ANALYSIS OF INCIDENTS involving

COGNITIVE ERROR and

ERRONEOUS HUMAN ACTIONS

Issued December, 1990

A report prepared by a Task Force of Principal Working Group No. 1 of the NEA Committee on the Safety of Nuclear Installations

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY
38, boulevard Suchet, 75016 Paris, France
CSNI PRINCIPAL WORKING GROUP No. 1

TASK FORCE 7:
Analysis of Incidents Involving Cognitive Error and Erroneous Human Actions
COMMITTEE ON THE SAFETY OF
NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA), is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop and coordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international cooperation in nuclear safety among the OECD Member Countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organizations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the coordination of work in different Member Countries including the establishment of cooperative research projects and international standard problems, and assists in the feedback of the results to participating organizations. Full use is also made of traditional methods of cooperation, such as information exchanges, establishment of working groups, and organization of conferences and specialist meetings.

The greater part of the CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant incidents.

In implementing its programme, the CSNI establishes cooperative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regards to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.
SECTION 1

1. Introduction

In 1987, Task Force 7 of CSNI Principal Working Group 1 produced an initial report (Ref 1) concerning reactor events involving misinterpretation/misunderstanding of the plant status by plant staff. That first report was based on a brief review and analysis of a number of IRS event reports in which errors of interpretation or understanding occurred. The aims of that first phase of the Task Force's work were to:

(a) Assess the potential significance of such erroneous actions to current plant safety.

(b) Provide information on the underlying causes for such actions.

(c) Comment on measures that may be effective in preventing such actions.

Based on the available IRS reports, a number of preliminary issues were identified and discussed in the report but the group felt that a rather more detailed analysis of a small number of incidents might be a useful extension of the Task Force's work. Accordingly, in September 1988, Task Force 7 started a second phase of their work in which 5 incidents were to be reviewed in some detail with the objectives of:

(i) Raising awareness of the potential for cognitive error by illustrating particular erroneous actions and indicating typical causes of such actions.

(ii) Providing information about erroneous human actions with the aim of helping IRS co-ordinators to identify and record relevant data from incidents involving human actions.

(iii) Providing a preliminary commentary of the effectiveness of defensive measures taken to reduce the impact of cognitive errors.

This report summarises the second phase of the Task Force's work and should be read in conjunction with the first report. Section 2 of this report gives a brief description of the 5 events, plus some analysis of the event causes. Section 3 provides additional analysis of the causes contributing to the actions made in those specific events based on the group's discussions. Section 4 contains a discussion of causes particularly aimed at generalising those causes which are seen to have wider applicability. Finally, Section 5 discusses potential defensive actions which may be relevant to mitigating the causes identified in Section 4.

SECTION 2

2.1 - INCIDENT IN THE NPP BIBLIS A, 17 DECEMBER 1987

Start up of the plant with first check valve in the pipe connecting one train of the emergency core cooling system to the reactor coolant system not closed.

2.1.1 Event Description

Before the event the plant had been in cold shutdown for about 3 days to repair a leaking weld of a condensate collection tank in the secondary circuit. The residual heat removal was performed by 2 of the 4 trains of the ECC/RHR-system with the RCS temperature at 70°C and the RCS pressure at 30 bar.

After finishing the repair work the plant was started up on 16 December 1987. Before increasing the pressure the 2 operating trains of the RHRs had to be taken out of service and switched to the ECCS mode by procedure. This was performed by the responsible operator from the RHR/ECCS control panel in the control room. During this task two things happened nearly at the same time:

- To provide RHRs suction from RCS hot legs during RHR mode the first check valves (isolating the RHR/ECCS trains from RCS hot legs in standby mode) are kept open by motor actuators in the operating RHR trains. When the operator tried to close the check valve TH22 S006 (see figure) of the second operating train, the CLOSED position of the valve was not indicated by the valve's position indicator. The same happened after a second attempt to close the valve.

- When an RHR/ECCS train is switched from RHR mode to ECC mode, the pressure in the train has to be released to the RWST via a test line prior to connecting the LPSI pump to the RWST. This step was forgotten by the operator. Since one of the 2 operating trains was connected to the sampling system, this train was already depressurised through the sampling line before connecting the LPSI to the RWST. But when connecting the second train to the RWST by opening the motor valves TH20 S001/2, the safety valves TH20 S090/94 opened and released a small amount of reactor coolant to the annulus. This caused with some delay the release of Iodine 131 and noble gases to the annulus and from there to the stack. The release was well within the allowed limits.

Since the operator did not give any information about the problems with the check valve in the second train to the shift supervisor, start up of the plant was continued. Furthermore the shift staff didn't properly respond to the alarms related to the misposition of the check valve on the CRT and the computer print-out.

During shift turnover, all alarms present at that time and documented on a respective computer print-out have to be discussed with the new shift. But the alarm related to the check valve position remained unnoticed during the next 2 shift turnovers.

About 14 hours after plant start up, and one hour after synchronising the turbine generator to the grid, a High Temperature alarm was received from a filter unit in the CVCS. After some investigations, the open check valve TH22 S006 releasing hot coolant via the relief valve TH22 S008 to the let down line of the CVCS, was recognised.
The shift supervisor decided to shutdown the plant to close the check valve and test its proper function. However, at a power of 100 MW, an attempt was made to close the check valve by providing a differential pressure across the valve. For this purpose, the valve TH52 S002 in the test line of that RHRS/ECCS train was opened for 7 seconds, but the check valve did not close. The test lines are designed for recurrent testing of the LPST and HPST pumps of the RHRS/ECCS and for depressurisation of the system before switching to the ECC mode. The pressure relief at conditions not foreseen in the design (158 bar and 300°C instead of cold water with less than 110 bar) caused the actuation of the safety valve TH50 S091 in the test line outside the containment releasing primary coolant to the annulus. Again, the amount of airborne radioactivity released through the plant stack was well within the allowed limits.

After the plant had been brought to cold shutdown, the check valve could be closed and successfully tested. Thereafter, the plant was started up again.

2.1.2 Human Behaviour Considerations

From the human behaviour point of view there are 3 areas of interest in this event:

- the behaviour of the operator responsible for the nuclear systems,
- the problem of recognising the stuck open check valve, particularly during shift turnover,
- the decision to open the test line with the primary check valve of the respective ECCS train stuck open.

These aspects shall be discussed in more detail.

2.1.3 Behaviour of the Operator Responsible for the Nuclear Systems

As mentioned above, the operator had to close the primary check valve in the hot injection line when switching an RHRS/ECCS train from RHR mode to ECCS mode. For this, the motor-operated stem of the valve lifting the valve disk device for RHR mode and keeping it in the open position has to be closed by the motor to release the disk device. The valve disk will then close by its weight. The positions of the motor operated stem and the disk are shown by separate indication lights on the control panel.

When the operator closed the stem to close the valve disk, the position indication of the stem changed to "Closed", whereas the indication of the valve disk remained in the "Not Closed" position. The operator immediately recognised that and tried to close the valve by opening and closing the stem a second time. But again, the position indication of the valve disk remained in the "Not Closed" position. At this point, the operator stopped his efforts with respect to the check valve and started the next activity. He did not inform the shift supervisor about the problems with the check valve, too. Some minutes later, when the primary pressure exceeded 32 bar, there was an alarm both on the CRT and the computer addressing the "Not Closed" position of the primary check valve. The operator, as well as other control room operators, did not properly respond to this alarm.

Afterwards, it seems impossible to identify the real reason why the operator recognised the "Not Closed" position indication of the primary check
valve, but in the end ignored it. Possible contributing factors and explanations are:

- Due to the setpoints of the protection circuits of the reactor coolant pumps the operating RHR trains have to be taken out of service in a short period of time during start up of the plant to prevent shutdown of the reactor coolant pumps.

- Apparently the operator did not assess the indication of a wrong check valve position as a safety relevant problem. Probably, he was convinced that the valve was in the closed position and that the position indication was wrong. Hints for such an assumption are:

- It was known from experience that it may happen that those check valves did not close when the stem was closed the first time. But moving the stem up and down again usually closed the valve disk.

- It was known from experience that the position indication had some sensitivity with respect to temperature. Thus, from time to time the position indication didn’t show the correct position at low temperatures. But at the operating temperature of the plant usually it indicated the correct position.

To some extent, this could explain why the operator did not inform the shift supervisor about the problem with the check valve, though it is the common understanding in the plant that a stuck open primary check valve during start up has to be reported to the shift supervisor, since the plant should not go to operation in such a situation. (It should be mentioned that the operator was characterised by his superiors as a careful and co-operative colleague.)

There are 3 possibilities to verify a closed primary check valve:

When depressurising the RHRS/ECCS, before switching it to the ECC mode with the primary check valve stuck open the system pressure should stay or decrease very slowly and the level in the RWST should increase, both indicating an open primary check valve. But since the operator missed to depressurize the RHRS/ECCS train he couldn’t get a hint by these indications.

In addition, an open primary check valve can be detected by measuring the temperature between the first and the second check valve, and by an alarm indicating the actuation of the relief valve TH22 S008 (see figure) in the line to the CVCS let down line. Both indications do not work until the RCS temperature is substantially above the temperature of the water in the RHRS/ECCS line and the RCS pressure exceeds the set point of the relief valve (110 bar). Thus, at the time the operator tried to close the primary check valve, there was no possibility to verify if the position indication failed or the valve itself.

There was no formal requirement in the plant to mark each step completed during start up on some kind of checklist. Thus, there is some chance that a step may be overlooked or a step not completed may be forgotten.

In addition, at that time there were no detailed instructions how to proceed if the position indication of a primary check valve indicated an
open check valve. Thus, it was left to the assessment of the operator how to proceed.

For an observer from outside the plant, there are some deficiencies in the practical application of the instructions regulating the responsibilities of the operators and the shift supervisor. It seems that too much responsibility had been delegated to the operators on an informal basis in the day-to-day work leaving to their decision when to inform the shift supervisor even in essential matters. Thus, it could happen that the shift supervisor did not become aware of important events like the stuck open primary check valve, because he relied on the operators and did not check those things by himself.

During situations like start up, the shift staff is subjected to high stress conditions due to the large number of tasks and tests to be performed, and alarms coming in and going off. In addition, real start up situations are becoming infrequent because of the high performance of the plants. Though plant start up is trained on the simulator with respect to stress, the real situation differs from simulator training.

The error of the operator happened in the seventh hour of that shift. It may be that there was some lack of attention for a short time.

As mentioned above, a second mistake happened when the operator omitted to depressurise the RHRS/ECCS trains before switching them to ECCS mode. In the first train, this mistake happened about half a minute before the operator became aware of the problem with the primary check valve. Because of the open sampling line no consequences occurred. (Thus, it may be concluded that this mistake did not directly influence the behaviour with respect to the primary check valve.) Missing the depressurisation in the second train happened some seconds after the operator stopped his activities to close the primary check valve in that train.

Plant start up is part of the operator training, including training at the full-scale simulator. In addition, depressurisation of the RHRS/ECCS has to be performed before the recurrent tests of the LPSI and HPSI pumps (one test per month and train). Thus, the operator was familiar with the actions needed to switch the RHRS/ECCS from one mode to another.

