COPIE REGISTRY
No pas prendre S.V.P.
Please do not take

Restricted NEA/CSNI/R(95)10/PART2

OECD OCDE PARIS

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 09-Feb-1996
Dist. : 13-Feb-1996

Or. Eng.

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

COMPILATION OF NATIONAL CONTRIBUTIONS TO A CSNI/PWG1 GENERIC STUDY ON HUMAN FACTOR RELATED COMMON CAUSE FAILURES

Report of the Expanded Task Force on Human Factors of the Principal Working Group No. 1

29082

Document incomplet sur OLIS
Incomplete document on OLIS

NEA/CSNI/R(95)10/PART2
Restricted
Or. Eng.

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 co-ordinate 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 co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on 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 co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the 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 the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative 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 regard 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.

* * * * * * * * * * * * * * * * *

The opinions expressed and the arguments employed in this document are the responsibility of the authors and do not necessarily represent those of the OECD.

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France

This material constitutes the technical appendice of the report on Human Failures Related Common Cause Failures (CSNI/R(95)10/PART2). It includes contributions from participating countries, namely: Belgium, Canada, Finland, France, Germany (leading country), Italy, Japan, Korea (Republic of), Russia (Federation of), Slovenia, Spain, United Kingdom, Ukraine, United States.

Belgium

O/Ref. AVN-94/015
Class. XG.CD.00

BELGIAN CONTRIBUTION TO TASK 4 OF ETF (PWG1)

HUMAN FACTORS RELATED COMMON CAUSE FAILURES IN BELGIAN NPP

by Yves Van den Berghe

1. Introduction

A screening of AVN's DIANE (Domestic Information About Nuclear Events) database, for human factor related common cause failure events was performed. This database is used to store and retrieve information on a selection of events which have occurred in the Belgian NPP since 1985. The sources of information are the incident reports which AVN receives from the utilities, completed with the reports of our inspectors on site.

The coding system used within this database is based on the IRS Coding Manual. This coding system does not always allow for an easy retrieval of events related to a specific subject. In addition the DIANE-coding system does not allow for direct retrieval of CCF-events.

The approach which was followed was the following one:

- First of all a broad working definition of a human factor related CCF was developed for this exercise, which is the following:
  "Actual or potential, simultaneous or consecutive failure of redundant, diverse or similar systems, components or barriers due to a single or repeated human performance deficiency."

- A first selection was made out of a total of 500 records in the database, covering the operation of all Belgian NPP from 1985 up to now; a search was made using the human factor related codes of the IRS for the codification of observed and root causes; this resulted in a total of 211 events.

- Because this number of events was still manageable, it was decided to quickly read all summary descriptions of these events; this screening allowed to retrieve those events in which the loss of redundant or similar equipment, due to a single or repeating cause, resulted from the event or was observed during the event; this selection exercise resulted in a total of 17 events which are reported in this document.

- For all 17 events which were finally selected, the original incident reports from the utilities, if available, as well as the additional information from the AVN inspector reports, were drawn out of their files and submitted to a careful reading; this was done in order to confirm the selection made previously on the basis of the summary information available in the DIANE database and to obtain more ample information on the event itself; for each event a summary was made consisting of a short description of the event, a description of the causes and the human factors involved, and a short discussion of the safety significance of the event; this information is available in section 2 of this report.

– In order to support the development of some general conclusions, an additional analysis was made, identifying the following items:
  - mode of operation during which the human error occurred
  - type of activity during which the human performance deficiency occurred; the following activities were used: design, testing, maintenance and operation
  - personnel category to which the person(s), which performed inadequately, belong(s)
  - behavioural factors which characterise the human performance deficiency (e.g. omission, lack of knowledge,...)
  - if a procedure (or other document), supporting the human action, was not followed or inadequate (which includes lacking)
  - type of dependency which lays at the basis of the common cause effect :
    - ◊ systems sharing a common component which was affected by the human error
    - ◊ components affected by a common instruction or procedure (which was omitted or inadequate)
    - ◊ systems or components affected by a common condition, resulting from the human error or existing during the occurrence of the human error
    - ◊ components submitted to a repeated error
  - type of components which were affected (redundant or similar)
  - how the failure was discovered (during a programmed test or audit, during a not programmed checking or during a real event).

  This information was summarised in table 3.1, which is provided in section 3 of this report.

– Finally some general conclusions were made, which are also presented in the final section of this report.

2. Selected events

2.1 FREEZING OF AUXILIARY FEEDWATER PUMP MINIFLOW-LINES
Diane record No. 130 (Doel 2, 15 January 1987)

Event description:
Heavy frost with temperatures down to -18°C caused the miniflow lines on 2 of the 3 auxiliary feedwater pumps to freeze. The installed electric tracing on these lines was proven to be insufficient. The situation was restored to normal within 36 hours.

Causes and involved human factors:
The insufficient capacity of the installed tracing system can be characterised as a **design deficiency**. Apparently temperatures down to -18°C were not taken into account during the design of this system. The root cause is an insufficient consideration of possible environmental conditions during the design of the plant, which has the potential to cause CCF.

Safety significance:
The freezing of the miniflow-lines was detected by the operators during a routine surveillance. The actual safety significance of the freezing of the miniflow-lines was small as the valves in the injection lines from the auxiliary feedwater pumps to the steam generators are maintained in open position during normal operation. The inoperability of the miniflow-lines could cause pump degradation in the longer run of a loss of normal feedwater transient, when the auxiliary feedwater flow to the steam generators is reduced and the blocking of the miniflow-lines would be left unnoticed.

2.2 UNAVAILABILITY OF THE GROUNDWATER SUPPLY SYSTEM DUE TO COLD WEATHER
Diane record No. 85 (Tihange 1, 19 January 1987)

Event description:
During a functional test of the groundwater supply system, in order to verify its operability in spite of the cold weather conditions, it was discovered that the four pumps (4 x 50%) started correctly but no flow was obtained after opening of the valves in the connection lines to the normal service water system. The reason for the lack of water flow was the freezing of remaining stagnating water in the common collector on the discharge side of the four pumps. The concrete collector could be unfreezed with the heat of a torch and a ventilation system and the operability of the system was restored within 3 hours.

Causes and human factors involved:
The origin of the remaining water in the common collector could not be retraced with absolute certainty. The operating instructions ask to drain the collector after each operation of the system. It was believed that this draining operation was omitted or performed inadequately after a previous functional test. The importance of the draining operation, especially during

NOTEAVN.DOT - X:\WINWORD\MEMO\94-1\V001.DOC - 21/12/94 - 14:12

winter, was brought to the attention of the operators. The root cause for the event can be identified as an **operating deficiency after testing (omission error)**[1].

Safety significance:
The inoperability of the system was discovered during routine surveillance.
The function of the groundwater supply system is to remove residual heat in the case of an event, such as the failure of a dam downstream on the river, which affects the availability of the normal heat sink system. It is also the ultimate heat sink in the case of a station black-out situation.
The site specific situation is such that a simultanious loss of the normal heat sink as a result of the cold weather situation, which contributed to the loss of the groundwater supply system, is rather improbable.

