TRAINING IN THE 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

JANUARY 13 - 24, 1992

COMPUTER AIDS FOR PLANT OPERATORS

Jean-Paul JOLY
Operating Department
Electricité de France
Paris, France

TABLE OF CONTENTS

1 INTRODUCTION

For some time, particularly since the TMI accident, nuclear power plant operators have been aware of the difficulties involved in diagnosing accidents and returning plants to their stable, safe operating mode.

There are various possible solutions to these problems:

- improve control organization during accident situations,
- rewrite control procedures,
- integrate safety engineers in shifts,
- improve control rooms, and

- **implement additional computer aids.**

The purpose of this talk is to describe the efforts undertaken by EDF over the last few years in this field.

2 THE ADVANTAGES OF COMPUTER AIDS

While maintaining present instrumentation and control tools, computer aids offer the following processing capabilities:

- improve the man/machine interface in a conventional control room with a "reduced automation" level;
- provide control room operators with synthesized information structured on a priority basis;
- introduce additional automatic processing procedures that are impossible with conventional equipment;
- supply crisis teams, operating outside the control room, with on-line information on the unit status @ without impeding operators' work;
- obtain diagnostic redundancy by the different members of the crisis team (on or off site).

3 SELECTING A COMPUTER AID

In an accident situation, operators use two types of information:

- vital information for the application of accident procedures,
- non-essential information provided to facilitate analysis.

The digital equipment used depends on the type of information provided.

3.1 Vital information (type A)

This type of information is supplied by qualified equipment (1E or 2E, code ASME).

This hardware must satisfy the following:

- functional requirements (factory and on-site validation and verification of software packages);
- equipment requirements (equipment design constraints - RCC.E);
- reliability requirements (constraints related to mission losses and spurious orders).

This hardware is exclusively simple, specific, **programmed controllers** (operating in either 1/2 or 3/4). They tend to be **purpose designed.**

This hardware has been installed in selected 900-MWe PWR plants. The most recently installed equipment is the core cooling and reactor vessel level monitoring system, which enables measurement of the level of water in the reactor vessel, maximum temperature of the core outlet and the subcooling margin (▲T SAT). This hardware is vital for applying state-by-state approach procedures.

3.2 Non-essential information (type B)

This type of information is provided by non-qualified systems, which are thus subject to less stringent requirements. The level of hardware reliability will depend on the design specifications imposed by the operator.

This hardware comprises more complex computer systems than type A, and is **programmable and highly open-ended.** They tend to be **standard products.**

This hardware is not safety qualified. In case of unavailability, the usual control methods based on qualified hardware can be used as a backup.

More hardware has been installed at plants than type A and notably includes the following elements:

- the safety panel (KPS),
- the environmental impact control system (KGE).

While this hardware is easy to install, it has a less clearly defined status and is not always used by operators, who tend to limit themselves to qualified equipment.

However, this hardware is extremely important, indeed vital, for personnel not directly involved in accident control operations (in particular Crisis Teams).

Some computer aids, despite their high level of performance, have remained at the prototype stage and have not entered widespread use. This is the case of:

- the power supply monitoring expert system (KSE).

4 WHERE TO INSTALL A COMPUTER AID AND WHO SHOULD USE IT

Under accident conditions, three categories of personnel are involved in diagnosing unit status or in plant operation:

- operators (in the control room),
- the safety engineer (in the control room),
- experts (in the Local and National Technical Crisis Centers).

All of these staff members must be given access to computer aids.

Present-day technology enables qualified hardware to be installed only in the control room. This hardware can therefore be accessed only by operators and safety engineers.

Only non-qualified hardware is linked to external equipment. Therefore, the safety panel is equipped with four panels/consoles:

- two in the control room,
- one in the Local Technical Center,
- one in the National Technical Center.

5 WHEN TO USE A COMPUTER AID

It is essential that operators be fully conversant with the computer aid in order to be able to use it correctly in accident situations. Given that operators must cope with the stress of an accident situation, it is hardly the appropriate time for them to "discover" the product and have to deal with any dialogue difficulties.

The computer aid must therefore offer functions enabling it to be used under normal operating conditions. These functions should include:

- ensuring compliance with technical operating specifications,
- the overall safety status of the installation.

