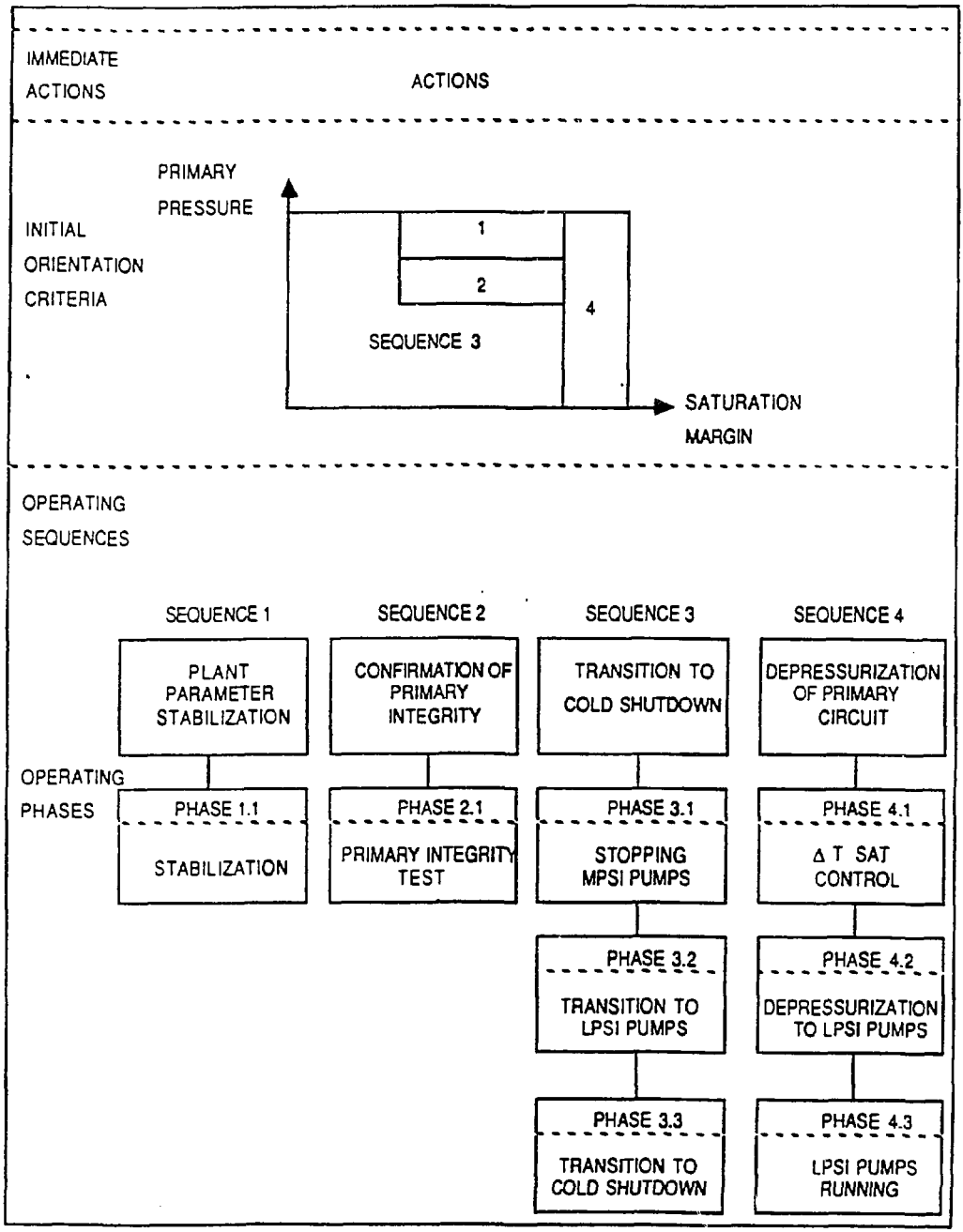

Figure 3 STRUCTURE OF A PHYSICAL STATE ERG'S DOCUMENT

In each phase, the need to linearize operator's actions for operational reasons and the necessity to continuously adapt the actions to changes in the reactor state have been combined in a looped structure which is shown in figure 4.