2.3 PARTIAL FAILURE OF TURBINE BYPASS TO CONDENSER FOLLOWING TURBINE TRIP

Diane record No. 118 (Tihange 2, 19 October 1987)

Event description:
During the search for the defect in the instrumentation of the turbine oil system, which was responsible for a previous turbine and reactor trip, a false electrical contact caused a turbine trip. The turbine bypass to condenser relief valves opened as required, except for 2 valves for which the opening was considerably delayed (normal opening time in less than 3 s, opening delay up to 15 s). The failed turbine bypass relief valves are pneumatic valves of the type "failed closed" i.e. a build-up of air pressure underneath a membrane is needed to force the relief valve to its open position. During a local inspection it was noticed that eight (out of sixteen) relief valves, including the failed ones, showed air leaks at their servomotor. This lack of air-tightness was believed to be responsible for inadequate air pressure build-up, which resulted in the failure of the two relief valves.

Causes and human factors involved:
It was verified that, during the previous outage that year, the membranes of the eight affected relief valves were replaced. Inspection of these relief valves showed an inappropriate tightening of the fixation screw-nuts of the valve stems to these membranes, which ensure the tightness of the air compartment in the valve drive mechanism. The root cause of this event can be characterised as a **deficiency during maintenance (commission error)**. A **lack of requalification** of the system after the maintenance intervention can be identified as a contributing cause.

[1] within this report draining, venting and line-up tasks have been considered to be operating activities because they are of the responsibility of the licensed operating staff

Safety significance:
The partial unavailability of the system was discovered during a real event (no routine surveillance is provided for this system).
The turbine bypass system, which is not classified as a safety system, enables to create a fictive load on the secondary side in case of important load drops or a turbine trip. In this way reactor trip and respectively opening of the steam generator safety valves or pressuriser relief valves can be avoided. The proper working of the system allows to avoid the challenging of safety systems.

2.4 UNAVAILABILITY OF THE CONTAINMENT SPRAY SYSTEM
Diane record No. 166 (Doel 1/2, 1 November 1987)

Event description:
On the 9th of October 1987 the plants Doel 1 and Doel 2 (twin unit with common safety systems) were both in shut down condition and subjected to the annual black-out sequence tests, which include the functional testing of the common safety injection system. The Doel 1 plant remained in cold shutdown for refuelling, whereas the Doel 2 plant resumed power operation shortly after completion of the tests.
On the 1st of November it was discovered, during the monthly check of the position of the valves in the safeguard systems, that four valves on the discharge side of the containment spray pumps were closed and containment spray was not available to both units. Unit 2 had operated during 18 days with unavailable spray system, unit 1 being still in shutdown condition where the availability of the spray system is not requested by the Technical Specifications.

Causes and human factors involved:
The incident investigation showed that the four manually operated valves were operated for the last time during the common black-out sequence tests, for which these valves are closed as an additional precaution to avoid a spurious spray of the containment. It was concluded that these valves had been left in the closed position after completion of the test, although it was verified that the test procedure requested to re-establish the proper line-up of the spray system.
The reason for this omission could not be retraced with certainty. The following possible contributing factors could be identified:
- the checklist which is used at the end of the tests did not require to sign off the actions
- the valves which were used to isolate the spray discharge lines had no position indication in the control room
- the line-up of the safety systems was performed at the end of a long day of testing and trouble shooting (the tests started at 7.45 am; the line-up of the safety systems, which was performed simultaneously with an additional test of the emergency power boards, could only start after 7 p.m. of the same day).

Corrective actions were taken to address all these factors. The testing procedure was adapted in order to limit the duration of the black-out sequence testing on the same day to the maximum allowed continuous working time of 11 hours a day.
The root cause can be characterised as an an **operating deficiency after testing (omission error).**

Safety significance:
The unavailability of the system was discovered during routine surveillance.
The containment spray system can be used to reduce containment pressure after a loss of coolant accident. The containment ventilation system, including the corresponding cooling batteries, which remained operable during the event, provides a diverse system for containment pressure control. In addition the containment spray system should be used to remove iodine from the containment atmosphere in case of a design basis accident (DBA). For this function no diverse system is available. However during a DBA enough time would have been available to allow operator intervention on the closed isolation valves.

2.5 LOSS OF RESIDUAL HEAT REMOVAL SYSTEM DURING EMPTYING OF REACTOR POOL

Diane record No. 211 (Tihange 3, 8 June 1988)

Event description:
The plant was at the end of the refuelling outage when the water level in the reactor pool was lowered using a residual heat removal (RHR) pump aligned for this purpose. A second RHR-pump was running and aligned in order to cool the reactor core, the third one was tagged out for maintenance. The emptying of the reactor pool was initiated and continued in large flow mode, in violation of the operating procedures, even when the pool water level reached 30 cm above the pool bottom. The emptying operation continued until the level of the reactor coolant system loops was reached, when both RHR pumps tripped due to cavitation (in fact by actuation of the second level protection system). The reactor coolant system inventory was restored by the operators using the low head safety injection system. The operability of the RHR system could be restored by the operators after 36 minutes, after venting of the RHR pump casings.

Causes and human factors involved:
Three steps are provided in the operating procedures for reactor pool emptying: (1) large flow mode operation with a RHR-pump up to 30 cm above the pool bottom, (2) low flow mode operation with the same pump up to the vessel flange, (3) followed by use of a small spent fuel pool pump.
During the event this switch of operation mode was not respected by the local operator, who did not monitor permanently the pool level (because he was busy with the switching of the refuelling water storage tanks). Contributing factors were the lack of indication of the reactor pool level in the main control room and the fact that a shift turnover, which was not performed locally, occurred at the time when the water level reached the pool bottom.
The operating procedures related to this activity were modified and a graduated ruler was installed along the wall of the reactor pool.
The root cause can be characterised as an **operating deficiency: inadequate work organisation and planning, inadequate work practices (commission error).**

Safety significance:
The actual safety significance of the loss of the RHR-system, resulting in a limited reactor coolant heat-up, was minor due to the fact that it occurred at the end of a refuelling outage, when residual reactor core heat is low, and the fact that the pumps are adequately protected by the provided protection system. However prolonged cavitation of the RHR-pumps, if not stopped by an automatic protection signal as at the Tihange 3 plant, could result in a potential degradation of these pumps. This event shows also the importance to maintain reactor coolant make-up systems , such as low head safety injection, operable in shutdown conditions (not requested by Technical Specifications) and to maintain one of the RHR trains, if available, in standby for reactor cooling when the reactor inventory is reduced.

2.6 TRIP OF ALL SERVICE WATER PUMPS DURING MAINTENANCE ACTIVITY
Diane Record No. 217 (Doel 1, 29 September 1988)

Event description:
During the intervention of a maintenance crew on the drive mechanisms of the sliding gates, on the suction lines of the main circulation water pumps, the open limit switches of both gates were inadvertently touched within a time lapse of 2 minutes, causing the two pumps to trip followed by turbine and reactor trip.

Causes and human factors involved:
Spurious actuation of the limit switches is normally prevented by a protective cap, which had to be removed by the maintenance personnel in order to be able to inspect, clean and lubricate the sliding gate drive mechanisms, in preparation of a planned shutdown of the plant. The maintenance crew were not fully aware of the implications of a spurious actuation of the limit switches, thinking that this affected only the valve position indication in the main control room. This was the root cause of the event, which can be characterized as a lack of awareness due to a lack of knowledge of the maintenance staff. A contributing factor was the fact that such maintenance activities had not to be authorised by the operation crew, the operation staff being unaware of the maintenance intervention on these valves and the potential risks involved by this intervention.
Corrective actions were taken with regard to maintenance practices and procedures (inclusion of precautions), improving attention of mechanical maintenance crews for electrical components such as switches, push buttons and relays and improving communication with main control room staff.