We will see later that these functions have been included in the safety panel.

6 COMPUTER AIDS DEVELOPED BY EDF

Two types of hardware have been developed by Electricité de France:

- qualified hardware (type A),
- non-qualified hardware (type B).

Three hardware packages are detailed below:

- **Type A:**
  - the core cooling and reactor vessel level monitoring system (currently being installed at EDF's 900-MWe PWR plants);
- **Type B:**
  - the safety panel (installed at all plants);
  - the power supply monitoring expert system (KSE) (still model form, and not in general use);
  - the environmental impact and effluent control system (KGE) (under development and scheduled to be installed shortly).

6.1 Core cooling monitoring system

6.1.1 Description

The core cooling monitoring system is a digital device that indicates the status of the primary coolant and measures the water level in the reactor vessel.

This system is designed with a redundancy factor of 2. The readings and data processed in each computer are reciprocally validated at all time. They are transmitted to the centralized data processing system (KIT) and the safety panel (KPS). The KPS uses this data to assist the operators in applying the procedures.

Each core cooling monitoring system receives the following data:

- 8 in-core instrumentation system temperature readings at the core outlet,
- 1 in-core instrumentation system temperature reading under the cover plate,
- 1 reading of the pressure difference between the top and bottom of the reactor vessel,
- 1 reading of the primary coolant pressure,
- the state (on/off) of the primary pumps.

Using these data, the two monitoring systems calculate:

- the in-core instrumentation system maximum temperature,
- the core subcooling margin (▲T SAT),
- the margin under the cover plate ("bubble" monitoring in the case of thermo-siphoning),
- the reactor vessel water level.

Status indicators show whether the core subcooling margin is sufficient or overheated. An indicator shows which data are not validated.

6.1.2 Installation

All data (status indicators or digits) can be read on the mimic board just above the two color KFD displays.

6.1.3 Experience feedback

The core cooling monitoring system is currently being installed at all EDF's nuclear power plants and is already in service in 1300-MWe PWR units using state-by-state procedures.

When these systems were brought on line, difficulties were encountered in correctly calculating measurement systems. This problem has since been solved.

In general, operators have widely accepted these systems, since they do not require value access dialogue. The core cooling monitoring system is used according to the state-by-state approach procedures. Since it is qualified hardware, operators place great trust in this equipment, which is far from the case for the KPS (safety panel).

6.2 The safety panel (KPS)

6.2.1 Background

To improve assistance to operators in dealing with the risk of human error, a computer aid known as the Safety Panel, or KPS, was developed.

- 1980
Preliminary studies began, geared towards assisting post-accident monitoring by bringing together all the necessary safety-related information in a comprehensive structure, defined on a priority basis.

- 1982
The different functions for assistance in diagnosis, control and monitoring of non-specified units were defined. The hardware was selected and writing of software packages got under way.

- 1983
The Safety Authorities stipulated that the monitoring of all electrical supply sources be taken into account. This extended the functions of the safety panel to many non-accident situations.

- 1984
The first functions were tested on simulators.

- 1985
All CP1 and CP2 900-MWe PWR units were fitted with the first functions.

- 1986
These units and a simulator were connected to the National Technical Crisis Center.

- 1991
Additional functions are under development, scheduled for implementation in the near future.

The development of this project required the participation of all EDF departments involved in safety:

- Nuclear and Fossil Generation Division
- Research and Development Division
- Plant Design and Construction Group

6.2.2 Presentation of the Safety Panel

6.2.2.1 Composition

The control system comprises three important elements:

- status indicators
- core cooling monitor
- computer hardware.

Two rows of status indicators are directly connected to the wired logic of the different protection hardware. On each of the two redundant channels, the status of the main safety functions is indicated: safety injection, turbine trip, reactor trip, etc.

Core cooling monitoring systems: these determine the reactor vessel level, the maximum temperature of the core outlet (T RIC MAX) and the subcooling margin (ΔT SAT).

The safety panel, KPS: this acquires, processes and displays information. It comprises three consoles:

- Operator station: 2 color semi-graphic screens and one keyboard. It is an active console, which enables processing validation and activation. The two screens can perform the same functions.