Again, it is difficult to identify the cause why the operator missed the depressurisation. Looking to the computer log, all of the following actions and mistakes happened in less than one minute: missing depressurisation in the first train, closing the stem of the check valve, opening and closing it again to close the disk of the check valve, misinterpreting the "Not Closed" indication and missing depressurisation of the second train. It seems that the operator performed his task quickly without properly checking all steps.

Possible causes or contributing factors for missing the depressurisation are similar to those discussed above:

- The operator felt very familiar with the task and performed it without looking to the detailed procedures.

- Pressure of time to avoid shutdown of the reactor coolant pumps.

- Lack of a formal instruction to each individual step performed in a checklist.
High stress situation

Some lack of attention at the end of the shift.

2.1.4 Problem of Recognising the Check Valve not Closed, Particularly During Shift Turnover

The wrong position of the primary check valve of the hot injection line of the RHR/ECCS train 2 was indicated by the position indication light of the valve disk on the RHR/ECCS control panel in the control room, and by alarms on the computer CRT and print-out. The information from the position indication light and the computer printout was available all the time (more than 14 hours) until the open check valve was discovered, due to the investigations to identify the cause of the high temperature alarm in the CVCS. During a period such as start up the alarm on the CRT disappears very fast from the display due to the large number of alarms (250-300 per shift). Thus, it was not available later on.

During shift turnover, a computer print-out of all alarms present at that time has to be discussed between the shift staff leaving the control room and the staff entering it. This is fixed in a formal instruction and should ensure that the new shift becomes familiar with problems still existing. The alarms on the print-out are ordered by systems. Thus, it is possible to separate the more significant alarms from the less significant ones without too much effort, even in situations such as start up.

Nevertheless, the alarm concerning the open check valve was not detected during the next 2 shift turnovers, though it was present on both print-outs. Possible reasons are:

- The instructions dealing with the discussion of the print-out did not fix in detail how to do that. In practice, the operators of the old and the new shifts discussed the print-out. The shift supervisor was not obliged to participate in that discussion and probably did not do that each time. (This is another indication that, in fact, some responsibility had been delegated to the operators on an informal basis.) Apparently, the discussion of the print-out was not very detailed. It seems that the operators of the new shift relied on the summary of their colleagues from the old shift, and did not check the situation by themselves.

- In addition to the organisational deficiencies, the position indication of the relief valve TH22 S008 failed because it was not properly adjusted. It should be mentioned that adjustment of this position indication is difficult due to the small stroke of the valve (2 mm). Thus, no alarm appeared in the control room when the RCS pressure exceeded 110 bar and the valve opened. Probably the operators would have recognised the open check valve if this alarm had not failed.

2.1.5 Decision to Open the Test Line with the Primary Check Valve of the Respective RHR/ECC Train not Closed

About 14 hours after plant start up and one hour after synchronising the turbine generator to the grid at 3 am (night shift), a "High Temperature" alarm was received from a filter unit in the CVCS. After some investigations, the open check valve TH22 S006 was identified to release hot coolant via the relief valve TH22 S008 to the let down line of the CVCS. At this time, the power of
the plant had reached 910 MWe. It was decided to shut down the plant to close the check valve and test its proper function with the plant in the RHR mode.

At about 5.30 am (half an hour before the end of the night shift), and with a power of 100MWe an attempt was made to close the check valve by providing a differential pressure across the valve. For this purpose, the valve TH52 S002 in the test line of the corresponding RHRS/ECCS train was partially opened for 7 seconds, but the check valve did not close. The shutdown was continued and the plant was brought to cold shutdown.

Investigations performed after the event show that the decision to open the valve in the test line with the first check valve not closed, and the RCS under full pressure and temperature, gives rise to safety concerns. One basic principle of reactor design is that there should be 2 valves to isolate the RCS from systems having a lower design pressure. The design pressure of the test line behind the valve TH52 S002 is 45 bar, that is much lower than the design pressure of the RCS (172 bar). Thus, with the primary check valve not closed, the low pressure part of the test line was isolated from the RCS just by the valve TH52 S002.

For the HPSI pump running (zero head about 110 bar, cold water) and the containment isolation valves erroneously closed the low pressure part of the test line inside the containment is protected against over-pressure by the safety valve TH50 S090. In combination with the orifice this valve is designed to limit the pressure in the test line to 45 bar.

When the valve in the test line was opened with the primary check valve not closed, water with 158 bar and more than 300°C was released to the test line. Assuming that the valve TH52 S002 failed to close, there would have been a loss of coolant to the RWST. To stop this loss of coolant, the containment isolation valves should have to be closed. But, subjected to hot primary coolant, the pressure drop across the orifice is much less due to a lower velocity of the hot medium and the safety valve TH50 S090 would not be able to limit the pressure in the low pressure part of the test line to 45 bar. A first assessment performed shortly after the incident without taking into account design margins of the system indicated that the pressure in the test line would increase to a value about 10 bar below the RCS pressure, that is 3 times the design pressure of the test line. With the first containment isolation valve in the test line 10 m outside the containment shell there would have been some probability for a rupture of the test line outside the containment under those conditions. In-depth investigations performed afterwards identified substantial as built margins in the system. Thus, even if one assumes the valve in the test line failing to close, the pressure in the test line actually would have been limited to a value, where the containment isolation valves would have closed properly and no threat for the piping existed. Therefore the probability of serious consequences has been very low.

When the shift decided to open the test line after discussion with the unit’s operation management, these problems had not been known. The main reason to decide to open the test line for some seconds was to try to close the check valve as soon as possible. Furthermore, no danger was expected because the shift staff was convinced that the valve in the test line would reliably close, as it did. (There had been very good operating experiences with this valve in the past.)

Asking for the reasons why the shift decided to open the valve in the test line, the following factors may have contributed:
The procedure did not give detailed enough instructions what to do when the first check valve is discovered to be open during power operation of the plant. Especially the procedure did not explicitly forbid to open the valve in the test line with primary check valve not closed.

There may be situations during operation of the plant where the shift has to perform actions not precisely described in the procedures, e.g. in the events having an unexpected sequence or during localisation of failures. This cannot be avoided completely. But apparently the procedures of the plant did not contain a sufficient frame of boundary conditions to follow in such situations.

It seems that due to the deficiencies in the procedures there have been corresponding deficiencies in the training of the plant staff how to react in such a situation.

The valves in the test lines have to be opened before each periodic test of the LPSI and HPST pumps, that is once per month and train. Thus, the operators are used to this action. Because of the good operating experiences with the valves, they relied on them and did not expect any danger.

The action was taken at the end of the night shift at 5.30 am after some discussion with the unit’s management of operation by telephone. At those times the plant staff, except the shift, is not available on the site. It may be that discussing the problem with the technical department would have resulted in a different decision. But that is difficult to tell, since the safety significance of the event did not become evident before the investigation performed later.

2.1.6 Conclusions

The event highlights 3 different areas of human failures:

(i) There are some causes that may have contributed to the errors when the RHR/ECCS from the RHR to the ECC mode. But, in fact, it was not possible to identify the actual causes. Probably one can learn from those events that such failures may happen. Therefore, measures should be taken both to reduce the probability of such failures and to cope with them.

(ii) An example of a measure to cope with such failures is the discussion of the computer print-outs containing all alarms during shift turnover. As can be seen from the event, this measure failed. This is more serious in our opinion than the errors. The reasons are deficiencies in the procedures and possibly excessive reliance on verbal information communicated from one shift to the other. Apparently, the operators did not verify what their colleagues told them. The same argument might hold for the shift supervisor, whose workload could be particularly demanding during plant startup.

(iii) The third area (decision to open the valve in the test line with the primary check valve stuck open) is an example of taking an action being unaware of all possible consequences. The main reasons that this action could happen are a lack of the procedures to provide a frame of boundary conditions which have to be followed in unexpected events, and some lack of training how to act in such situations.
Figure: ECCS Train 2 of 4 (Hot Leg)
2.2 - OSCILLATIONS AT LA SALLE UNIT, 9 MARCH 1988

2.2.1 Introduction

At 5:30 pm, the La Salle Unit 2 boiling water reactor (BWR) was operating at steady state conditions at 84% power. A personnel error by Instrument Maintenance Department personnel resulted in a pressure pulse that actuated the instrumentation which causes a trip of both reactor recirculation (RR) pumps in order to decrease power in the event of an Anticipated Transient Without Scram (ATWS).

Both RR pumps tripped, causing a flow reduction and a large rapid power reduction (about 45%). Control rods remained in the high power (92% Flow Control Line) position. This region of the BWR Power-to-Flow Map was known to be susceptible to instabilities in some BWRs. As a result of the large drop in power, as well as rapid changes in feed water control resulting from the original personnel error, the steam flow decreased resulting in large changes in extraction steam flow and extraction steam pressure. These changes in the steam flow and pressure caused severe perturbations in the feed water heater level control system. The high water level in the feed water heaters caused the extraction steam input to the feed water heaters to isolate to prevent the induction of water into the main turbine. This automatic trip of steam resulted in the temperature of feed water to the reactor decreasing by 45F in 4 minutes, the equivalent of a positive reactivity addition. This reactivity change increased the power-to-flow ratio and further reduced the margin to instability. All licensed operators at La Salle had been provided with guidance and training on how to recognise the onset of instability.

The control room personnel spent the first 20-30 seconds after the RR pump trip and associated ATWS alarms confirming that no condition existed which required a scram without a scram occurring. Having correctly determined that an ATWS event had not occurred, but that an instrument problem had resulted in the loss of both RR pumps, the control room operators were attempting to restore the feed water heaters. Approximately 3 minutes after the RR pumps tripped, the control room operators observed that the Average Power Range Monitor (APRM) indications were oscillating between 25% and 50% power every 2-3 seconds; the Local Power Range Monitors (LPRM) down scale alarms began to annunciate and clear.

The APRM indications confirmed the onset of instabilities and the operators attempted to start a RR pump in order to increase flow to leave the instability area. Attempts to start the RR pump were unsuccessful and the staff commenced preparations to scram the reactor. Before the staff was able to manually scram the reactor, the reactor automatically scrammed on high neutron flux seen by the APRMs. The automatic scram came about 7 minutes after the RR pumps tripped.

The calculated decay ratio for La Salle Unit 2 was 0.60 for this fuel cycle, meaning that the transient reactor behaviour observed during this event was not predicted to occur. This event may have resulted in the NRC General Design Criterion 12 being violated in that undamped power oscillations occurred and no procedures or methods were implemented to reliably and readily detect and suppress these power oscillations.
Although the major importance of this event arises because of its mere occurrence, the event has some interesting human factors aspects. It is the human factors aspects that are the focus of this report.

2.2.2 Analysis of the Event

The actual event that occurred at La Salle was benign in that there was no core damage. The NRC formed an Augmented Inspection Team to assess the root cause, safety significance, operator performance, adequacy of procedures, effects on reactor, reporting actions and potential generic implications. The results of their inspection are published as Report 50-3173/88008. In addition, the NRC Office for Evaluation and Assessment of Operational Data published a Special Report, AEOD/S803, AEOD Concerns Regarding the Power Oscillation Event at La Salle 2 (BWR-5) concerning the event. The analysis of the event that follows focuses on the operator behaviour, the available procedures, and operating training in general. It is based on statements in the AIT report and the AEOD special study.

2.2.3 Operator Actions to Restart Recirculation Pump(s)

When power oscillations of 25% magnitude (25%-50%) were observed on the APRM recorders, the Shift Engineer (SE) had arrived in the control room and assumed responsibility for efforts to recover from the oscillations. The AIT report states:

... operators all recognised that they were in the region of core instability, but were uncertain of what actions should be taken to leave the region of instability.