Safety significance:
The main circulation water system is not a safety system. In addition to the provision of cooling water to the turbine condensers, it provides a first line heat sink for the component cooling system. When this system is lost, an emergency cooling system is started, consisting of a closed loop circuit with atmospheric cooling towers. The loss of the main service water system challenges in this way the actuation of a safeguard system.

NOTEAVN.DOT - X:\WINWORD\MEMOS\AVD01.DOC - 21/12/94 - 14:12

2.7 SUCCESSIVE TRIPS OF DIESEL GENERATOR DUE TO SPURIOUS ACTUATION OF OVERSPEED PROTECTION

Diane record No. 255 (Doel 4, 14 February 1989)

Event description:
During the performance of a requalification test, after the yearly overhaul, of a bunker (second protection level) diesel generator (DG), a trip occurred during the run phase due to a spurious actuation of the overspeed detection device. Following an intervention on the overspeed protection setpoint (at 1120 rpm), the DG started with success. The operability of the DG was confirmed by a load rejection test, during which the maximum rotation speed reached 1090 rpm.
A few days later it was decided to remove a temporary compression measurement instrumentation, which is installed every year after the overhaul. A new requalification test was decided, during which the overspeed protection device tripped again during the run phase of the DG.

Causes and human factors involved:
The adjustment of the overspeed setpoint is done by the maintenance staff by means of an adjusting screw without pointer nor dial: the required position of the screw is relative to the position where the calibrated device trips at nominal rotation speed (1000 rpm). The design of the adjusting screw was identified as the main cause of the wrong adjustment of the overspeed protection setpoint. The exact scenario which resulted in the successive trip device failures could not be retraced with certainty. A contributing factor however was the fact that the maintenance personnel have to manipulate the same screw for venting of the hydraulic circuit of the overspeed protection system. It was supposed that during this latter operation, which requires an additional temporary two turns rotation of the screw in the outward direction, a human error was made which can be characterised as a deficiency during maintenance. It was also established that the maintenance procedures did not provide sufficient detailed instructions regarding the setting of the adjustment screw.

Safety significance:
In this event no actual CCF occurred which affected redundant safety components, although successive failures occurred of the same equipment, which were not corrected to satisfaction. As the resulting failure apparently passed through the first requalification program and was only detected by chance in a subsequent requalification test, which was performed for a not related reason, this type of failure is of concern and could potentially lead to a CCF of the diesel generators (3 in total).

2.8 LOSS OF BOTH FEEDWATER PUMPS DUE TO LOSS OF A SINGLE ELECTRICAL BUSBAR

Diane record No. 265 (Tihange 3, 18 October 1989)

Event description:
During normal operation conditions, both turbine-driven feedwater pumps are provided with two lubricating pumps, one in operation and one in standby, which are fed from two independent 380V power supply boards, themselves connected to two independent 6.6 kV power boards. Both power supplies are common to the two feedwater pumps. However the lubricating pumps are normally operated in such a way that a loss of the two feedwater pumps due to a loss of lubrication, resulting from the loss of a single power busbar, can be avoided. In this event the burning of a voltage transformer following a temporary short-circuit occurred on one of the two 6.6 kV power boards. The operators decided to cut the power to this board, which resulted in the unexpected loss of both feedwater pumps, followed by a very low water level in all the steam generators and a reactor trip.

Causes and human factors involved:
It was found out that during the event the four lubricating pumps were all connected to the same 380 V busbar, which lost its tension due to the operator action. The reason for this could be traced back to a previous periodical test of a DG. This test requires to transfer during a short time, only for the purpose of the test, all the loads of the corresponding 380 V busbar of the same train to another busbar of a different train. After the completion of the test the original configuration was not restored, which is an operating deficiency after testing (omission error). A contributing element was the lack of instructions in the test procedure to re-establish the redundancy of power supplies.

Safety significance:
The normal feedwater system is not a safety system in itself. However the loss of normal feedwater challenges the actuation of the safety systems and may be a precursor to core melt.

2.9 LOSS OF PRIMARY PUMP EMERGENCY SEAL INJECTION SYSTEM

Diane record No. 303 (Doel 4, 22 June 1990)

Event description:
During a cold shutdown for intervention on several leaking valves, approximately one month after the yearly outage, a loss of the primary pump seal injection, delivered by the chemical and volume control system, occurred due to an error in the depadlocking of a component in this system. As provided by the bunkered second level protection system, the two common positive displacement pumps of the emergency seal injection system started, one after the other, on detection of the loss of seal injection flow. However only a very small flow to one of the three primary pump seals was noticed. During a prompt local investigation of the line-up of the system, the operator found, from his interpretation of the valve position indication, that the throttle valves in each of the three injection lines were in closed position. He immediately opened the throttle valves and the emergency seal injection flow was adjusted.

NOTEAVN.DOT - X:\WINWORD\MEMO94-YV001.DOC - 21/12/94 - 14:12

Two months later a functional test of the emergency seal injection was performed, during which it was noticed that the injection flow to the three primary pumps was not properly balanced and two of the three pumps received in fact an insufficient seal flow. In addition it was observed that the head pressure (220 bar) of the seal injection pumps was quite above the setpoint (213 bar) of the safety valve on the discharge side of the pumps, resulting in a partial loss of seal injection flow. An inspection of the throttle valve positions showed they were opened over only 1/6 to 1/8 of a turn (a full opening corresponds to 7 turns).

Causes and human factors involved:
The procedure which was used to adjust the seal injection flow to the three primary pump seals was critically analysed. This procedure asked to adjust the injection flows to each pump to 1.5 m³/h. This was in fact an inappropriate instruction, as the function of these valves in the original design was to balance the flow delivered by the piston pump equally to the three primary pumps. The attempt to adjust the injection flow resulted in an almost closed position of the throttle valves and in a deviation of the seal injection flow through the safety valve on the discharge side of the positive displacement pump. In addition it was supposed that the pressure peak occurring at the head side of the starting piston pump could push the valve disk against its seat, resulting in a no-flow situation. In accordance with the preoperational test procedures of the plant the seal injection flow was readjusted to ± 2.6 m³/h, corresponding with a ± 2 turns valve opening and resulting in a piston pump head pressure of 170 bars. The operating procedures were corrected accordingly.
Root causes of this event are the incorrect implementation of design data in the operating procedures **(document control problem)** as well as insufficient analysis of previous low seal injection flow occurrences **(operating deficiencies)**.

Safety significance:
The emergency seal injection system is a second level (bunkered) protection system, which is provided to avoid loss of coolant accident scenarios as a result of an accident of external origin (plane crash, external explosion ...) or a station blackout condition (i.e. loss of off-site power and loss of first level protection diesel generators). The faulty operating procedures, which were in use since the start-up of the plant in 1985, could potentially have resulted in a primary pump seal degradation in such a hypothetical accident.

2.10 UNAVAILIBILITY OF HIGH PRESSURE SAFETY INJECTION SYSTEM
Diane record No. 283 (Tihange 2, 3 July 1990)

Event description:
In the course of the start up of the plant (reactor below 10% rated power), it is discovered, during an independent not programmed check of the line-up of the safety systems, that the isolation valves in each of the three high pressure safety injection lines to the cold legs of the primary circuit are in closed position and that they are disconnected from their power supplies. This situation of violation of Technical Specifications (TS) was supposed to exist from the 30th of June, when the temperature of the reactor coolant system was brought above 180°C (mode 3).