- Safety engineer's station: comprising 1 screen, 1 keyboard and 1 printer. It is also an active console. The Versatec printer can also be controlled by the operator console.

- The Technical Crisis Center (TTC) console: this comprises 1 screen, 1 keyboard and 2 Versatec printers. This console is for consultation purposes only.

The National Technical Crisis Centers are equipped with a screen and printer giving them access to all safety panels installed on site, and thus to the KPS at the site where the accident has occurred.

6.2.2.2 Location

- The operator console is located at the end of the front Front Panel near the primary coolant monitoring and control tools.

- The safety engineer's console is also located in the control room, but is deliberately placed outside the control zone. The safety engineer is thus able to perform his duties of monitoring the activities of the control team without interfering with its work.

- The TCC console is located in the Technical Crisis Center where the crisis teams, composed of plant operation specialists, work.

- The NTCC console is locared in Paris where the national crisis team works.

6.2.3 KPS functions

6.2.3.1 Objectives

The functions incorporated in the KPS must perform the following tasks:

- Identify all protection and safety actions and display them in chronological order.
- Monitor the progress of automatic actions and conformity of the safeguard systems with technical specifications.
- Aid in safety injection diagnosis and control.
- Display changes in the main safety parameters.
- Identify and locate the impact of power supply losses.

6.2.3.2 Developed functions

. Identification of the initial fault

This function gives the operator:

- in chronological order, the faults which triggered the protection and safety actions;
- reports on the correct or unsatisfactory progress of these actions.

Processing begins as soon as a cause or order to activate the safety systems has been detected. The "initial fault" image appears automatically on the operator console screen at the start of processing.

The image supplied by the KPS give the following information:

- Elapsed time since the startup of the Safety Injection.
- Identification of the channel which ordered activation of the automatic protection system.
- The reference of the protection command.
- Origin of the order.
- A report of the progress, per channel, of each action requested.

. Safety actuator monitoring

This function consists in presenting the following in block diagrams:

- position of the safety valves,
- any discrepancies with reference status,
- their availability (identified by monitoring their power supplies).

The reliability of information supplied is indicated. Information is said to be "certain" if the data transmission polarity is operating. .

The DEF function key enables display of block diagrams which identify at least one safety valve revealing either discrepancies or faults.

This monitoring function can be used under all unit states. It is extremely useful for monitoring compliance with technical operating specifications.

The KPS currently counts 11 block diagrams:

- reactor coolant systems (2)
- containment isolation (3)
- steam-water system (1)
- turbine generator (1)
- containment spray (1)
- safeguard auxiliaries (1)
- power supplies (2).

The following has been agreed for block diagrams:

- If the information supplied is not "certain", the safety valve is shown in magenta.

- If the safety valve reveals discrepancies with its design position, it is shown in flashing red. If, in addition, these upstream resources are not available, it is shown in red (not flashing).

- If the safety valve is unavailable and the availability data is certain, a red square is placed alongside the valve. If the information is uncertain, the square is shown in magenta.

. Assistance in diagnosis and AO accident procedure selection

As there are multiple causes of an SI, a concise diagnosis must be provided for the operator. This diagnosis is currently performed using the AO procedure. This procedure directs the operator towards other control procedures.

The operator performs this procedure for the first five minutes, during which the instrumentation and control system prevents the operator from stopping the SI.

The images are only available five minutes after the appearance of an SI order. .There are three types of images:

- type A: this contains the triggered procedure, the unit status, possible operation actions and confirmation of the choice of procedure;

- type B: this gives the results of the different tests which allowed the final procedure to be obtained;

- type C: this provides an operating history of the procedures determined by the process.

. Assistance in safety injection control

This function helps the operator to assess whether he can or must reduce or increase the safety injection. A series of images is provided according to the procedure under way. These images comprise backgrounds, which vary according to the status of the installation and the result of the diagnosis. The following can be distinguished:

- green areas: reduced SI
- red areas: increased of SI
- blue or white areas: maintain application of procedures.

The image shows the evolution of the operating point over the previous 30 minutes.

There are five types of images:

- Pressurizer/subcooling margin level (▲T SAT) (scale of 0 to 75°C)
- Pressurizer/subcooling margin level (▲T SAT) (scale of -20°C to 55°C)
- Pressurizer/time level
- SI rate/time level
- Reactor coolant pressure/Tcore (RIC - in-core instrumentation system).