Thoughts were given to driving in control rods in sequence; using the "CRAM" array of control rods; starting a RR pump; or scramming the reactor.

The operators did not want to scram the plant if they could avoid it, and believed that driving control rods in, in sequence, would have been too slow. The use of the "CRAM" array of control rods with the RR pumps tripped and the feed water heating lost was not addressed in procedures, so that the operators were uncertain if they should use the "CRAM" rods. The operators therefore decided to try to leave the instability region by starting an RR pump.

The AEOD special report observes that a successful restart of a recirculation pump might have had potentially adverse consequences. With a downcomer filled with cold water and an unstable reactor, a successful restart would have led to additional rapid reactivity insertion. A calculation made by Brookhaven National Laboratory, using the BWR Nuclear Plant Analyser, showed that a calculated 0.5 dollars of reactivity was inserted just before the plant trip.

The AIT report states that

... It is also likely that if an RR pump had been successfully started, the reactor may have scrammed anyway on the resultant power increase ...

An author of the AEOD special study, a former licensed senior reactor operator, has also observed that he would expect a reactor scram if an RR pump was restarted under the conditions that existed at La Salle.
The AIT evaluated the procedures that the operators at La Salle had available at the time of the event. The reactor Technical Specifications (TS) required measures to place the unit in at least HOT SHUTDOWN within 6 hours be immediately initiated with no reactor recirculation pumps in operation. The La Salle abnormal operating procedures provided little guidance on what do after the onset of instability had been recognised, other than to specify that operators perform surveillances required by TS and get the reactor out of the region of instability. Interviews with the operators indicated that, although they recognised very well the onset of instability, they were confused and uncertain as to how to exit the region of instability.

The action of the operators to attempt to restart an RR pump was not the best corrective action that could have been taken. Rapid recognition by the operators that the start of an RR pump, although allowed by procedures and training, could likely result in a reactor scram, would probably have led the operators to initiate a manual scram rather than attempt to start an RR pump.

2.2.4 Procedures and Training

In 1984, General Electric issued SIL 380, Revision 1, BWR Core Thermal Hydraulic Instability. the SIL recommends that control rods be inserted if a recirculation pump(s) trip event results in operating at conditions where thermal hydraulic instability may be encountered. Since analyses had predicted that this type of event at La Salle would not occur, procedures had not incorporated the SIL recommendations and the operators had not been trained to respond to the event.

Although the possible occurrence of oscillations has been recognised at other BWRs few, if any, of the simulators used by utilities are capable of modelling the type of oscillation that occurred at La Salle. Hence, operator training on recognising and responding to power oscillations at all BWRs may be poor.

2.2.5 Other Aspects of the Event

The AEOD special report on the La Salle event notes that there are other concerns that arise from this event: the resolution of 2 generic issues, GI B-19, "Thermal-Hydraulic Stability" and GI B-59, "N-1) Loop Operations in BWRs and PWRs", may be inadequate; and previous efforts taken in regard to ATWS mitigation may be inadequate. These concerns arise because of the occurrence of the event and not because of the behaviour of equipment or personnel in response to the event.

In addition, both the AIT report and the AEOD special study focus attention on the fact that the calculated decay ratio for the La Salle core was 0.60, a value at which oscillations are not supposed to occur. The occurrence of undamped oscillations at La Salle implies a value of 1.0. The AIT report poses the question, "Have calculations been discredited as acceptable evidence of core stability?".

2.2.6 Conclusions

Review of the event highlights several contributory factors that impacted the ad hoc operator action:
1. Procedures and operator training concerning oscillations were inadequate. The licensee made a deliberate decision not to include procedures and significant training because on the calculated margin to safety and a sceptical attitude regarding the susceptibility of the La Salle reactors to instability. This scepticism may have been transferred to the operators and allayed their concerns about potential adverse interactions during the event. The original decision not to develop specific procedures for this situation was made at a higher organisational level than the reactor operators and had a significant impact on their capability to cope with the event.

2. There was a potential that certain operator actions could have worsened the event. It is unclear whether a successful restart of the recirculation pumps may have worsened the situation because of a sudden collapse of voids in the core. The Shift Engineer took responsibility for recovering from the incident as is his authority. The governing procedures allow him to make a determination about the need for immediate plant trip based on his judgement of the viability of the reactor protection system to contain the situation. Having made that decision, he must rely on his training and experience to direct an effective recovery. As noted in the event debriefing, the operators did not want to scram the plant if they did not have to. This undoubtedly coloured their judgement about what actions to take.

3. Out of phase oscillations could be difficult to recognise and could result in more severe consequences. Tacit reliance on calculations in the FSAR and other training material may induce a false sense of security when faced with a unique situation.

These concerns highlight the difficulties operators face in diagnosing and responding to these type of events.
2.3 - INCIDENT OF 20 OCTOBER 1986 AT BLAYAIS 3

2.3.1 **General**

During the incident of 20 October 1986 at Blayais 3, technical operating instructions were not complied with several times:

- The unit was brought out of normal cold shutdown while the breaker of the charging pump (which also acts as the high pressure safety injection pump) in train B was unplugged and the direct injection lines on the discharge side of the low pressure safety injection pumps were unavailable (safety injection valves RIS 61 and 62 VP closed).

- The unit was brought out of intermediate shutdown under residual heat removal system conditions without either the preceding faults having been corrected or the part of the reactor protection system (RPR) allowing automatic or manual safety injection tripping being available (switches RPA and RPB 216 CC open).

These faults were detected by the shift radiation protection and safety engineer (ISR) in the afternoon of 20 October, approximately 3 hours after his shift had started, whereas the reactor had in fact been brought out of cold shutdown at the end of the previous afternoon. About 20 hours had therefore lapsed before the abnormal situation described above had been detected.

In order to analyse this incident involving both technical and human aspects, a team including experts in both fields from Electricité de France and the safety authorities was set up.

Using an incident analysis methodological approach, the team tried to identify all the various aspects of the incident at an initial meeting with plant management following by separate interviews of the 3 shift teams involved in the event, as well as the Deputy Shift Supervisor responsible for overall plant shutdown planning.

2.3.1.1 **Sequence of Events**

It should be noted that during shutdown, lockout of the entire primary side "covered" the separate lockouts required for the different operations involved. The general lockout ended on 18 October 1986. Since the work being done on the primary system had not yet been completed and the procedure for filling the primary circuit was not clearly detailed, the plant condition did not comply with the technical instructions from approximately 10 pm on 19 October 1986 (when the plant was brought out of cold shutdown) to approximately 6 pm on 20 October 1986. The radiation protection and safety engineer then observed the alarm signals which had been present since cold shutdown.

2.3.2 **Incident Description**

2.3.2.1 **Failure to plug the contactor of the high pressure safety injection pump in train B (pump RCV O2 PO)**

The pump availability check was programmed at a date when it was not possible to leave the contactor plugged in as repair work was being done on the primary circuit.
When the work was completed, the pump breaker was not plugged in again.

This might have been detected in the periodic test performed in order to check that the safety injection pumps would operate correctly, but this test was scheduled under hot shutdown, therefore too late.

The unplugging of the breakers was signalled in the control room by a red alarm. This collective alarm also receives signals from the different breakers relative to the low pressure pump and 9 motor-operated valves belonging to the same train B.

This actual situation continued for 20 hours and, in the meantime, the reactor condition changed twice (from intermediate shutdown to residual heat removal system conditions, then to hot shutdown).

2.3.2.2 Valves closed on the direct injection lines (RIS 61 and 62 VP)

These valves are located on the discharge side of the low pressure safety injection pumps. They must be opened in advance in order to achieve injection line flow as soon as possible in the event of a major primary break. They do not receive any confirmation order to open upon the safety injection signal. It is therefore essential to position them correctly.

Valves RIS 61 and 62 VP remained closed when all the circuits were lined up again at the end of the plant shutdown because work was being carried out at the same time on the primary side of the reactor. Furthermore, they should be closed when the primary system is being filled with water.

They were not reopened at the end of this operation, possibly because the procedure followed was not sufficiently clear.

The erroneous position of each valve was signalled in the control room by a red alarm (these alarms each signal erroneous positions of 11 valves).

2.3.2.3 Unavailability of the system allowing manual or automatic safety injection tripping

Unavailability was due to the fact that 2 switches in the reactor protection system were in the open position.

The procedure describing the transition from hot to cold shutdown for refuelling explicitly requests the switches to be opened in order to prevent the risk of spurious safety injection during this period.

On the other hand, the procedure used for restarting the reactor following cold shutdown for refuelling does not mention that these switches should be closed. It indicates a general requirement for availability of the reactor protection system.

When the switches are open, neither automatic nor manual starting of the safety injection sequence is possible.

In compliance with technical operating instructions, the switches must be closed prior to isolating the residual heat removal system.
The abnormal position of the switches was signalled in the control room by alarms which were not heeded by the operators for about 4 hours following isolation of the residual heat removal system.

2.3.3 Potential Consequences

This incident's potential consequences are connected with reactor operation at pressure and temperature without safety injection and with a residual power corresponding to two-thirds of spent assemblies (since the plant was restarting after shutdown for refuelling).

The risks of a primary or secondary break during the restarting phase after shutdown for refuelling cannot be dismissed in view of the many operations which had just been performed.

If a break had occurred only the safety injection accumulators would have been available.

In view of the changes shown by any physical parameter involving the entry into service of the safety injection system, eg primary pressure, it is difficult to predict how soon the operator might have restored availability of the safety injection system:

- First he would have had to choose between two possible explanations:
  
  . The physical parameter changes were real and the safety injection system had therefore failed.
  
  . The physical parameter changes were not real and a sensor had failed which was not a protection sensor since safety injection had not been initiated.

- He would then have had to operate the actuators functioning upon the safety signal or to reclose the incorrectly positioned switches locally.

He would not then have been able to restart the second safety injection pump (pump RCV 02 PO), which would have had to be connected locally. Since no signal had been sent during the safety injection sequence to the valves located on the direct injection lines (RIS 61 and 62 VP), these would probably have remained closed.

It would have been difficult to detect the faults from the alarm signals present because of the high number of alarms involved, and the fact that they were grouped and had not been identified previously.

It would therefore have been difficult to restore the safety injection function rapidly. The possibility of major consequences for the fuel cannot be excluded in spite of the low residual power.

2.3.4 Analysis of the Causes

Each of the 3 faults mentioned was caused by a procedure implementation error but they all shared indirect causes connected with the following:

- Interactions between procedures implemented in parallel.
The line-up procedures were followed although not all the conditions required for them to be implemented fully were met, so that they had to be resumed later. Completion of the procedures therefore depended on the quality of the range data supplied by the previous operators.

Drafting inadequacies in the procedures, since some of the instructions were ambiguous.

Finally, the faults were not diagnosed in time owing to:

- An insufficiently precise re-starting procedure, which was difficult to apply.
- The absence of an overall view of the reactor condition before deciding to change it.
- The red alarm signals were not taken into account.

It should be noted that the conditions required in technical operating specifications for isolating the residual heat removal system were checked by a shift team with the assistance of the Radiation Protection and Safety Engineer, and that the operations required in order to obtain these conditions were performed by the next team in accordance with instructions, transmitted when the new team took over, without final checking.