Causes and human factors involved:
The different trains of the high pressure safety injection system (HPSI) had been lined up in conformity with the operating procedures on the 22th respectively on the 28th of June (HPSI pumps still disconnected when below mode 3) . On the 28th and 29th of June it was required to close (but not to disconnect) the isolation valves again in the HPSI lines to the cold legs of the reactor coolant system, in order to verify the leaktightness of the check valves downstream of these valves. It is believed that , although this action was not requested by the test procedure, the valves were disconnected from their power supplies in analogy with what is required by the line-up procedures for the isolation valves on the injection lines to the hot legs of the primary circuit. The corresponding test procedure itself does not provide specific instructions to restore or verify the proper line-up of the system. However, on the 30th of June after completion of this test, the operating procedures instructed twice the operators to verify the proper line-up of the safety injection system without however giving specific instructions regarding the required position of the valves. As a result of these instructions the HPSI pumps were reconnected to their power cabinets (only allowed when passing to mode 3) and the line-up of the system was verified on the basis of the synoptic in the main control room (valve position is indicated in the CR). From the analysis of the process computer printout it could be demonstrated that the HPSI isolation valves have not been manipulated after the 30th of June 5 p.m. (the printer had been inoperable between 11 a.m. and 5 p.m. that day, the information could not be retrieved from the magnetic tapes either).
Several successive human errors can be identified in this event which resulted in a TS violation:
– omission to re-establish the required line-up of the HPSI system after completion of the leaktightness test procedure, with as a contributing cause the lack of specific instructions in the test procedure to do so;
– disconnection of the power supplies of the HPSI cold leg injection isolation valves (commission error); it should be noted that these valves receive an opening command when safety injection should occur; however the opening would be too slow to avoid fuel damage as a result of a DBA;
– failure to observe the closed position of the valves during the verification of the line-up of the system as instructed by the procedure used to change operating modes;
– failure to observe the closed position of the valves during the verification of the line-up of the system as instructed by the procedure applied when changing TS-modes (independent verification of the operability of the safety systems as required by TS).
All these errors can be characterized as operating deficiencies.
As a result of this event, procedures and administrative provisions have been improved to avoid recurrence.

Safety significance:
This event resulted in the total unavailability for more than 3 days of an important safety system. Several layers of defence were breached in order to come to such a situation, which was only discovered that soon by chance due to an independent not programmed checking. In addition the verification of the position of these valves is performed monthly as required by the surveillance requirements of the TS.
This event has been rated as a level 2 event on the INES scale.

NOTEAVN.DOT - X:\WINWORD\MEMO\94-YV001.DOC - 21/12/94 - 14:12

2.11 WRONG CALIBRATION OF ALL MAIN STEAM SAFETY VALVES
Diane record No. 384 (Doel 1, 17 May 1991)

Event description:
During a QA-audit of the working methods and organisation related to the calibration of safety valves, it was discovered that the reference document, which was used to calibrate the main steam (MS) safety valves, provided setpoint values which were 1 bar above the nominal values required by the Technical Specifications. Investigation of the actual safety valve settings, during the last performed calibration, showed that for the Doel 2 plant the set values were just within the limiting conditions for operation. However for the Doel 1 plant, 6 out of 12 safety valves had to be recalibrated. The 2-loop plant was brought to cold shutdown for this purpose.

Causes and human factors involved:
Several documents were in use which provided different values, some in different units (such as bar rel, ata and just bar). The two reference documents which were used by maintenance staff for calibration purposes were coherent in providing systematically setpoint values which were 1 bar to high for the MS safety valves. The calibration of these valves was witnessed by an independent inspector who did not question the setpoint values provided by the reference documents used by the utility. The observed cause of the wrong calibration is a confusion about the setpoint values to be applied. The root causes were classified as a **lack of management program, i.e. inadequate document control** resulting in use of setpoint values which differ from TS requirements and **inadequate working methods** resulting in the use of several contradictory documents.

Safety significance:
A wrong calibration of the MS safety valves could theoretically lead to a challenge of the integrity of the steam generators during an overpressure transient (such as loss of load with failure of the non-safeguard steam relief valves). This event was rated as a level 1 event on the INES scale.

2.12 MICROBIOLOGICAL CONTAMINATION OF EMERGENCY DIESEL GENERATOR FUEL TANKS
Diane record No. 397 (Doel 1/2, January 1992)

Event description:
Following the discovery of biological contamination of the turbine lubricating and regulating oil circuits, it was decided to take some samples of the four emergency diesel generator (DG) fuel tanks (on site power supply for ECCS), which are common to both units (twin-plant). Analysis of these samples showed also biological degradation of the fuel contained in these tanks. A similar analysis of fuel tank samples of the DG's, providing power supply in the case of an accident of external origin, was negative.

Causes and human factors involved:
The bottom layer of fuel was drained from the DG fuel tanks. A separate water phase was not observed but analysis of this bottom layer showed the presence of enough water to explain the development of bacteria. In addition during the analysis of the remaining fuel in the tanks traces of mildews were found. Development of microbiological contamination of the DG fuel could have been avoided through an adequate surveillance program of the fuel in the tanks (surveillance program deficiency).[2]

Safety significance:
The bacteria which were found in the DG fuel were able to break down the complex hydrocarbon chains, resulting in a degradation of the fuel quality. This phenomenon could jeopardise on site power capacity by affecting the ability of the DG's to provide rated power.

2.13 INSUFFICIENT COOLING CAPACITY OF EMERGENCY DIESEL GENERATORS FOLLOWING MODIFICATION

Diane record No. 400 (Doel 1/2, 21 May 1992)

Event description:
During a newly introduced overpower-test (at 1.1 times rated power) of an emergency diesel generator, the DG is tripped by the operator after 2 minutes due to the appearance of a "high oil temperature" alarm. The test is repeated twice the same day , this time at rated power (2100 kW), resulting in a similar alarm after 10 to 20 minutes, depending on the time of the day. The next day the three redundant DG's are subjected to a rated power test. This time oil temperatures are again above allowable values but remain just below alarm threshold.
On the following days the first DG is subjected again to nominal power and overpower tests, with outside temperatures reaching 28°C. This time the diesel is allowed to continue running until the high cooling water temperature protection trips the DG after 1 to 1.5 hour.
From the analysis of the test data it is shown that the capacity of the installed cooling batteries allows the DG's to run at only 85% of rated power, with design basis outside temperatures of 30°C.

Causes and human factors involved:
The high oil and cooling water temperatures occurring during the tests of May were a direct result of the high outside temperatures. The three other DG were already tested previously with lower outside temperatures and declared operable. The overpower test was performed as the result of a new surveillance requirement in the recently adapted Technical specifications of the plant.All DG had been modified shortly before this requalification test campaign: the nominal power of the DG had been increased as a result of a safety revaluation of the plant, showing the need for larger on site emergency power capacity. During the redesign of the DG system it was apparently omitted to redesign the cooling system of the DG in order to be able to take the additional heat charge under design base conditions. This failure was also not

[2] for the purpose of this report the surveillance of the quality of fuel is considered as a maintenance activity

observed during the design review of the modification. This event was categorised as a design deficiency. It was exacerbated by a failing design review process.

Safety significance:
Technical Specifications require a minimum of 3 operable DG (including single failure considerations). During the first phase of the design basis reference accident the 2 running DG are loaded up to power levels of 2300 to 2400 kW (when supplying to 2 emergency power boards at the same time). After 5 minutes the operator is allowed to reset the safety injection signal. Subsequently he is allowed to decrease DG load by stopping some less important emergency equipment.
The resulting long-run capacity of the DG was insufficient to face the design basis reference accident. In addition an exceeding of allowable cooling water temperatures, at design basis outside temperatures, would have occurred after only 15 to 20 minutes, which was considered to be rather short. Awaiting a design modification of the DG cooling batteries it was decided to adapt the TS of the system (shorter allowable outage times for DG's) and to provide the operator with simple, quick to implement, instructions for unloading DG's, which supply 2 emergency power boards.
This event was rated as a level 1 event on the INES scale.