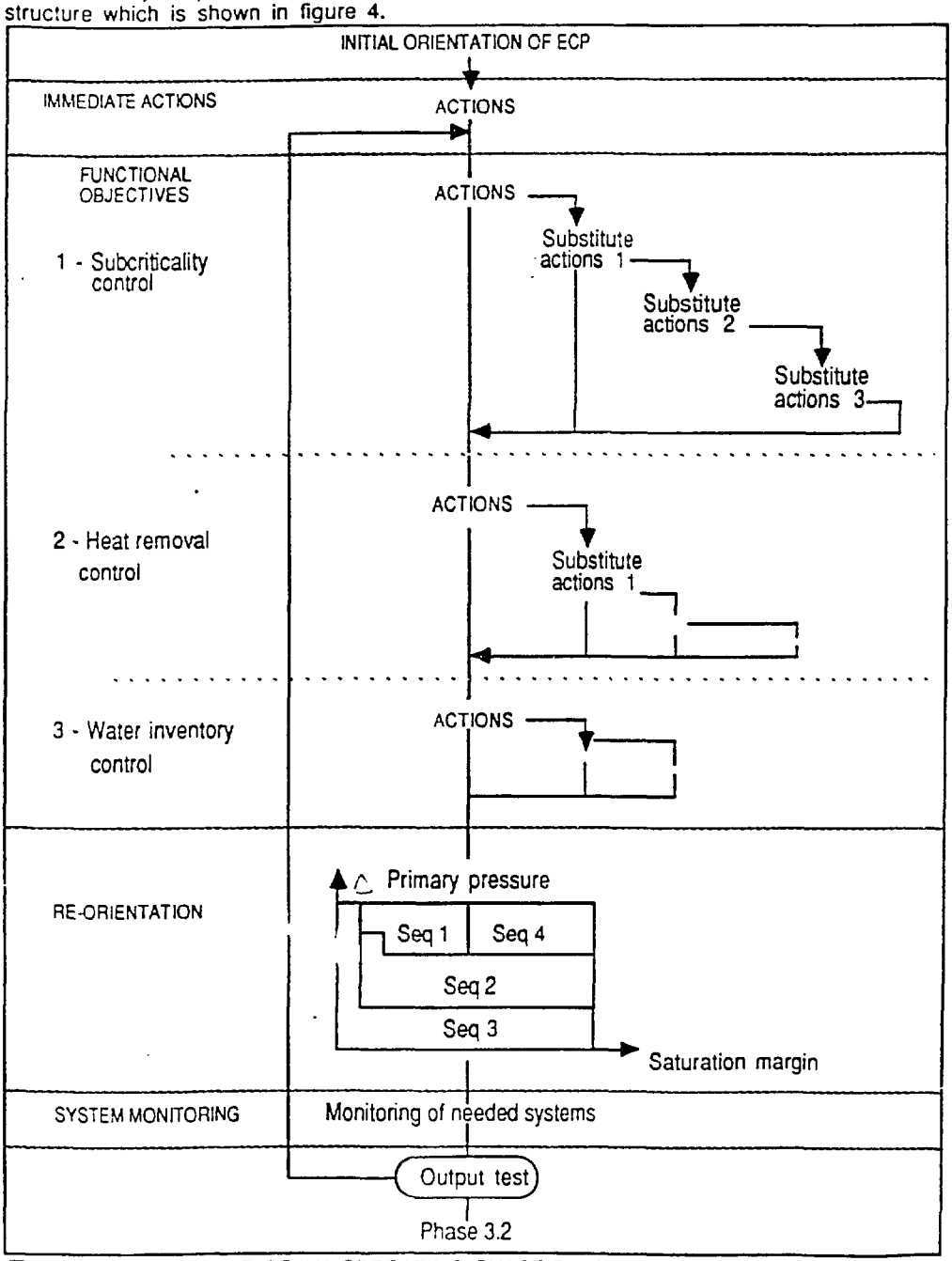

Figure 4 - STRUCTURE OF AN OPERATING PHASE PHASE 3.1 : STOPPING MPSI PUMPS

Each phase includes its own operating and functional objectives (the priority between the functional objectives depends upon the whole plant state and can vary from one sequence to an other one), its own specific means with continuous monitoring of needed systems, a re-orientation grid which allows the operator to decide to stay in the same phase or to change phase or sequence with the variation of the reactor state.