2.3.5 Analysis of the Root Causes of the Failure to Appreciate the Plant Unit Condition

2.3.5.1 Repair work scheduling inadequacies

The schedule adopted required overlapping of several alignment procedures (RCV (Chemical and Volume Control System), RIS (Safety Injection System), alignment for primary system drainage), with an overall primary system lockout, compounded by a lockout for work on the emergency shutdown breakers. This required the interruption of certain operations, such as replugging in pump RCV 02 PO, opening valves RIS 61 and 62 VP, reconfiguring switches RPA and RPB 216 CC to 'ON' (otherwise any automatic or manual safety injection orders would be ineffective).

The phases of build-up to hot shutdown are governed by a certain number of procedures (G1: transition from normal cold shutdown to hot standby, FRCV 05 ...., FRIS 1: availability of RIS system ...). The implementation of these operations is however impaired by a failure to appreciate the risks of certain configuration sequences remaining incomplete, such risks being particularly high when tests are run in parallel (EP RIS 10 performed between 17 October and 18 October) involving several repair teams.

From this standpoint, the presence of an ISR (radiation protection and safety engineer), assigned to follow-up of the plant unit shutdown, would certainly have contributed to:

- awareness of potential safety consequences of repair work planning.
- assurance of a certain continuity with less risk of overlooking interrupted operations, the completion of which is nevertheless indispensable.
This provision has since been adopted.

In addition, the setting up of an appropriate structure would have contributed to the improvement of co-ordination between the various parties concerned and to highlighting risks of incompatibility between the different actions implemented here in accordance with an extremely tight schedule.

This provision has since been adopted, as a "Restartup Committee".

2.3.5.2 Procedure inadequacies

At the time of the incident, the procedures used comprised no provisions for checking that the conditions required by the technical operating specifications were actually complied with. 'Hold point scales' have since been introduced with a view to programming conformity checks at main standard plant station changes.

Moreover, some of the procedures used at the time lacked precision and could leave the operators in doubt as to the correct position of equipment.

Thus, for instances, procedure D20 indicated the following instructions for the reopening of the RIS 61 and 62 VP valves upon completion of primary system vacuum filling:

p.16: 'Then, end of test:
- align normally the valves on page 10'.

But on page 10, we find: 'RIS 61 and 62 VP closed'.

Similarly, procedure G1 for transition from normal cold shutdown to hot standby made no mention of resetting switches RPA and RPB 216 CC to 'ON'.

In general, the various procedures were ill-adapted to the programming of work among several shifts: specifications omitted, need to backtrack for additional data, absence of cross-references, etc.

It is important to stress the significance of the procedures as a data link between those who decide on operations and those who perform them. The quality and accuracy of the procedures depends, to a certain extent, on the efficiency of the organisational measures taken to provide against potential abnormal functioning induced by risky scheduling such as that observed here.

2.3.5.3 Aspects related to alarms

Obviously, alarms constitute a means of defence against risks of forgetting to reconfigure equipment correctly. In this respect, alarm design was notably deficient.

(a) Thus, the fact that alarm RPR 710 AA (yellow alarm requiring a 'delayable action') has indicated that switches RPA and ROB 216 CC are 'OFF' ('normal' position in view of the repair work on the 48V switchboards) practically throughout the entire plant unit shutdown, whereas this position was the required position, undeniably constitutes an obstacle to alerting the operators at the time when knowledge of this situation becomes pertinent.
(b) More preoccupying is the design of the RIS 502 AA alarm, which is one of the 'synthetic' type, concerning notably the RCV 02 PO pump: the fact that the alarm was on for most of the shutdown provided no indication as to pump RCV 02 PO availability.

This type of alarm is designed for essential functions, where summarising data made available to the operator is delicate'. The status of this type of alarm is ambiguous: from the basic principle standpoint, the 'synthetic' alarms are the sole exception to the rule whereby red alarms should not be grouped. Non-compliance with this rule is only justified in cases where:

- there is only one signal channel,
- prescribed operator action affects the same function,
- the signals can be easily differentiated by consulting recorders, indicators or the TCI.

The incident is a good illustration of the contradictions inherent in this 'synthetic' alarm design.

In the event of an alarm signalling function unavailability (here HPSI), it should appear if, and only if, this function is required in the context of the plant unit condition considered. Thus, the RIS 502 AA alarm should only appear if a fault affects the HPSI function during normal intermediate shutdown, hot shutdown or standby, or event power operation, but not during cold shutdown nor intermediate shutdown under RRA (residual heat removal) conditions. But, it does in fact appear because of the scheduled unplugging of certain RCV and RIS valves and pumps under these plant unit conditions. In particular, the alarm would have remained on, even if pump RCV 02 PO had been reconnected on 19 October, towards 10 pm, when the unit was brought out of normal cold shutdown. It was, in fact, only at 2 pm on 20 October that the alarm was to cease, when the RIS 033 and 035 VP valve cells were plugged in. (This being noted, it is however a fact that the alarm remained 'ON' from 2 pm to 6 pm on 20 October, ie for 4 hours, during which the HPSI function on Channel B was unavailable). The fact that it was 'ineffectively' actuated through the plant unit shutdown doubtless contributed to the impairment of its warning capacity.

Furthermore, the argument that other data are available (status indicator, KIT (Computer and Data Processing System)) has to be reconsidered in the light of the fact that access to such data implies acute operator awareness, involving consultation of the corresponding alarm data sheet. In other words, the more one becomes accustomed to seeing the display window alight, the less one is inclined to react against overlooking it.

(c) As regards the red alarms RIS 505 and 506 AA, relating notably to the RIS 61 and 62 VP valves, they feature the same drawback, in that they have been on continuously since 14 October, thereby blunting their operator warning capacity.
2.3.5.4 The problem of information transfer during Shift Change-over

Considering the number of system configuring sequences interrupted by shift changes, it is essential that the shift teams transmit essential data, notably that relating to incomplete actions (in the case considered, RCV 02 PO reconnection, RIS 61 and 62 VP valve opening, RPA and RPB 216 CC switch closing). The shift log and documents available in the lockout office are intended to meet this requirement. However, a question remains to be solved in a satisfactory way, that is: how to make sure that data is correctly transmitted over long periods, as in the case considered.
FIG 1 : GÉNÉRALITÉS SUR LES CIRCONSTANCES DE L’INCIDENT

RCV system alignment

14/10/86

15/10

17/10

18/10

19/10

22 H

ARRÊT

NORMAL

18 H

FROID

19 H

ARRET

INTERMÉDIAIRE

MONOPHASIQUE

INTERMÉDIAIRE AUX CONDITIONS DU RRA

ARRÊT

INTERMÉDIAIRE

NORMAL

ANNULAGE DU CIRCUIT RCV
LIGNAGE ET REQUALIFICATION DE LA POMPE RCV 02 PO
ELLE RESTE NON EMBOUCHÉE, DU FAIT DE LA CONSIGNATION MERE

ARRÊT

15/10

SIGNIFICATION MERE PRIMAIRE

CONSIGNATION MERE PRIMAIRE

RIS system alignment

LIGNAGE DU CIRCUIT RIS
LES VANNE RIS 61-62 VP RESTENT FERMÉES, DU FAIT DE LA CONSIGNATION MERE
Valves RIS 61-62 VP stay closed due to the overall lockout.

End of overall lockout

LEVIER DE LA CONSIGNATION MERE

1. POURBIOTE ET FIN DU LIGNAGE DU RCV

1. POURBIOTE ET FIN DU LIGNAGE DU RIS

18/18, 10H:

18/20, 10H:

FIN DU LIGNAGE:

10/19, 15 H

10/19, 15 H

LIGNAGE EN VUE DE LA MISE SOUS VIDE DU CIRCUIT PRIMAIRE

FIN DES TRAVAUX SUR LES DÉCONTIUS LE 18 AVRIL MIDI DU SDB

SWITCHES RPA, RPB 216 CC SONT EN POSITION H5

7 PERIODICAL TEST OF RIS 10

SWITCHES RPA AND RPB 216 CC SWITCHED ON THEN OFF AGAIN, REPAIR WORK ON EMERGENCY SHUTDOWN BREAKER

19 OCT. AFTERNOON OR EVENING

REALISATION DE L'USINE 17

LES COMMUTATEURS RPA ET RPB 216 CC SONT EN POSITION EN SERVICE

TRAVAUX SUR LES DÉCONTIUS PRINCIPAUX, ARRET D'URGENCE

LIGNAGE EN VUE DE LA MISE SOUS VIDE DU CIRCUIT PRIMAIRE

FIN DES TRAVAUX SUR LES DÉCONTIUS LE 18 AVRIL MIDI DU SDB

LES COMMUTATEURS RPA ET RPB 216 CC SONT EN POSITION H5

LIGNAGE DU CIRCUIT RIS
LES VANNE RIS 61-62 VP RESTENT FERMÉES, DU FAIT DE LA CONSIGNATION MERE

ARRÊT

NOMAL COLD SHUTDOWN

SWITCHES RPA AND RPB 216 CC ARE OFF

NOTES

Switches RPA and RPB 216 CC should have been turned off again.

CONTINUATION AND COMPLETION OF RCV ALIGNMENT

RCV 02 PO should have been plugged in again.

CONTINUATION AND COMPLETION OF RIS ALIGNMENT

Valves RIS 61-62 VP should have been re-opened.

DISCOVERY OF THE 3 NONCONFORMITIES

DECOUVERTE DES 3 ANOMALIES
No clear instructions in the procedure concerning cell plug-in.

Procedure D20 ambiguous:
- no clear indication regarding valve RIS 610-62VP opening.

Procedure S4 makes no provision for checking S1 availability at end of a type C administrative lockout.

DECOUVERTE DES 3 ANOMALIES
2.4 - BREACH OF OPERATING RULES AT TRAWSFYNDD POWER STATION

2.4.1 Description

On the night of 6 January 1987, refuelling was to be carried out on Reactor 1 to a double dwell 1 and 9 refuelling programme No 1704 at standpipe 05J, to replace fuel of 5,600 MWD/Te channel average irradiation.

The Reactor 1 desk operator carried out the routine operations necessary, including switching the sector rods to low speed, for the fuelling programme of 7 channels. As the fuelling progressed, the sector rods in sector G/H slowly inserted and the sector rods in sector A/B slowly raised. Early on into the fuelling, the sector rod auto limit alarm was received on sector A/B, checked by the Desk Operator as being a frequent upper alarm and accepted. Later on into the fuelling programme, at approximately 05.00 hours, the sector rod auto limit alarm was received on sector G/H, seen as being a lower alarm, accepted by the Desk Operator who accepted the slow rod insertion rate.

Because of the diverse movement of sector rods A/B and G/H, combined with refuelling of high irradiation fuel, he did not attempt to clear the auto limit by switching the sector rods to manual and trimming. He decided to watch sector G/H rod movement closely and complete the fuelling programme which had approximately 2 channels to go. The fuelling programme was completed and the sector rod speed control switches were returned to high speed.