2.14 GAS BINDING OF 2 CONTAINMENT SPRAY PUMPS DURING PERIODIC TEST
Diane record No. 429 (Doel 1/2, 3 November 1992)

Event description:
During a monthly functional test of the containment spray pumps, it is discovered that for 2 pumps , tested sequentially and taking suction from the nearest refuelling water storage tank (RWST), no flow is obtained after start-up. The operators are able to re-establish for both pumps head pressure and flow after temporally closure of the isolation valves on the discharge side of both pumps.
When the test is repeated with both pumps lined up to the second RWST, which is connected with the first one and all four containment spray pumps through a common collector, it is noticed again that air is sucked in from the collector. The operability of the system can be re-established through an adequate venting of the common suction collector.

Causes and involved human factors:
During the previous outage, which ended two weeks before the event, the common collector of all four containment spray pumps was partially drained to allow an intervention on one of the two isolation valves on the suction line from the RWST closest to the pumps which failed during the event. After this intervention the collector was filled again and vented. In accordance with the operating procedures, applicable to the case of partial draining on a system for intervention on an valve, the requalification of the system was limited to a stroke test of the isolation valve on which the intervention took place. The failure of two pumps during a consecutive periodical test showed that the system was not adequately vented and that some air was trapped in the suction line of the pumps as well as in the common collector of the system. The monthly functional test procedures do not ask to line-up the containment

spray pumps consecutively to both RWST. In this way the possibility exists that the presence of an air pocket in the common collector would not have been detected by the test procedures. The root cause can be characterised as a deficiency of the requalification of the system (operating deficiency) after intervention for maintenance.[3] [].

Safety significance:
The partial inoperability of the system was discovered during a routine surveillance. A combination of the failure of 2 out of 4 pumps with a loss of off-site power and a single failure of the on-site power supply system could have resulted in a temporary loss and delayed actuation of the complete system.
The containment spray system can be used to reduce containment pressure after a loss of coolant accident. The containment ventilation system, including the corresponding cooling batteries, which remained operable during the event, provides a diverse system for containment pressure control.
In addition the containment spray system should be used to remove iodine from the containment atmosphere in case of a design basis accident (DBA). For this function no diverse system is available. However during a DBA enough time would have been available to allow operator intervention to restore at least partial recovery of this system function.
This event was rated as a level 1 event on the INES scale.

2.15 WRONG LINE-UP OF ALL STEAM GENERATOR BLOWDOWN LINES
Diane record No. 450 (Doel 3, 22 April 1993)

Event description:
During the performance of a functional test of the second level protection system acting on the six isolation valves on the 3 steam generator blowdown lines (2 valves on each line), it is noticed that for one of the valves the anticipated signals during the test are not received. The functional test in question is a "blocked test" with reduced voltage on the actuation relays in order to avoid actual closure of the valves during operation. As the test-circuit itself was suspected to be failing, an investigation of the test circuit was performed without result. A subsequent investigation of the valves themselves showed that all of them were mechanically locked in open position. The valves are pneumatic valves of the type fail closed and are provided with a hand wheel, which allows to lock the valves in open position.

Causes and human factors involved:
During a previous not programmed cold shutdown for a primary to secondary system leakage, which ended on 4th of April 93, it was necessary to drain the secondary side of all steam generators (SG) through the blowdown (purge) system. As the actuation of the second level of protection system on low SG level cannot be blocked, it was necessary to lock the isolation valves mechanically in open position. This locking intervention was not covered by the operating procedures, nor was it submitted to administrative control. As the number of

[3] within this report requalification tasks have been considered to be operating activities because they are of the responsibility of licensed operating staff

interventions was limited during the shutdown of the plant, it was decided not to apply the usual requalification procedures, which require a complete independent line-up control of all safety systems. Instead each intervention was administratively followed through a padlocking procedure. The depadlocking procedure was used to verify the correct line-up of each system on which an intervention was made. As the mechanical locking of the isolation valves was not covered by the padlocking process, it was not removed during the line-up of the system after intervention.
The following contributing causes were identified:
- **inadequacy of configuration control**
- **inadequate requalification of a system after intervention for maintenance** (not sufficient independent controls)
- **lack of operating procedure** for draining of steam generators (required line-up was not defined a priori).

All causes can be characterized as **operating deficiencies.**

Safety significance:
The blowdown isolation valves, which were affected in the event, receive
- a containment isolation signal from the first level of protection, the operability of which is not requested by Technical Specifications (TS) as the blowdown lines are not considered to be containment penetration lines
- a second level protection isolation signal on very low steam generator level; this protection which helps to maintain SG water inventory after an accident of external origin, is submitted to TS.

An additional isolation valve is provided on each line downstream these isolation valves. It receives an isolation signal from the first protection level in the case of loss of normal feedwater or low SG level (protection against feedwater line break accident). The mechanical locking of these valves during the SG draining operation was not necessary as the actuation by this first level of protection can be blocked.
This event was rated as a level 1 event on the INES scale.

2.16 ERROR DURING LAST MINUTE ADJUSTMENT OF REACTOR PROTECTION SETPOINT

Diane record No. 452 (Doel 3, 13 September 1993)

Event description:
The plant was in hot shutdown after an outage during which the steam generators had been replaced and several reactor protection setpoints had been modified as a result of a power uprating of the plant. The performance of functional tests of the reactor protection system was still running (on the critical path for start-up), when discussions on the final values of the parameters for several reactor protection signals were still going on. As a result of this discussion it was decided among others to modify the time constants of a newly introduced lead lag module in the overtemperature protection signal (protection against DNB in rod bank withdrawal accident). The performance of these modifications had to be performed as well on the critical path to start-up of the plant, following a modification procedure for urgent

modifications. During the adjustment, a confusion was made between the dynamic module in the protection formula itself, which should be left unchanged, and the newly introduced dynamic module on the delta T-measurement , which had to be adjusted. During this modification the incoherence between the as-found and the to be modified values of the time constants was noticed and reported. However due to time constraints it was decided to proceed with the modification. The reactor was then made critical for physical tests. After comparison of the values in the different documents, subsequent to the noticed incoherence during the adjustment of the protection setpoints, the confusion error was discovered. The reactor was made subcritical in order to correct the setpoints.

Causes and human factors involved:
The following root causes were identified:
– From the analysis of the event it was clear that there was a **communication error** between the person who gave instruction to perform the adjustments of the reactor protection and the staff responsible for the execution of the modification: the **technical instructions were inaccurate.**
– When the incoherence between as-found and to be modified values was detected, the technicians consulted several field documents. However these documents were not yet updated and did not mention the newly introduced dynamic module: **documentation deficiency.**
– Both instruction and performance of the modification happened during the start-up phase of the plant (on critical path). In the perception of the staff involved, the modification was prepared and executed under **time pressure.**
– Because of the large amount of setpoint modifications in the project a specific quality assurance procedure, with additional checks and precautions, had been established. Because of the urgency of this particular last minute modification, this QA procedure was not followed and the usual QA-rules were applied during the adjustment.
For the purpose of this report this error has been characterized as a **maintenance deficiency,** as the adjustment of the setpoints is of the responsibilty of I&C technicians.