The continuous monitoring of systems used in an operational phase allows the operator to detect possible failures. The operating documents advise the operators of a substitute solution to keep moving toward the phase's main objective and in parallel to call for appropriate restorations.

The solution consists of the utilization of substitute systems in order of ease of use and possible counterpart on the installation or applying another sequence or procedure or ignoring the corresponding actions if its impact is not significant for safety.

These substitutions constitute a fundamental aid because they never allow the operator to be confronted by an unforeseen situation.

In conclusion, this looped structure enables operation to be adapted to the state of the NSSS at any given moment. Reciprocally, it also enables monitoring of the evolution of physical states at a reorientation level, given the efficiency of the actions which have been carried out.

3.4 Tests and practice on full scope simulator

By the end of 1987, 15 series of tests with around 20 operator teams, have been carried out, representing a total of approximately 500 hours.

The simulator tests have shown that, by following these procedures, all "single" accidents (primary or secondary system breaches, steam generator tube rupture etc...) can be controlled very efficiently. This also applies to any combined accident, including combined losses of a large number of systems. Approximately hundred different scenarios have been successfully tested, more than eighty of them corresponding to multiple accidents or incidents, either simultaneous or successive.

The operators very quickly place confidence in these procedures, which appear simple and reassuring because :

- a solution is always proposed, whatever the combination of equipment and/or human failures involved (use of subsitute systems).

- it is easy to check, at any given moment, that the sequence of operations under way is appropriate to the situation, however complex (use of periodic reorientation criteria); the operators thus have at their disposal an auto-correction tool.

3.5 Application of the second generation physical state EOP's

In view of the many tests already carried out with operating teams and the very positive results of these tests, it is now considered that the new physical state procedures constitute a particularly powerfull tool for controlling accident situations on PWRs, ranging from the simplest to the most complex.

The new generalized physical state procedures will be applied in the PWR 1300 MWe units from 1989 and will then be extended to the PWR 900 MWe.

3.6 Improvement of Measurements

As demonstrated in the Three Mile Island accident, the effectiveness of operation under accident conditions essentially depends on control room measurement capability. A comprehensive review of the measurements necessary for implementing the new approach was carried out and indicated the need for the measurement of additional parameters such as :

- A reactor vessel level based on redundant sensors of the pressure difference between the top and the bottom of the reactor vessel.
  In addition a digital treatment and a permanent cross-validation process between the redundant reading of subcooling margin and reactor vessel level gives the most reliable measurement for display in the control room.

- A new method to detect the activity of the steam passing through the steam generator lines, available when the reactor is under power or shutdown.
  This system has already been finalized and tested with success on reactors with primary to secondary leaks, and will be progressively implemented in all the reactors.

3.7 Operator Aid

In units of the 1300 MWe series, the operators have a data processing system which can be used for aid in applying procedures. A study has been performed to define and create functions for aid in application of physical state procedures. The study is scheduled to be completed in 1989.

Units of the 1400 MWe N4 series are provided with a computerized control room and a preliminary study has been performed with the assistance of the Commissariat à l'Energie Atomique (CEA) concerning on screen display of physical state procedures which is to be tested on a full scope simulator (S3C) in 1989.

4 Conclusion

All the emergency procedure steps implemented by EDF demonstrate the idea of in-delph defense, from the application of incident and accident operating procedures to the utilization of resources designed to limit the consequences of serious accidents within the scope of internal emergency plans, while maintaining a coherent approach with environmental measures.

These steps also indicate the care taken to account for all risks of error or an anomaly chain by providing for, in call cases, surveillance and procedural resources appropriate to the accident situation in progress.