Following the completion of the fuelling programme, the Desk Operator attempted to clear sector G/H lower auto limit. With the rods being at approximately 600 crus on the chart, he lowered the bulk group 4 rods but had to stop as sector A/B rods were then at 920 crus and raising. (940 cru = top of active core.) He then demanded 2°C on sector A/B which lowered in the rods but they did not clear the upper limit. He then had group 4 rod 12F in sector B put on trim by a plant operator and he trimmed out the rod to bring sector A/B rods below their upper auto limit. The earlier action of lowering 2°C on sector A/B had caused sector rods G/H to turn and were observed to be slowly raising. Because the end of shift was approaching and he would find difficulty in obtaining the services of a plant operator to put a further rod on trim, the Desk Operator decided to leave the reactor to settle down and hand over shift. He felt that he was in control of the situation at all times and therefore did not call on the services of, or point out any of his actions to, the control room supervisor.

The control room supervisor during the later part of the night shift, whilst the routine fuelling on Reactor 1 was progressing, carried on with his other duties in the control room and on the shut down Reactor 2. He left the control of Reactor 1 and the fuelling to the very experienced Reactor 1 desk operator.

The night shift charge engineer did not get involved with any of the control room operations during this period but carried on with his other duties.

The night shift desk operator was interviewed by the panel of inquiry and he accepted that the sequence of events as reported above were factually correct. The operator was experienced and knew the Operating Rules well, but
when asked why the reactor was not placed on manual control he gave no convincing reasons. The panel believe that this desk operator felt "safer" with the reactor on auto-control as this would give less chance of a trip.

Reactor 2 was undergoing its biennial outage and the desk driver was originally scheduled to control gas duct entries until the Shift Charge Engineer reported sick and positions rescheduled. As a result, the normal handover was late by some 5 minutes. It was, however, conducted in a fairly normal manner with the on-coming desk driver readily admitting that the state of the sector control rods was highlighted to him.

The day shift desk driver assured the panel that he was aware that sector G/H rods were too far inserted. This state had been highlighted to him at shift change-over but the implication in terms of the Operating Rules was not fully appreciated. He was about to rettrim the reactor when he received a request from pile cap to reinstate the rod at 05J, which had been removed to give access for the fuelling machine. This request was refused as the rod was not selected to trim.

Before he could organise either the rettrimming of sector G/H rods or the reinstatement of 05J, the desk operator was asked if he could allow IMD to conduct routine guard line testing. This testing would require the reactor to be held in a steady state. The panel believe that as the request to carry out the guard line testing came from the control room supervisor, the desk operator chose this as his first task. The testing took up most of the morning, during which time the sector G/H rods were at 605 crus at all times in breach of the Operating Rule.

The panel was not satisfied that the desk driver, at the time of the incident, was fully aware of the Operating Rule or its purpose. This reflects on the training and selection techniques, the supervision and the experience of desk operators at Trawsfynydd. This point will be discussed later.

2.4.2 Assessment

The Trawsfynydd reactor core is divided into 5 sectors, one central sector with 2 grey rods and 4 peripheral sectors each with 4 grey control rods. The complete automatic control system incorporates 5 separate but identically structured servo loops, each actuating independent low frequency generators driving the rod groups at constant motor velocity.

All control rod insertions are displayed on a reactor mimic mounted on a paper in front of the desk operator. Within a sector group, the rods are maintained nominally in line, a maximum spread of 50 crus in indicated insertions being allowed operationally. (0-1000 control rods units (cru) represents fully inserted to nominally fully withdrawn. The range is non-linear and is proportional to the number of turns on the control rod pancake drum).

From one control rod of each sector group, the rod position synchro signal is teed off via a synchro/analogue converter to feed the channel recorders mounted in the sector servo vertical panels behind the reactor desk. It is from these recorders that the high and low alarms are generated at 850 cru (operation upper limit) and 615 cru (Operating Rule minimum insertion) respectively. Both these alarms are fed to a common panel "sector rod auto limit" alarm.
Operating Rule 6.5: "Under normal operating conditions, including the times when routine operations are being carried out within the core, the auto sector control system shall only be in operation when all sector rods are at 615 cru (control rod units) or above. If one or more sector rods are lower than this level, all sectors shall be switched to Manual Control. Except when in the process of engaging or disengaging automatic control or switching over equipments, either all sectors or no sectors shall be on auto control."

This rule was designed originally to protect against a composite fault developing as sector groups fully insert during a controlled asymmetric sector rod withdrawal fault. Improved modelling has since shown this fault to be no more onerous than the limiting fast uncontrolled fault.

The rule has been retained for simplicity as a bounding condition for single coarse rod withdrawal fault protection. On auto control such as fault may be localised to an extent that 2 lines of protection are not available. In conjunction with existing single rod handling limits, it has been shown that melting temperatures would not be reached provided the initial sector rod insertion is limited to 615 cru or above when on auto control.

In normal operation, because of high fuel burn up, it is not unusual for the sector rods to be high and the alarm to be active. This obviously masks more onerous conditions of rod low and the panel of inquiry believes that action should be taken to separate these alarms.

2.4.3 The duties of the Control Room Supervisor with Operational Plant

The control room at Trawsfynydd has 2 reactor unit desks and a centre desk. Apart from supervising the 2 reactor desk drivers, the supervisor is also responsible for the Station's electrical systems and high voltage switching for the grid. These functions are well understood by all the control room supervisors.

It is normal at Trawsfynydd for the supervisor, once he has taken over control, to check both reactors to ensure that he knows the state of each. This check includes rod positions and standing alarms. It is generally accepted that the supervisor is informed of all significant events and operations, and that the state of the reactors is checked at least twice more during each shift, and finally as he writes up his log.

The day shift supervisor agreed that the normal level of checking had not been conducted. This was due to the normal day shift pressure and to him concentrating on other problems being generated from the shut down reactor, eg high speed pony motor testing.

The panel of inquiry felt that the supervisor had been careless by not personally checking the state of Reactor 1 plant.

2.4.4 Non Urgent and Unrelated Activities in the Control Room

The following lists all the work that was undertaken by the control room staff during the shift on 6 January 1987:

Control Room Activities - Day Shift, 6 January 1987.

26
District staff working on T/A 4 unit and generator transformer - alarm checks.

Pfostiniog Power Station carried out diesel generator tests/liaised with Trawsfynydd main control room 400 kV Substation, 11 kV supplies failed to close checks and trip resets.

Reactor 2 outage was into its 5th day and, after 4 days off, "catching up" reading carried out. Reactor 2 circuit 11 high speed pony motor tests (3 off) carried out - alarms. Reactor 2 start of dry air purge co-ordinated from the main control room. Liaison with Mechanical Maintenance Department, Assistant Shift Charge Engineer Plant, Charge Face and Health Physics.

Health Physicist visited the main control room to advise on discharge of CO₂/air mixture.

High CO₂ in shield cooling north and south R2 alarm annunciating. Bellows sniffing high alarms annunciating on circuits 10, 11 and 12, which involved further liaison with health physics and reactor personnel. Reactor Chemist visited main control room to bring details of Reactor 2 condition and discuss the location and method of sampling gas concentration, moisture, etc.

Party of observers visited the main control room to study video of previous evening's emergency supplies board. Loss of supply test. Continuous requests via the control room supervisor's desk telephone (PAX 360) for messages to be put out on the public address system. Personnel and their supervisors were asked not to use PAX 360 for that purpose unless it was urgent, but to no avail.

Whilst the control room supervisor was busy with Reactor 2 and the control room in general, the Reactor 1 desk operator, after giving permission to work on the auto reset TTAs, became involved in the following:

IMD telephoned from the BCD room informing the desk operator that they were going to work on BC10 - alarms. Further attempt made to reinstate fuelling standpipe rod at 05J but insufficient plant operators available (all on R2). Checks carried out on BC10 following unsatisfactory work on BC10 precip.

BC40 way valve out of step alarms on No 10 (standing fault) No 4 and No 12 valve. Adjustments made in an attempt to make them more reliable but occasionally out of step throughout the morning.

Routine change-over of prescans and backscans on BCD east and west for fuelling programmes.

Instructed control room supervisor on method of updated new "Status Board" programme on computer.

Requested and carried out T/C change for fuelling programme. Repairs being carried out on BCD 40 way valve remote advance/hold control panel.
Information obtained for temperature assessment.

Discussed duct access requirements for the following day with the planning engineer.

Wrote message on computer for other users as requested by Planning Engineer.

This highlights the distractions which can occur, especially on day shift, and emphasises the need for both control room supervisor and the desk operator to plan and control all activities in the control room. This in no way excuses the breach of rules but may explain why it could go unresolved for so long.

2.4.5 The Phasing of Planned Work

The maintenance staff at Trawsfynydd are primarily based on days only. 5 maintenance engineers are on shift. It is thus inevitable that the greater interference to steady state operation must occur on day shift. To balance out this interference, permits for work are normally prepared on evenings or nights but the station is still busier during the day.

The testing and calibration on the guard line is a job which should only be handled on days as it requires a specialist IMD engineering input and often witnessing by an AEI surveyor. This, and other work not directly associated with reactor operations, has been studied and, in general, this work should proceed on days. This will inevitably place a greater strain on desk drivers and control room supervisors, who must be of sufficiently strong character that they remain in control, and that safe reactor operation remains the first and overriding priority.

2.4.6 Factors Contributing to the Incident

It is useful to consider separately each member of personnel involved in this incident, the errors they made and the likely reasons for the errors.

2.4.6.1 The Night Shift Operator:

a. Failed to switch to manual control when required because:

   (i) planning of the operation placed him under time pressure to complete the refuelling,

   (ii) lack of practice and training undermined his confidence to control the rods manually.

b. Failed to inform his supervisor of the reactor state, because:

   (i) informal procedures whereby the operator takes key decisions are probably routine in the plant, indeed; it may not be possible to operate in any other way given the requirements and constraints imposed by the organisation.

c. Failed in his attempt to trim the rods once fuelling had been completed, because:
(i) he did not place sufficiently high priority on the task.

(ii) he considered it unlikely that he would be able to obtain the services of a plant operator to put a further rod on trim so late in the shift.

2.4.6.2 The Morning Shift Operator:

a. Failed to attempt to retrim the rods because:

   (i) he did not place sufficient priority on the task,

   (ii) to oblige his supervisor, he chose to give highest priority to the guard line tests.

2.4.6.3 Both Supervisors

a. Failed to carry out the required level of checking because:

   (i) they have too many formal and informal tasks to perform,

   (ii) alarm procedures are poor: the high and low rod position alarms sound alike and personnel become used to ignoring the many alarms that sound during refuelling.
2.5 - OSKARSHAMN UNIT 3

2.5.1 The Incident

Early Friday morning on 24 July 1987, so-called local critical tests were begun without the pre-requisites pursuant to the safety technical specifications and operational orders being complied with. The hydraulic reactor scram system (354) was neither operable nor tested. Other relevant systems according to the operational order were not systematically tested and operable.

During the local critical tests a reactor trip occurred on one occasion. Certain instrument readings in connection with the trip were discussed, but the trip did not induce other steps than to repeat the test with reduced step length in the control rod withdrawal. No records of the reactor trip in the form of computer print-outs were made.

The shift team which commenced on duty on Friday morning discontinued the test series after having noticed that system 354 was not operable. This shift team had then checked against the operational order and the prescribed technical specifications for operation. The so-called steering group meeting was informed that the tests had been discontinued due to the fact that the technical specifications were not complied with. The steering group meeting is a daily management meeting for the annual shut down. The daily operational meeting was already terminated when the information of the interruption of the tests reached the operational management of Oskarshamn 3. However, the operational meeting was informed that local critical tests were going on and that so-called RPS tests (i.e testing of system 354 and certain other reactor operation systems) remained. Nobody at the meeting questioned whether such actions were appropriate from a safety point of view.