Safety significance:
Thanks to the questioning attitude of the instrumentation staff an additional check, not prescribed by the applied procedure, was made after the modification and the anomaly could be detected in a timely manner (although critical and formally in violation of Technical Specifications, the plant was not yet at power). Without this questioning attitude related field documents and test procedures would have been adapted erroneously as well, so that the error would have been left undetected during the following periodical tests.

2.17 TOTAL UNAVAILABILITY OF FIRE PROTECTION SYSTEM DURING REFUELLING OUTAGE

Diane record No. 476 (Doel 4, 15 April 1994)

Event description:
Each of the three fire protection pumps has a common water intake with a separate emergency cooling water system train. During the refuelling outage of the plant, an in-service inspection

had to be performed on components of a system which is supported by this emergency cooling water system. This intervention, which was performed consecutively train by train and subjected to a formal padlocking and requalification procedure, required a draining of the common water intake collector. In order to avoid a dry running of the fire protection system pumps, these pumps were also disconnected, one train after the other, from their respective power supplies. At the end of the intervention on two of the three trains, it was omitted during the depadlocking/requalification procedure to reconnect the fire protection system pump to its power supply. This situation resulted in a partial unavailability of the fire protection system as 2 pumps are required to cope with a design basis fire. On the 14th of April the third pump, which had been reconnected correctly to its power supply after the above described intervention, had to be padlocked again for an additional intervention on that system. This situation resulted in a complete loss of the fire protection system.

During a functional test of the fire protection system on the 15th of April, the pressure in the fire protection system collectors dropped almost immediately to zero and a lack of water was observed. After investigation it appeared that the 3 fire protection pumps were out of service and that the connection line between the fire protection system collectors of the Doel 3 and Doel 4 plant was closed as well.

Causes and human factors involved:
The procedures for padlocking/depadlocking which are applied during refuelling outages are different from those which are used when the plant is not in an outage regime: instead of using a closely linked padlocking/depadlocking procedure for components subjected to an intervention, the requalification of systems, which were previously released for intervention during an outage, are requalified in a global way through the application of predefined requalification procedures based on a predefined padlocked state of the system. If additional components, which are not part of the predefined padlocked state of the system, have to be padlocked, a separate depadlocking/requalification procedure should be applied for these components.
In this event the padlocking of the three fire protection system pumps was not part of the predefined padlocked state of the system. However the operators apparently assumed that this was the case and omitted to reconnect and requalify these pumps separately (only one pump was reconnected to its power supply by chance).
In addition the operators omitted to apply an administrative procedure, which requires to establish for each Technical Specifications related component or system a card, which is used to identify an unavailable safety component/system and to report its inoperability to plant management staff.
The root causes can be characterised as **deficiencies of configuration control of safety** systems during the outage of the plant and **non appliance of administrative procedures.**

Safety significance:
The event resulted in a partial unavailability of the fire protection system (2 pumps inoperable), during a plant outage, for 6 days and a total unavailability of the system (3 pumps inoperable) for 1 day.

3. Conclusions

The results of the additional analysis is represented in table 3.1 and illustrated in figure 3.1. The numbers between brackets in the following text refer to the number of corresponding events.
The following findings could be obtained from the analysis of the selected events:

- **Mode of operation**

  A majority of the events (11 out of 17), which were selected for human factor related CCF, showed human performance problems during the outage-phase of the NPP. Among these, human performance deficiencies, which are specific to the start-up phase, are noteworthy (5). This conclusion does not come as a surprise.
  Two events are linked to power operation. The occurrence of the remaining events (4) are independent from the operation mode.

- **Type of activity/ personnel category**

  For the majority of events (9), the human performance deficiency was linked to a maintenance task. However one should make the distinction between the events, where the error was made during the maintenance task itself (6), and events where the error was made by the licensed operators (3).
  Maintenance errors are diverse: inappropriate tightening or adjustment of screws, touching of limit switches during operation, erroneous calibration of safety valves, erroneous adjustment of reactor protection setpoints and inadequate surveillance of safety systems. Operation errors linked to maintenance activities are inadequate line-up of systems, venting of systems and configuration control after or during maintenance .

  A second important family (4) consists in events where the human performance deficiency is linked to a testing activity. However in this case all human errors were performed by licensed operation staff at the end of the test during the reconfiguration of the system: inadequate draining and line-up of systems.

  Further activities where human errors were observed are design tasks (2) and operation tasks (2).

- **Behavioural factor/ use of procedures**

  Omission errors form the largest part (7) of the group of selected events. These errors correspond to the 2 groups identified above , where they were attributed to licensed operating staff and linked to maintenance and testing activities. In many cases (5), it was observed that the instructions or the procedures (technical and administrative) were not followed. In some of these cases (4) a lack of comprehensiveness of the supporting procedures was identified as a contributing factor.

  A second group was the lack of knowledge of the intervening personnel (4). The analysis

NOTEAVN.DOT - X:\WINWORD\MEMO\94-YV\001.DOC - 21/12/94 - 14:12

showed that a correlation exists with the errors which were attributed to maintenance staff. This stresses the need for more attention to training programs for maintenance staff. In all cases of this group, a lack of comprehensiveness of the supporting documents was identified as a contributing factor.

Further contributors were confusion errors (2), which were also linked to maintenance tasks, and lack of attention (2), attributed to licensed operators.

- **Type of dependency/ affected components**

For a large group of selected events (7), it could be observed that the existance of a common instruction (or procedure), affecting redundant (or similar) components, contributed to the simultanious failure of these components. In the majority of cases (5), this instruction was considered to be inadequate (document control problems or procedure not adapted to the situation). In 2 cases the instruction was omitted. In all cases of this group, one can speak of a single human error, conditioned by a common instruction or procedure.

For a second important group (5), the dependency had to be attributed to a common condition of the affected components. In most cases (4) this condition was the result itself of the human performance problem (design deficiencies, redundant components supported by single support system, surveillance deficiency). In one case the common condition was inherent to the system configuration and independent of the occurring human error. In all cases of this group, it was observed that the failure was due to one single human error. In addition its was observed that for this group all events involved the failure of redundant components.

In a third group (3) the human error was simply repeated on redundant or similar components. The contributing factors were in these cases lack of knowledge (with as additional contributor lack of supporting documents) and omission to apply an (administrative) procedure .

For a fourth group (2), the dependency is due to the existance of a common component, which was affected by the single human error. In both cases the event involved the failure of redundant subsystems (inadequate draining or venting of common collectors).

- **Way of discovery**

In most cases (9), the failing components or systems were discovered during a programmed periodical test. This means that in a large number of cases the provided test programmes enable to recover from a human error, which was made previously on the system. However in 2 of these cases the deficiency of the system, which was due to a design failure, could only be discovered thanks to the exceptionnal climatological conditions at the time of the test. In one case the error was detected through an audit of the supporting documentation.

In 5 cases the error was discovered (or occurred) during a real event and could not have been prevented by existing provisions. In 2 of these cases the failure affected systems which are considered to be balance of plant systems and which are not submitted to periodical surveillance or functional tests. In 2 cases the human error was performed during operation itself and affected immediately in an observable way the plant status.

Finally, in 3 cases the failed system was discovered (by chance) during a not programmed checking.