. Continuous monitoring of plant status

This process monitors the progress of the operating point of the rector as regards pressure and temperature. The authorized field appears, and varies according to the condition of the reactor. The image shows the progress over the previous 10 minutes.

This function is frequently used under normal operating conditions.

There are five authorized operating fields:

- RRA (Heat Removal System), not connected, at least 1 reactor coolant pump in operation (normal conditions)
- RRA (Heat Removal System), not connected, in thermosiphon mode
- RRA (Heat Removal System), connected, at least 1 reactor coolant pump in operation (normal conditions)

- RRA (Heat Removal System), connected, reactor coolant pump in idle mode (normal conditions)
- RRA (Heat Removal System), connected, reactor coolant pump and primary coolant T >70°C (incident mode).

Depending on the images, additional information is displayed:

- P steam generator
- Core temperature change over time

. Residual heat removal system (RRA) monitoring

This process enables detection of malfunctions in the shutdown heat removal system.

This function is frequently used under normal operating conditions, and is particularly useful during servicing of the water chamber of the steam generators.

The image is divided into two sections:

- the block diagram, which shows the main parameters of the system. For each actuator, data is provided on its position, safety, discrepancies, availability and availability certainty;

- the processing of monitoring during servicing of the steam generators: it checks the primary coolant T at <70°C and primary coolant ▲T/▲t <1°C/min.

. Safety function monitoring

The process is intended to assist the crisis team as regards installation status. It enables monitoring of the analog magnitudes of the safety systems, the evolution of which is shown as a curve y = f(t) for the previous 30 minutes.

Five main functions have been defined:

- monitoring of the nuclear power (2 images)
  (supply chains and intermediate chains)

- heat removal from the core (6 images)
  (N primary, T primary, T RIC, ▲T subcooling margin - ▲T SAT, etc.)

- (heat removal by the secondary system (3 images)
  (Pression and Level steam generator, Q Feedwater Flow Control System or Auxiliary Feedwater System)

- mass of the primary coolant (1 image)

- integrity of the containment (5 images)
  (activity, P containment, T containment).

Each image comprises a maximum of 5 curves.

. Control-aid synthesized image

This process is composed of a computer-generated image representing the main parameters of the primary coolant system. **This function is frequently used under normal operating conditions.**

Detailed description

The image comprises two sections:

- an alarm strip, showing the status of:

  . power supplies
  . cooling water
  . primary cooling system
  . containment monitoring
  . primary pumps
  . tanks
  . reactivity.

If no anomalies are detected, an overall report (OK) appears.

- block diagrams, showing the following information:

  . the mass of water entering and leaving the core
  . core parameters
  . pressurizer level
  . status of pressurizer heaters
  . status of relief and spray valves
  . status of primary coolant relief tank.

. Other functions

Other functions are available, but are not described in this document. These include:

- aid for the application of the SPI procedure (used by the safety engineer)
- aid for the application of the tag-out procedure.

6.2.4 Functions under development

Other functions are currently being developed and should be implemented in coming years. These include:

- an operator guide, enabling training of operators in the man/machine interface dialogue;
- an aid for the application of SPU/U1 procedures.

It takes a long time to implement these vital developments in all EDF units. Between the decision to go ahead and actual installation at the first unit, three years can elapse, due to the complexity and rigorous nature of the design process chain. It would be difficult to reduce this time, since data validation is a lengthy process.

Maintaining this software at EDF's 900-MWe PWR units requires the standing presence of:

- 1 engineer at the Plant Design and Construction Group
- 1 engineer at the Generation and Transmission Group
- 3 technicians at the Generation and Transmission Group to manage the data
- 1 engineer per site.

6.2.5 Hardware architecture

The computer hardware comprises two sub-assemblies:

- level 1: acquires and pre-processes data
- level 2: processes data.

6.2.5.1 Level 1

Level 1 functions are:

- acquire all data: 4,500 on/off (acquisition time: 40 ms) and 1,200 ANA (acquisition time: 5.20 or 60 seconds);
- process on/off signal inhibition: on/off output is inhibited following power supply loss for corresponding acquisitions.