After the steering group meeting the operational management appointed a task group to investigate what had happened and to report to the presidium of the central safety committee of OKG in the afternoon. An operation planner clarified the operational order to the control room, and tests were then restarted with the system 354 and the other reactor protection systems operable. Still no testing of the systems pursuant to the prescribed procedure had been made. Neither the operation planner nor the shift team had noticed that completed RPS tests were a pre-requisite of the systems being formally assigned to be in operable state for the operational year to come.

Local critical tests were then continued during the morning until they had to be discontinued because other tasks were to be resumed inside the containment.

At noon, a modified time schedule for the remaining work before the starting up was issued. The plan conflicted with the prescribed technical specifications for operation as the completion of local critical tests and even other tests with a new control rod operating programme in the plant computer preceded the testing of the reactor protection systems. However, the error was discovered and the schedule was withdrawn before the work had been started in a wrong way. During the afternoon and the evening, various systems were tested and the reactor was returned to power the the proper sequence between different activities.
2.5.2 Violation of the Prescribed Technical Specifications for Operation

The following violation of the prescribed technical specifications for operation has been noted during the events:

- Critical tests were started up during the night to Friday without the system 354 being operable and without a systematic and documented check that the other systems, which pursuant to the operational order and the technical specifications should be operable for the test, were so.

Furthermore, it can be stated that the local critical tests were continued on Friday morning with the system 354 operable but still without the actual systems having been tested for operability pursuant to the prescribed procedure.

2.5.3 Where and When did the Faults Arise?

2.5.3.1 In the Incident Itself

- In reviewing and modifying the actual work planning before the night shift the engineer on duty, together with the shift engineer in the night shift, did not check if the tasks of the night could be carried through without conflicts with the safety technical specifications.

- The shift supervisor and the reactor operator's review in the control room of the pre-requisites for critical tests were not satisfactory. The discussion which arose of the need of the 354 system to be available was conducted only between the reactor operator and the core physicist.

- The operational order for critical tests had certain deficiencies in its wording. Among other things, certain pre-requisites were lacking and the listing of the pre-requisites included was not clear enough with appropriate provisions for ticking off.

- The shift engineer made no closer analysis and took no steps to check, verify and record the safety situation after the reactor trip.

- The plant operation management started an investigation in the morning on account of a received report on a reactor trip and deviations from the prescribed technical specifications for operation during local critical tests. There was, however, no immediate reaction on the fact that critical tests were still performed in the wrong sequence in relation to the tests of the reactor protection systems. The tests were thus allowed to be continued in the morning with an operable but not tested 354 system.

2.5.3.2 In the Surrounding Circumstances

- A strong aim to complete the shutdown as planned and return to power on schedule. This, in turn, conducted to comprehensive overtime work. There was no checking of the amount of overtime and of resting periods except as a basis for overtime payment. A number of staff members with tasks of essential important to plant safety had so little rest during the actual period of time that a fully satisfactory performance could no reasonably be expected from them.
- Unclear instructions on order paths and responsibility in the control room during shutdown and preparation of starting up.

- Deficiencies in education and training on technical specifications, making them a living instrument.

- Deficiencies in the routines of handling operational orders.

- Deficiencies in the routines for altering of plans.

- Deficiencies in auditing of administrative routines for safety management, with the consequence that the above-mentioned circumstances were not discovered in due time.

2.5.4 Incident Analysis

The Oskarshamn (O3) incident is interesting from a human factors point of view, since it represents an incident reflecting deficiencies mainly in the human and organisational part of the socio-technical system. It is, however, not a clear incident of purely cognitive mistakes - they were part of the sequence of events preceding and following the reportable event, but that event in itself did not represent a typical cognitive mistake.

Relevant to the O3 incident is the distinction made by Reason (1988) between errors and violations. Human errors, categorised as either slips or mistakes, are understood with reference to the information processing of the individual. But Reason points out that this classification of errors cannot account for all possible varieties of aberrant behaviour. "What is missing is a further level of analysis acknowledging that, for the most part, humans do not plan and execute their actions in isolation, but within a regulated social milieu". Violations are then defined as "deliberate or unwitting deviations from those practices deemed necessary (by designers, managers and regulatory agencies) to maintain the safe operation of a potentially hazardous system". Unintended violations fall into the category of errors. Those having some degree of intentionality Reason divides further into routine and exceptional violations.

Important contributors to routine violations are (1) the general human tendency to minimise the effort spent to achieve a given goal, and (2) a relative indifferent environment (ie one that rarely punishes violations or rewards observance).

Exceptional violations are less clearly described, but can occur under various exceptional circumstances - "particularly tasks or operating circumstances that made violations inevitable, no matter how well-intentioned the operators may have been".

Often both errors and violations are present in the same action sequence, but "they have different psychological origins, are propagated along different system pathways and demand different remedial measures".

Reason also described how errors and violations can be viewed from the perspective of the total socio-technical system. He presents a resident pathogen theory of accident causation. In his own words:
"All man-made systems contain potentially damaging agencies, like pathogens within the human body. At any one time, each complex system will have within it a certain number of latent failures, whose effects are not immediately apparent but which can serve both to promote unsafe acts and to weaken its defence mechanisms. For the most part, they are tolerated, detected and corrected, or kept in check by protective measures. But every now and again, a set of external circumstances—called here local triggers—arises which combines with these resident pathogens in subtle and often unlikely ways to thwart the system's defences and bring about its catastrophic destruction. Resident pathogens include the effects of bad decisions made by policy makers, designers, managers, supervisors; latent maintenance errors; routine violations. Local triggers comprise component failures, atypical system states, environmental conditions, active operator errors and exceptional violations."

This distinction between errors and violations is of particular relevance to the Oskarshamn incident. In the sequence of events you will find both represented. It is also an illustration of how latent failures or 'resident pathogens' in combination with 'local triggers' contributed to the incident evolution.

2.5.5 The Incident Evolution

The incident can be broken down into the following sequences or events:

1. Delay of time schedule by 20 hours.

2. A revised start up plan is produced, where sequences originally in sequential order are put in parallel to each other.

3. Problems occur with tightening the hatch to the containment.

4. Another delay of the time schedule occurs involving a delay of RCS-tests of systems, 311, 314 and 354.

5. Shift turn-over between afternoon/evening shift. This is done verbally with the support of written personal memory notes.

6. The on-going shift supervisor (SS) does not perceive that RPS-tests of system 354 remain to be done.

7. At about 3 am during the night shift, the shift supervisor said, in passing to the deputy operating engineer, that the local criticality measurements (LCM) also could be carried out, which he did not perceive.

8. The SS takes out the operating order for the LCM and asks the reactor operator (RO) to start the preparations. He had previously looked through the operating order, but did not check that the pre-requisites for the test were fulfilled.

9. The RO starts with the preparations and focuses at first on the test procedure, since he had not done the test before.

10. While going through the pre-requisites in the operating order, the RO is distracted by alarms on the safety control panel. On resuming the
preparations he starts at the wrong line in the operating procedure which states that, amongst other things, system 354 should be ready for operation.

11. Further alarms were activated on the safety control panel, which the RO acknowledges. He then notices that the service valves to system 354 are closed.

12. The RO tells the reactor physicist that he thinks it is strange that a reactor scram could not now be triggered, but that the reactor could only be stopped by screw drive. He assumes that the shift supervisor also hears his remarks.

13. The reactor physicist (RP) said it was sufficient with screw stop. He made a judgement based only on reactor physics considerations which, however, was not stated.

14. LCMs are started without all safety systems in operation.

15. During measurement 2 SS/RR was activated.

16. The RO and RP assumes that there is an error in the computer update.

17. The shift supervisor noticed at the reactor desk that the rods were on the way in, but that the reactor scram tanks had not been emptied. He is satisfied with the explanation he gets from the RO and RP, since he assumed that they were following the operating order - he saw it all as an indication that everything was working as it should.

18. Measurements are resumed removing the rods more slowly to see if the computer displayed the pulse frequency as expected.

19. Shift turn-over between night and morning shift. This is done verbally, based on written notes.

20. Leaving SS does not mention that RPS-tests of 311, 313 and 354 had not been carried out.

21. During the turn-over, the night RO queries with the morning RO if it was correct to perform the measurements without system 354.

22. The morning RO continues the measurements, but wonders about the fact that system 354 was shut down. He completes the measurements and checks on computer the remaining faults with system 354, the operating order and the Technical Specifications. He noted that the service valves were closed and the RPS switch was off and that according to Technical Specifications system 354 should be ready for operation in order to perform the measurements. Thereafter, he stops the measurements and informs the shift supervisor of these events after he comes back from the operating meeting.

23. During the operating meeting in the morning, it is noted that LCMs are under way and that the RPS tests of systems 354, 314 and 311 still had to be carried out.

24. The operating order for the LCMs were clarified, although without consideration to the fact that the RPS tests should have been made before the LCMs were resumed.
25. The LCMs are resumed, with system 354 switched on, but without RPS tests having been made.

26. The measurements are stopped for other work to be made.

27. A revised start up plan is distributed to the control room still with the LCMs preceding the RPS tests.

28. Other personnel in the office noted the flaw in the revised start-up plan and pointed out that the RPS tests should be carried out before the LCMs.

29. The revised start-up plan is recalled.

30. RPS tests are made and LCMs resumed at 2100 and completed at 2315.

2.5.6 Analysis of Events

2.5.6.1 Sequence 1 and 2

First of all, it is obvious that the delay of the time schedule would not have caused the same problem should they have delayed the time for start-up keeping the original plan for the work to be done. In the original plan the sequencing of events guaranteed that the LCMs were made after the RPS tests. The strong focus on keeping the start-up date and the revised start-up plan can thus be classified as latent failures, or resident pathogens, in the socio-technical system which represent factors that can propagate errors and violations.

There has been a tendency to try to minimise the time periods for outages. Any unforeseen problems occurring during an outage then naturally will increase the demands on the whole organisation. With every change in the original plans, it is necessary to be aware that the goals pursued are coupled to their consequences for safety.

Another issue to remember when scheduling the work during an outage, and this applies to the original plans as well as any rescheduling of tasks, is that the tasks to be performed are put in relation to the availability of personnel - not only in terms of competence, but also time. There is a risk that the work planned, particularly for rare specialists, assumes a high amount of overtime. In this case, it can be argued that in the revised start-up plan you already embedded a violation of the work hour law in terms of excessive overtime for certain categories of personnel.

2.5.6.2 Sequence 3 and 4

The technical system failure can be classified as a 'local trigger', which in turn caused a further delay of the time schedule. This is also the first instance wherein you can notice that the delay of the RPS tests did not call upon extra measures in the administrative routines.

2.5.6.3 Sequence 5

This is a violation of the procedures to be followed during shift turn-over, which were regulated by the company. This should have been followed by those involved. However, it is most probably a reflection of the principle of "least effort", as well as a case wherein following the procedure
is seldom rewarded and not following it sanctioned. It could then be classified as a routine violation. But considering the special circumstances at the time, with delays of time schedule, further problems having occurred during the afternoon shift, etc, may also be regarded as an exceptional violation.