– **Corrective actions**

From the above selection of events, the following possible corrective actions have been identified to avoid CCF due to human errors:

◊ reduce perception of time pressure during the start-up phase
◊ improve training of maintenance staff
◊ improve procedure support for maintenance staff
◊ improve communication between operating and maintenance or testing staff
◊ improve procedures for line-up of safety systems following testing or maintenance activities (more explicit check-off lists for required system configuration)
◊ improve requalification procedures for safety systems
◊ improve configuration control procedures during outages
◊ introduce redundant and diverse verifications to cope with possible omission errors
◊ improve document control programme
◊ improve design (modification) review procedures
◊ perform more FMAE-analysis of critical components in order to detect latent weaknesses in existing maintenance, testing and surveillance procedures
◊ avoid common components in redundant safety systems; give special attention to such components in existing designs

NOTEMAN.DOT - X:\WINWORD\MEMOS\AVN94-015.DOC - 21/12/94 - 14:12

Table 3.1

No.	Event	Mode of operation	Type of activity				Personnel category	Behavioural factor	Procedure was	
			design	testing	maintenance	operation			not followed	not adequate
130	Freezing of AFW pump miniflow lines	independent (operation)	X				designer			
85	Failure of groundwater supply system due to cold weather	independent (operation)		X			licensed operator	omission	X	
118	Failure of turbine bypass to condenser	outage			X		maintainer	lack of knowledge		X
166	Unavailability of containment spray system	outage (start-up)		X			licensed operator	omission	X	
211	Loss of RHR during draining of reactor pool	outage (cold shutdown)				X	licensed operator	lack of attention	X	
217	Trip of all service water pumps	operation			X		maintainer	lack of knowledge		X
255	Successive trips of DG due to spurious overspeed detection	outage			X		maintainer	lack of attention		X
265	Loss of feedwater pumps	operation		X			licensed operator	omission		X
303	Loss of primary pump emergency seal injection	outage (start-up)				X	licensed operators	lack of knowledge		X
283	Unavailibility of HPSI system	outage (start-up)		X			licensed operator	omission; lack of attention	X	X
384	Wrong calibration of all main steam safety valves	outage			X		maintainer	confusion		X
397	Microbiological contamination of emergency DG fuel tanks	independent (operation)			X		maintainer	lack of knowledge		X
400	Insufficient cooling capacity of emergency DG	independent	X				designer			
429	Gas binding of containment spray pumps	outage			X		licensed operator	omission		X
450	Wrong line-up of SG blowdown lines	outage (start-up)			X		licensed operator	omission	X	X
452	Wrong adjustment of reactor protection system	outage (start-up)			X		maintainer	confusion		X
476	Total unavailibility of fire protection system	outage			X		licensed operator	omission	X	

Table 3.1 (continued)

No.	Event	Type of dependency				Affected components are		Discovered (or occurring) during		
		common component	common instruction	common condition	repeated error	redundant	similar	programmed testing or audit	not programmed checking	real event
130	Freezing of AFW pump miniflow lines			X		X		X		
85	Failure of groundwater supply system due to cold weather	X				X		X		
118	Failure of turbine bypass to condenser				X		X			X
166	Unavailability of containment spray system		X			X		X		
211	Loss of RHR during draining of reactor pool			X		X				X
217	Trip of all service water pumps				X		X			X
255	Successive trips of DG due to spurious overspeed detection				(X)	(X)		X		
265	Loss of feedwater pumps			X		X				X
303	Loss of primary pump emergency seal injection		X				X			X
283	Unavailibility of HPSI system		X			X			X	
384	Wrong calibration of all main steam safety valves		X				X	X		
397	Microbiological contamination of emergency DG fuel tanks			X		X			X	
400	Insufficient cooling capacity of emergency DG			X		X		X		
429	Gas binding of containment spray pumps	X	X			X		X		
450	Wrong line-up of SG blowdown lines		X			X	X	X		
452	Wrong adjustment of reactor protection system		X			X			X	
476	Total unavailibility of fire protection system				X	X		X		

(X): no actual CCF occurred

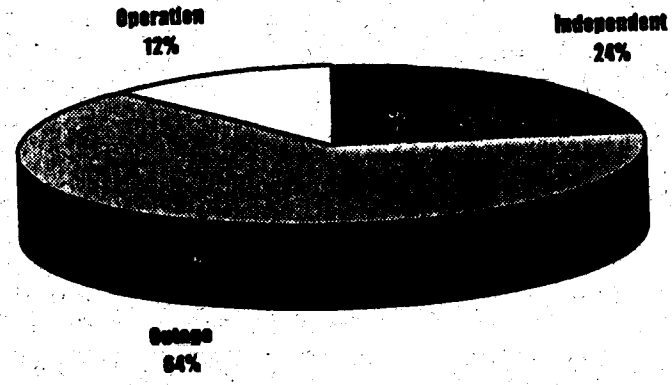
Table 3.1 (continued)

No.	Event	Corrective actions addressing human factor related deficiencies
130	Freezing of AFW pump miniflow lines	
85	Failure of groundwater supply system due to cold weather	training of licensed operating staff
118	Failure of turbine bypass to condenser	
166	Unavailability of containment spray system	improvement of checklists (inclusion of check-offs); use of valves with position indication in CR for isolation of lines during testing; limit working time
211	Loss of RHR during draining of reactor pool	improvement of operating procedures; provision of graduated ruler in reactor pool
217	Trip of all service water pumps	training of maintenance staff
255	Successive trips of DG due to spurious overspeed detection	improvement of maintenance procedures
265	Loss of feedwater pumps	improvement of test procedures
303	Loss of primary pump emergency seal injection	improvement of operating procedures
283	Unavailibility of HPSI system	improvement of operating procedures and more strict administrative provisions
384	Wrong calibration of all main steam safety valves	improvement of operating documentation; improvement of document control programme
397	Microbiological contamination of emergency DG fuel tanks	
400	Insufficient cooling capacity of emergency DG	
429	Gas binding of containment spray pumps	improvement of requalification procedures; more extensive testing of system
450	Wrong line-up of SG blowdown lines	writing of operating procedure for draining of steam generators
452	Wrong adjustment of reactor protection system	indoctrination that provided QA-procedures should always be followed even under time pressure; removal of time pressure perception for critical actions in start-up phase
476	Total unavailibility of fire protection system	improvement of padlocking procedures for induced unavailabilities

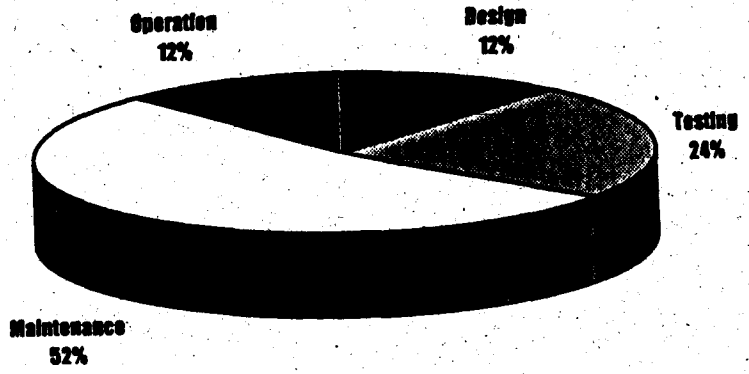
NOTEAWI.DOT - X:\WINWORD\MEMO\94-YV001.DOC - 21/12/94 - 14:01