Level 1 functions are performed by two computers, powered by two different sources operating as main and backup supplies. The central processing unit is a Sintra Alcatel CLX-S.

6.2.5.2 Level 2

Level 2 functions are:

- validate the analog signals and additional processing;
- monitor the alarms; filing and display of data;
- manage the operating terminals (4).

Level 2 processing performed requires the permanent calculation of more than 2,000 logic equations. Level 2 functions are performed by a Solar 16/65 computer.

6.2.6 Costs

The following costs were calculated on the basis of 1987 fran values:

The cost of the entire project for 900-MWe PWR units (34 totalled FF146 million, including FF11.4 million for R&D.

This cost does not include liaison with the National Technica Crisis Centers. The present configuration represents a cost c FF2.7 million. Functions under development are estimated to cos a further FF4.5 million. The cost of first training programs fc this product totalled FF2 million.

6.2.6 Experience feedback

The safety panel has been in operation since 1985 at all 900-MW PWR units.

6.2.6.1 Functional experience feedback

Experience feedback is difficult to define accurately, since fortunately, there have been very few accident situations However, we can draw several conclusions as regards the function used under normal operating conditions and functions unde accident conditions through use of the simulator.

Actual use of the safety panel varies according to the users:

. The operator thinks that has little need to use the safet panel in an accident situation. His or her actions are focuse on "paper" procedures, which moreover require the use o qualified equipment only. The low level of use can be traced to

- The computer aids used and control procedures are not ver complementary. "Paper" procedures have not been modifie since the introduction of the safety panel. Therefore, i an accident situation, the operator can choose whether t consult the KPS or not.

- The image design is very similar to the "paper" procedures Therefore, any modification in procedures requires a chang in the computer data.

- The data updating process is often very long (2 to 3 years) Some functions no longer fully comply with desig specifications.

- The system is non-qualified, making operators reluctant t use it.

- The computer system has been introduced in a conventiona environment.

- The lacking of training

. The Safety Engineer regularly uses the system under normal operating conditions for safety actuator monitoring as per of the technical specifications. In an accident situation, the Safety Engineer uses the SPI procedure and watches the safety panel to check his diagnosis.

. The crisis teams, who have much less information available since they are not in the control room, recognize the importance of this product in providing concise, validated data.

6.2.6.2 Equipment experience feedback

This equipment is not qualified in terms of ASME codes. However, it offers an availability rate of more than 99.7% for five to six interventions per year.

The use of the safety panel processes under accident conditions demands rigorous validation of logic equations. Furthermore, each new version of the program must be tested, verified and validated.

Some functions can be validated at the manufacturer's. But others can only be tested on the full-scale simulator, as it is the only device capable of simulating all the logic equations.

6.3 Environmental monitoring system (KGE)

The KGE system is a computer aid which enables a concise display of the environmental impact of gaseous releases from nuclear power plants. It can be used in real accident situations or during simulation exercises.

The environmental impact and effluent control system is scheduled to be implemented at all sites as from mid-1992.

Composition of the system

In an accident situation, the National Technical Crisis Center is directly involved through its role as advisor. There are two levels of crisis management:

- local: at the nuclear site
- national: through the National Technical Crisis Center.

Local computer facilities comprise four stations:

- 2 graphics workstations at the Health Physics Crisis Center (HPCC) (on site)
- 1 graphic workstation at the effluents laboratory (on site)
- 1 workstation at the environmental laboratory (off-site).

National computer facilities comprise 2 graphics workstations similar to those at the HPCC.

Operating functions

The functions defined in the KGE must perform the following:

- calculate the extent of released effluents,
- evaluate the propagation of these effluents,
- assess the possible diffusion (function not yet developed).

These calculation results must be displayed in two ways:

- through an "environment message" containing meteorological data, the extent of the release, measurements taken within the plant environment and the estimated radiological impact;
- propagation charts: graph representation of the propagation of the effluents.

Conclusion

This equipment, which does not require qualification, is considered to be a vital aid for members of the crisis teams during accidents. It offers concise, pertinent running information and, furthermore, relieves the operator of manual or repetitive tasks, while also reducing the risk of error.