The importance of routines during shift change-over have been illustrated also in other major incidents. The problem of keeping up a strict routine over time, particularly during normal operation, has been reported. The routine may need to be adjusted for the outage period.

2.5.6.4 Sequence 6

In the verbal communication between the afternoon RO and the on-going night RO, the information regarding RPS tests of system 354 is not forwarded and perceived in a clear way. It may have been avoided with a better turn-over routine.

But it is also important to understand why this miss in the verbal communication occurred. On the part of the night shift SS it can be classified as an attention slip, a miss in the first stage of information processing. There are several information units transformed to the SE and it should be remembered that there is a limit to the number of information units that simultaneously can be handled in the short-term memory. Complementing with a written information could serve as an 'external memory' in this situation.

Closely related to this is alertness, ie decreased alertness lowers the attention level. This is particularly noticeable in the early morning when the alertness level is decreased due to the influence of circadian rhythms, thus further limiting the capacity to process information. Added to this is the fact that the on-going SS had been working in a very demanding shift system together with overtime during 12 days preceding this shift change-over. This could have further contributed to a decreased alertness.

2.5.6.5 Sequence 7

Another slip characterised by attention failure. The combination of time of day, sleep deprivation and workload is a very positive contribution to this error (see further a description of the conditions at the time in the report).

2.5.6.6 Sequence 8

It is hard to classify this as a slip or mistake, since the SS read the pre-requisites for the test, but did not check the plant status. It could be a reflection of a routine violation in the sense that he relies on the RO for checking the plant status (in order to save time and effort) since he is at the time occupied with other tasks. In the report, his reliance on the opinion of the reactor physicist (who had written the operating order), his view of the status of the test and his (and the whole group's) lack of knowledge how it was coupled to requirements in Technical Specifications, are further facts pointed out as contributing to the action.
2.5.6.7 Sequence 10

A clear slip. It is well-known that slips of action are likely to occur when some internal activity or external distraction catches the attention of the operator (see, eg. Reason, 1984). A remedial action to decrease the risk of action slips is to make the central control of the actions more conscious (ie to force oneself to think about the action sequences performed). In this case, a better designed operating order, through separation of the pre-requisites for different systems into different rows, followed by demands on signature (acknowledgement requirement), could have served this purpose.

2.5.6.8 Sequences 11 and 12

This could have been an illustration of a distraction putting the RO on the right track, since it gives him a chance to reflect over the fact that system 354 is not in operation. (In the case of mistakes, only slips or negative feedback can make a person deviate from the chosen path of behaviour.)

The fact that he does not react to his own doubts can be an illustration of what has been referred to as the 'group think' syndrome (see further the summary of symptoms given by Reason, 1987, page 124). Two of the symptoms of this syndrome that fit in here are: "self-censorship of any doubts felt by individual members and a shared illusion of unanimity arising both from self-censorship of doubts and the assumption that silence means consent" (the RO assumed that the SS heard him presenting his doubts). The tendency for group think phenomena to occur increases when the group is under stress (cf. Janis & Mann, 1977). The time of day, sleep deprivation, time pressure and work-load could all have contributed as stress factors.

2.5.6.9 Sequence 13

The RP was, in fact, the person who was responsible for writing the operational order and he should have known the pre-requisites. He had, however, copied his operating order from last year and made his judgement based primarily on reactor physics considerations. He was also unaware of the requirements in the Technical Specifications. Whether this is an error or violation is not clear. The best classification seems to be an unintended violation and, as such, it falls into the category of mistakes rather than slips. A mistake occurring due to organisational factors in terms of how the responsibilities for the LCMs are and safety were, formally and informally, distributed within the group. It is important that experts involved in part-tasks have the necessary competence also in the safety goals at large. Also, to be very aware of the risk associated with 'experts' being assigned a greater responsibility by others in the group due to his expertness in a particular task.

2.6.6.10 Sequence 14

The violation that also led to the reportable event. This violation was, however, not noticed at this time and, therefore, the incident continued after this action. It may be termed an exceptional violation and understood in terms of the latent failures preceding this action.
2.5.6.11 Sequence 15 and 16

The interpretation of the cause of the reactor scram was in part a mistake. The reconstruction showed that the neutron flux, measured with SRM and presented on the computer screen, was also considerably lower in the initial stages than was expected, based on previous experience and with predictions prior to the reconstruction. They interpreted this as a case of delayed feedback from the computer, based on earlier experiences of computer response times. Improved instrumentation was suggested as a remedial action.

2.5.6.12 Sequence 17

A mistake illustrating a misinterpretation of plant status. The SS is mentally already set on the hypothesis they are following the operating order written by the reactor physicist. It is well known that we form hypothesis about a situation very early in the problem solving stage. Also, that we usually look for confirmation of this first hypotheses rather than testing alternative hypotheses or those who will negate the first one. The SS said he looked at it in a positive way. He was also at the end of the shift and he was preparing for shift change-over. In addition to these circumstances, we have the other stress factors mentioned above (time pressure, workload, time of day, sleep deprivation) that will reinforce this tendency of choosing only one hypothesis and testing primarily for positive instances of this hypothesis.

2.5.6.13 Sequence 18

A relevant action considering their interpretation of the cause of the scram.

2.5.6.14 Sequence 19 and 20

See sequence 5 above.

2.5.6.15 Sequence 21 and 22

When a new person is introduced, ie someone who has not been part of the first erroneous phases of problem solving during a task, this can lead to the correct solution being found. In this case, the night SS also forwarded his doubts to the morning SSs(a further indication of a group think phenomena in the former group). The "defence in depth" principle for the technical system, with redundancy and diversification, may thus have some relevance also on the personnel side when avoiding mistakes to occur and to continue. An extra person (redundancy) who is not at first involved with the task (diversification) could then possibly break a wrong problem-solving task being pursued. It is, however, particularly important then that he asks questions to those performing the task instead of being informed by them.

2.5.6.16 Sequence 23 to 28

Crucial in all these sequences of events is the RPS tests.

Representatives from many different parts of the organisation fail to acknowledge that the tests should precede the LCMs. This reveals a lack of knowledge of Technical Specifications. But it also reflects the status or safety importance ascribed to the LCMs. They were thought to be relatively
harmless and they were also moved from the chapter "Requirements and limitations for operations" to the chapter "Requirements and limitations for outages" in the Technical Specifications. The full meaning of the term "ready for operation" was also unclear in the organisation. On the whole, these factors reflect an organisation culture/safety culture issue.

The fact that these mistakes and violations are noticed is again due to other persons than those not directly involved noticing the flaw.
SECTION 3

In performing its event analysis, Task Force 7 held 2 meetings to discuss the reactor events, and to compare and contrast different viewpoints concerning the human actions taken in these events. These meetings were particularly valuable and the discussion wide-ranging and thought provoking. Some of the content of these discussions is contained within the event descriptions and analysis presented in Section 2. However, that section does not entirely reflect the group’s discussion, and thus this section contains some brief points which occurred during discussion.

3.1 Biblis

Points noted in the discussion included:

- This event, like La Salle, illustrates an operator’s willingness to take innovative action to cope with an unexpected situation, which was not covered by procedures.

- The operator’s safety consciousness with regard to what might be thought of as absolute rules of practice, e.g. primary circuit integrity, containment integrity, reactor protection system functioning, etc., does not appear strong enough. In unfamiliar situations, it might be expected that the operational staff would be guided by overriding safety rules, rather than invent ad hoc courses of action.

- In the Biblis incident, the exact risk from the ad hoc actions was not immediately obvious, but operators should be aware that in dealing with complex plant the consequences of particular procedures often require detailed analysis.

- The reason for the operator’s decision to continue plant start-up with the non-return valve open is of great concern. The operator may well have believed that the valve was actually shut but, unfortunately, the operator had little possibility of checking the actual valve leakage, if any. A high workload on the operator during start-up, plus pressures of time schedule, may have also been contributory factors.

- Past experience is a very powerful influence on operators. Thus, previous problems with non-return valve instrumentation may have led him to conclude that the valve was actually shut. Similarly, the use of the test line to check the HPI system was a routine action which seemed superficially very similar to the use made of the test line to try to close the non-return valve.

When faced with problems it is a natural human reaction to try to rationalise the problem into some familiar pattern. Thus, evidence is looked for that confirms the familiar pattern and contrary evidence is ignored. (This trait was also noted in the Oskarshamn event.) It should not, therefore, be expected that plant staff will make an objective analysis of all plant evidence when faced with a problem. It is far more likely that they will try to fit the problem to a known circumstance (often a very successful strategy), and proceed with action on that basis.
The redundancy of supervisory monitoring clearly failed at Biblis (as also at Oskarshamm and Trawsfynydd). Despite clear operational procedures requiring monitoring and formal checking, operational teams may frequently evolve a method of action which relies on independent action. In many cases, this will be an efficient and effective solution to perform team operations. However, the "rules" of such team operation are then informal and are difficult to define or regulate.

3.2 La Salle

Points noted in the discussion included:

- There is a similarity between the La Salle and Biblis events in that both involved the plant staff improvising actions in circumstances where the plant procedures were unspecific. However, in both cases, the obviously safe action was deferred in preference to an alternative course of action which had operational advantages. Such alternative courses of action may be judged acceptable because no risk is perceived, or because the plant safety systems may be thought adequate to protect against any problems that could occur. Either rationale implies a reduced safety consciousness in the face of operational pressures.

- It is difficult to be entirely prescriptive about what action operators should/must take in unfamiliar reactor states. There may be some situations in which it is advantageous for the operator to use his ingenuity. However, the general trend would appear to be that actions planned in haste are unlikely to recognise problems and are, therefore, likely to be flawed in concept or implementation. A well thought-out contingency procedure, planned in advance, is probably a preferable situation.

- Errors of misunderstanding occur not only at operational level but also at management levels. In the case of La Salle, there may have been a lack of appreciation by plant management that plant safety requires positive action against many contingencies, many of which seem improbable. A more positive recognition of safety needs may have avoided the situation in which operators had little useful guidance as to what action to take.

3.3 Blayais

Points raised during discussion included:

- Plant re-start is always an extremely busy time during which everyone has many tasks often with conflicting requirements for equipment. This problem is exacerbated by changes/delays to original planning schedules. It can be extremely difficult to establish a proper order for the many tasks which reflect their importance and the most appropriate sequence for action.

- It can be reasonably assumed that none of the errors made, which led to the inappropriate plant staff, were made deliberately. Nonetheless, the plant staff were clearly not aware of the plant state but had relied on the procedures to ensure that a safe plant state was maintained. Where groups of people are involved in planning procedures, there is a tendency to rely on other members of the group to detect problems, and
thus the group conclusions may be given more strength than is
appropriate. A belief that a planning group had thought through the
procedures may lead to a less questioning approach by those implementing
the procedures. This lack of awareness of potential problems may have
contributed to this event.

Where changes in plant state are being made, there is a need for a break
in the hectic activity to check that all the safety requirements are
satisfied. A formal checking-off of the specifications may be most
appropriate.

During periods such as plant start up, it is inevitable that errors and
slips may be made. These errors can be minimised, but probably not
totally avoided, by good design procedures, hardware and work patterns.
There is thus a need to ensure that errors are detected before they lead
to a safety problem by appropriate provision of alarms, information,
checking and supervision and test of safety related systems. This
additional detection safety level acts as a redundant defence.

3.4 Trawsfynydd

Points raised during discussion included:

- A shift supervisor responsible for 2 reactors, one in shutdown and the
other operating normally, will be preoccupied with the higher workload
from the shutdown reactor. It may, therefore, be unreasonable to expect
him to give the normal monitoring supervision to the other reactor under
these circumstances.

- The desk engineer operated largely independently, as he was probably
used to doing, and did not inform his supervisor of the difficulties
(see comments on Oskarshamn). However, the engineer clearly felt
apprehensive about taking over manual rod control, thus indicating that
his independent attitude was not well-founded. He may, however, have
been influenced by his supervisor's workload on the shutdown reactor.
The planned human redundancy (ie supervision) was totally negated in
this event.

- With increasing reactor automation and the long, steady running of
well-tried reactor plant, the operator's familiarity with manual
operation may be reduced to an unsatisfactory level.

- In this event, the operators clearly appreciated that the plant was in
breach of the Operating Rules and yet put little priority on that
problem. It may be speculated that the Operating Rules were not viewed
with sufficient seriousness. Alternatively, it may be that the purpose
of this rule was unclear; the perception of problems from a high rod
insertion may be difficult to appreciate, and there may have appeared to
be little danger from allowing this state to persist.

Where the potential for operation in breach of safety rules exists,
there is a requirement for additional protection over and above that
provided by the operator. This may be in terms of hardware (alarms,
interlocks, etc) or effective human redundancy.
3.5 Oskarshamn

Points raised in discussion included:

- Oskarshamn and Blayaïs have some similarities in occurring during the start-up period of reactor operation. Both incidents reflect problems due to:
  - high workload
  - task scheduling and parallel tasks
  - supervision and monitoring of plant state
  - group judgements
  - communications during shift change-over, etc

Taking some of these points in more detail for Oskarshamn:

- Changes in original planning schedules are a major potential source of problem. An original schedule can be prepared without great time pressures and should, thus, incorporate appropriate thought about order of tasks, etc. If this schedule is changed the original reasoning may not be apparent and the new schedule may be judged satisfactory under large time pressures. Thus, at Oskarshamn, the original schedule had the RPS tests preceding the local criticality tests.

The general point is that planning made in advance should not be easily overridden under circumstances where careful consideration is often difficult.

- Supervision of plant operators presents a difficult task for shift engineers. The shift engineer generally wishes the operators to be self-motivated and responsible, only referring back important information. To insist on a constant high level of monitoring and feedback can be demotivating for the operator and impractical during high workloads. However, the operators may not be aware of the right balance between seeking advice and taking action themselves. In this event, the operator was clearly concerned that the hydraulic scram system was inoperable, but did not specifically bring the issue to the shift engineer's attention for a decision.

- The role of "experts" and group decisions also contributed to the incident. "Experts" such as the reactor physicist have no formal responsibility for plant operation, but can be "given" that responsibility by operational staff. The experts generally do not have the width of perspective or knowledge to exercise such responsibility but may, nevertheless, give advice which is interpreted as being more soundly based that it actually is.

The failure of group meetings to detect the inadequacy of the revised task schedule on several occasions again reflects the problem that groups may be inefficient in a checking role, and yet it is assumed the decisions taken by groups have been well considered.

- Communications during shift change-over, as in a number of other incidents, were clearly a contributory factor. While formal requirements for shift change-over procedures can be helpful, it should be recognised that a procedure involving a heavy workload is unlikely to
be regularly used unless there is a continual monitoring by plant management. Humans have a strong tendency to minimise apparently useless effort.
SECTION 4

While many of the underlying causes of the inappropriate human actions, taken in the 5 events analysed, have been specific to those events, it is clear that the event analyses have indicated a number of more general concerns which are likely to have wide applicability. Some of these areas are noted below, together with brief comments.

4.1 Start-Up Situations

A number of events occurred during the high workload, high time pressure and rather confused state of plant start-up. This state is characterised by:

- abnormal state of many alarms and equipment,
- unfamiliar tasks often infrequently practised,
- many parallel tasks to be performed together,
- work schedule subject to frequent modification.

All these characteristics indicate that mistakes are very likely to occur under these circumstances and that the normal supervisory control may be ineffective.

4.2 Inadequate Instrumentation

Correct operator action relies heavily on appropriate and reliable instrumentation. Several of these events had contributions due to poorly-designed information (grouped alarms, alarm states during shutdown) and due to unreliable instrumentation which had not been rectified. Operators cannot be expected to function efficiently, particularly in high pressures situations, unless accurate, unambiguous information is provided. Past experience with poor instrumentation is a particularly difficult problem where operators' reactions are pre-conditioned and can override strong contrary indications.

4.3 Human Redundancy

The principle of supervision and monitoring human actions as a means of detecting errors, and thus providing human redundancy akin to the more normal hardware redundancy, is well established. However, in the majority of events analysed, the effectiveness of this human redundancy was questionable. Establishing the right balance in the information flow between operator and supervisor appears to be very difficult, and may breakdown at times of high workload. The actual formal responsibilities at a plant may, in practice, be replaced by an informal ad hoc system evolved by the personnel on a day-to-day basis.

4.4 Communications at Shift Change-over

Several of the events involved work which continued over a number of shifts. Communications at these shift change-overs were generally informal and important information was not satisfactorily transferred. Some plants have formal requirements for shift change-over but, in some cases, these requirements are impractical in high workload situations (eg start-up), or are not generally used because there has been no enforcement of the requirements. The fresh viewpoint provided by staff on a new shift is a very important way
of detecting past errors. This can only work well if good information transfer occurs.

4.5 Technical Specifications/Operating Rules

The safety of all plants relies on operation within specified limits but, in a number of cases, these limits were broken. In some cases, this was apparently because the limits were not viewed with particular importance (rightly or wrongly). In other cases, the knowledge of the limits was inadequate. The complexity and lack of priority of operating rules contributed to this situation, as did the difficulty of understanding the reasoning behind some of the rules. Further problems concern rules which were unclear or were not sufficiently comprehensive to provide clear guidance to the operator. All of these problems were exacerbated during high workload situations where competing objectives lead to inadequate or biased interpretation of the operating rules.

It should not be assumed that rules are only broken by inexperienced operating staff, in several cases the operators involved were very experienced and reliable.

4.6 Responsibility for Plant Safety Rules

Particularly during plant start-up and other high workload situations, overall responsibility for plant safety status can be unclear and is difficult to ensure. Sometimes responsibility for some areas is effectively delegated, for example to a test engineer, because of the high workload on the shift engineer. When there are multiple tasks being performed in parallel, it may be practically impossible to monitor the plant state effectively.

4.7 Ad hoc Actions

Plant procedures are not completely prescriptive and do not comprehensively cover every situation which may occur on a plant. As a result, operators sometimes take actions which are invented for the occasion. This process led in several instances to inappropriate actions being taken. The problems were generally due to competing priorities influencing the choice of actions, eg keeping the plant operating rather than shutdown to cure the problem. However, the safety significance of some of the actions was difficult to appreciate and this illustrates the potential problems of planning action on a short timescale.

A number of factors may condition an over-optimistic viewpoint of the ad hoc procedures. These include past experience of broadly similar situations and reliance on a group activity to prepare and review the procedure. On a short timescale, a group may be an ineffective method for review.

Generally, operating staff are expected to act intelligently and thus ad hoc actions, which may be very inventive and clever, may be difficult to avoid.

4.8 Limited Practical Experience

A contributory factor to a number of the events was a lack of familiarity and confidence with some aspects of the plant operation. Thus, plant start-up is a relatively infrequent event, as plants become more
reliable, and any one shift may have very limited experience of the procedures. Similarly, the increased use of automatic control systems reduces the operators familiarity with manual control of plant parameters. Practice ensures that staff are both familiar with the procedures and have an intuitive "feel" for how the plant behaves during these situations. This experience is difficult to reproduce in the rather stereotyped environment of a simulator.

4.9 Plant Management

A number of problems experienced during incidents were, in part, due to poor management decisions in the plant's previous operations. Thus, the acceptance of unreliable instrumentation even when this clearly has an important safety significance will be a major contributor to staff error. Similarly, problems due to staff work overload can be due to the acceptance of unrealistic work schedules and the toleration of excessive overtime working.
SECTION 5

5.1 Based on the analysis of the events detailed in Section 2, the group considered how some of the more general causes of human error may be avoided. In particular, it considered some possible defences against cognitive errors and discussed whether these defences may have mitigated the specific events. In several cases, it is clearly a matter of opinion whether the events could have been avoided, but this discussion is intended as a constructive contribution to the consideration of potential changes in design and operation.

5.2 Many of the events involved staff making a range of errors related to their limited perspective, their knowledge of operating rules, the pressures of time, etc. While action can be taken in the majority of cases to reduce the frequency of these errors, it is difficult to believe that such mistakes can be avoided. The critical issue may, therefore, be whether these errors can be detected, before any serious consequence occurs. The situation at plant start-up is typical of the difficulties encountered with avoiding error in complex circumstances. For this situation, 3 specific suggestions may be of value:

(i) Changes of plant state should be subjected to a "hold" on further work while the safety status of the plant is formally reviewed. This would require a statement of the conditions that the plant must satisfy, together with a formal procedure and responsibility for performing this action. In addition, appropriate tests of safety related systems should be performed to ensure the operational requirements.

(ii) Each shift should include staff whose task is to verify adherence to safety procedures while work is being performed. These staff should operate both inside and outside the control room and have a formal responsibility both to advise on and to monitor the performance of work.

(iii) The alarm and information display systems available to operators should be adapted to shutdown states by permitting the switching off of alarms which are permanently 'on'. This would clearly require very careful implementation including the retriggering of alarms when the plant state changes. However, the potential benefit to operators in the detection of inappropriate plant states is judged to be significant.

5.3 The shift engineer is the person on most plants who is responsible for the supervision of the plant's safety status. While this may be a reasonable situation during normal plant operation, the situation during plant shutdown and start-up is very different. In these situations, the workload on the shift engineer is such as to make it impossible for him to perform his supervisory role adequately. Consequently, during these abnormal plant conditions, there is a requirement for the plant safety supervision task to be separated from the work management task. This separation must involve a clear and written specification of responsibilities.

5.4 Current technical specifications/operating rules and plant procedures often lack clarity, comprehensiveness and adequate guidance to operational staff. A thoughtful and unhurried consideration of potential plant problems is always likely to be more successful than swift, innovative, ad hoc responses. However, these procedures and rules must be well explained so that their importance and significance is understood. While ad hoc actions will be
difficult to avoid (and in some circumstances may be desirable), they may be reduced if better guidance is available.

5.5 The importance of plant management recognising the impact of their decisions on plant safety cannot be over-emphasised. Unreliable instrumentation of safety significance should not be acceptable unless alternative and unambiguous information is available. Work schedules should be practical and allow proper resources for checking and supervision. Changes to preplanned work schedules must be capable of being reviewed away from the time pressures of daily plant meetings.

5.6 The rather unspecific nature of several of the above points, emphasises the difficulty of defending against cognitive errors. By their nature, such errors involve operational staff performing as thinking, innovative systems with the capability to override many procedural defences unless these defences are very well designed. Perhaps the most reliable defence is to accept that such errors will occur, no matter how clever the defences, and to try to design plant and operational procedures to mitigate their consequences and to allow speedy recognition and efficient recovery.

12 September 1989

D3.1/GMB/TF7