6.4 On-line monitoring of power plant electricity supplies (KSE)

EDF wanted a more accurate system for on-line monitoring of electricity supplies in its nuclear power plants. A prototype, known as KSE, was thus developed to monitor the power supply systems at the Bugey 2 unit. This system runs on a computer using artificial intelligence.

6.4.1. Development

- 1984-85
Start of research into expert systems for operator aids.

- 1986
Initial tests on a full-scale simulator, revealing the benefits of expert systems.

- 1987-88
Development

- 1989
The prototype was brought on line at the Bugey 2 unit in November.

- 1991
Review of operating experience.
Decision taken not to implement this system at all plants.

6.4.2 Operating functions

This system is a computer aid for monitoring a plant's electricity supply systems. It is used for:

- real-time processing of events caused by power supply system failure;
- preparing for the removal from service of electrical equipment;
- training operators in the optimum use of the plant's electrical distribution system.

6.4.3 Advantages of the KSE

The KSE system offered many advantages:

. Integrated tool, thereby ensuring efficiency and quality.

. Simulation tool, available for training or preparation for removal components from use.

. Highly accurate identification and diagnosis of unit states.

. Accurate diagnosis even with multiple failures.

. Full graphics display, with good man/machine interface. The unit can be monitored even during shutdowns for refueling.

. It was developed in cooperation with nuclear power plant operators, who in effect made their own product.

6.4.4 Drawbacks of the KSE system

The following drawbacks identified on the KSE system prevented EDF from introducing it on a broad scale on French nuclear power plants:

. The system is not and cannot be qualified, making it impossible to integrate it with emergency procedures.

. As a new computer aid in the control room, with its own screen and keyboard, it introduces block diagrams and dialogue quite different to existing computer aids.

. It represents a new alarm processing system for the control room.

. It has a new database, which the plant staff must keep up to date. This represents many man/months of work. The Bugey 2 plant encountered numerous difficulties in the implementation of the database.

6.4.5 Conclusion

Although this computer aid is technically perfect, this is not enough to justify widespread implementation in control rooms. Other factors have to be taken into consideration:

- Integration in the control room.

- Definitions of the respective elements of computer aids, conventional tools (e.g., indicators, "paper" procedures, etc.) and operators.

- The already large number of different types of computers installed in plants.

- The number of databases which must be regularly updated - and the vast amount of work involved in this process.

6.4.6 Costs

Completion of this prototype required:

- 22 man/years by EDF
- 2 man/years by the Energy Division of the Sema group (subcontractor).

7 CONCLUSIONS AND RECOMMENDATIONS FOR SUCCESS

7.1 The capabilities of computer aids

To be accepted, accident management computer aids must meet the following objectives:

- Be useable in both accident and normal situations.

- Under normal operating conditions, provide assistance for compliance with technical specifications, thus offering major safety gains.

- Under accident operating conditions, provide valuable assistance for non-operating staff, such as the Safety Engineer and the Crisis Team, in diagnosing and monitoring the evolution of the accident.

- In an accident situation, allow operators to check their own actions.

7.2 Restrictions

- A sufficient amount of data must be collected (ANA or on/off) in order to obtain validated information and sophisticated processing capabilities. It would be advisable to take this opportunity to install a centralized data processing system which can be used under normal operating conditions, if this has not already been done.

- Ensure that the system is available and carry out periodic checks on its availability.

- Carry out detailed studies on the impact of the tool on the control room and, above all, on accident procedures. These instructions and the definition of images to be used should be completed at the same time.

- Ensure that a simulator enable activating all the functions of the safety panel.

- A rigorous data management system must be implemented, capable in particular of verifying and validating all logic equations. The computer aid is an open-ended product, which must be constantly updated as regards the status of the installation.

7.3 Pitfalls to avoid

- Avoid developing images that simply copy "paper" instructions, as operators tend not to use them. Only synthetised images represent a veritable operator aid.

- Do not think that once the system has been installed it is complete and requires no further development. Maintaining

it up to date with unit status and "paper" instructions calls for a permanent team of experts.

- Avoid using different staff to develop the computer aid and define "paper" instructions.

- Do not seek to qualify the product.

- Ensure that appropriate training actions are provided to support the product.