FIGURE 3.1

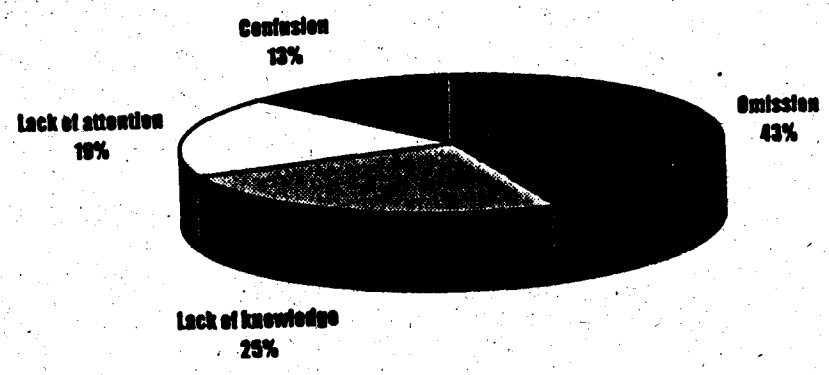
Mode of Operation



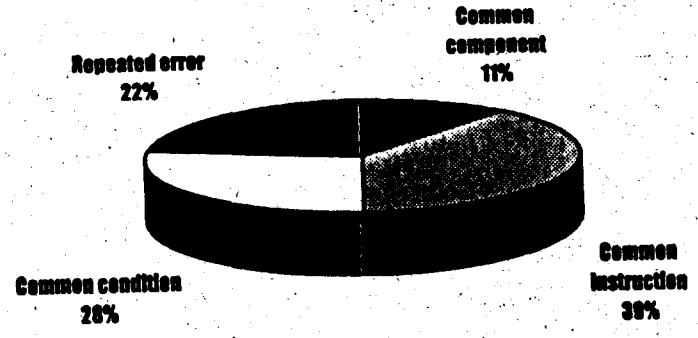
Type of Activity



Behavioural Factor



Type of Dependency



Canada

Atomic Energy Control Board, Canada.

Summary of a common cause failure event which occurred in a Canadian utility.

"Failure to Verify Poison Isotopic"

Background

Operating Policies and Principles (OP&Ps) are referenced in the reactor operating license, and contain not only general safety principles, but also define safety parameters and their numerical values for the operation of the nuclear power plant. Gadolinium Nitrate and Boric Oxide are both neutron absorbers or "poisons" which stop the nuclear reaction, with certain isotopic forms of these being better neutron absorbers than others. These poisons are placed into the moderator (D2O) at particular concentrations as a means of controlling the nuclear reaction. The concentration of the poison is a critical parameter, as a small change in moderator poison concentration coincident with other failures (eg. loss of coolant) can result in a sudden increase in power, which if unchecked in a timely fashion can lead to fuel damage. In other words, failure to ensure that the poison isotopic is pure and at the correct concentration can result in a compromizing of the effectiveness of the safety shutdown systems. Thus, it is extremely important in CANDU reactors that the concentration of moderator poison meet the required specifications if extreme consequences are to be avoided.

Chronology of the Event

One month prior to the event a memo was entered by the Chemistry Unit as a Note to File which stipulated that whenever new shipments of either Gadolinium Nitrate or Boric Oxide arrived in Stores, the shipment must undergo quarantine so that samples could be taken and forwarded for analysis. This is required by the OP&Ps, and is done to ensure that neutron flux depression capabilitiy and D20 content are within specifications.

The following month, orders of Boric Oxide and Gadolinium Nitrate were placed, which stipulated on the purchase order the quarantine of the shipment upon arrival. Furthermore it was stipulated that the Chemistry Unit must be notified upon arrival of the shipment. This order subsequently arrived, was quarantined, and the Chemistry Unit notified for appropriate poison verification. These actions were completed.

Two separate second orders, one for Gadolinium Nitrate and one for Boric Oxide were placed with a different supplier approximately four months later. The purchase orders did not stipulate the requirements to quarantine, inform the Chemistry Unit or to test samples. It only stated that correct isotopic and chemical purity were required.

Four months later the second order of Gadolinium Nitrate arrived, but was not quarantined, the Chemistry Unit was not notified, and the required verification was not done.

Seven months later the second order of Boric Oxide arrived, and this too was not quarantined, the Chemistry Unit was not informed, and the required verification was not done.

Behavioural Analysis

In documenting the requirements for dealing with the poisons the Chemistry Unit felt that a "Note To File" was sufficient to ensure that the OP&Ps were met. They felt that the frequency of shipments was so low that a more formal means of control was not necessary. The situation was not detected because normally the chemical shipments require only an particular data sheet and no special Purchase Clauses highlighted in order to pass through quarantine. Since poison verification had been completed successfully with past shipments, the Chemistry Unit assumed that the existing administrative procedure was adequate. Finally, when the Unit 1 Liquid Injection Shutdown System Commissioning Group contacted the Chemistry Unit they were given verbal confirmation that the poison had been correctly analysed, verified, and released for station use.

Causal Factors

1) Work Practices: The methods used did not ensure that adequate interdepartmental communications existed.

2) Resource Management: Too many duties were assigned to the Chemical Engineer, who because of this relied on his memory inappropriately.

3) Written Communication: The Purchase Order did not include the stipulations for quarantine, notification, and testing.

4) Managerial Methods:
   a) Failure to monitor and assess the effectiveness of the methods chosen for dealing with shipments.
   b) Methods did not ensure adequate communications between the Commissioning Section and the Chemistry Unit.
   c) Methods allowed for approval of a Work Plan without adequate technical review and formal documented proof of poison verification.

Proposed Corrective Actions

1) Written Communication:

a) update descriptions of Gadolinium Nitrate and Boric Oxide with warnings to quarantine upon arrival, and requirement for notification of Chemistry Unit so that they may complete the testing and verification.
b) Initiate a Purchase Condition Clause on all moderator poisons which requires immediate quarantine.

2) Resource Management: Relieve Chemistry Unit personnel of sole responsibility for sampling and testing poisons. Through the use of the Purchase Condition Clause and the updated descriptions give more responsibility to Station Stores.

3) Managerial Methods:
a) initiate more effective methods for dealing with poisons
b) amend Chemistry Unit procedures so that they more closely match those of the Technical Section.

Finland

A METHOD FOR IDENTIFICATION OF HUMAN ORIGINATED TEST AND MAINTENANCE FAILURES

Pekka Pyy
Technical Research
Centre of Finland (VTT)
SF-02151, Finland

Tapio Saarenpää
Teollisuuden Voima
Power Company (TVO)
SF-27160, Finland

Abstract

In the Nordic co-operation in the field of nuclear power, human error research has been continuously under major interest. In connection with the project Optimisation of Technical Specifications using Probabilistic Methods (RAS-450), method development to use probabilistic safety criteria to evaluate safety and to investigate the effect of testing and maintenance on nuclear safety has been performed. Especially the effect of inadvertent human activities has been under investigation.

In order to improve the coverage of PRAs and the maintenance planning at nuclear power plants, Technical Research Centre of Finland (VTT) has developed a method for identification of possible test and maintenance caused common cause failures in close cooperation with Teollisuuden Voima Power Company (TVO). The method has been tested in analyses of safety related systems at TVO nuclear power plant in Olkiluoto, which consists of two 660 MW BWR units.

The method is praxis-oriented and provides a simple way to cluster operating and maintenance experience to improve safety. The starting point of the method is to go through a process systematically in group sessions and by using a special form. Identified possible common cause failures are classified into three categories in respect of the risk they are considered to cause to the installation. The procedure is developed further in the RAS-450 project.

Introduction

Human errors have been under major interest in Nordic co-operation in the field of nuclear safety for several years. Two programmes round the subject have been running during the years 1977-1985. The third Nordic joint programme on nuclear energy funded by the Nordic Council of Ministers and coordinated via the Nordic Liaison Committee for Atomic Energy (NKA) includes several projects addressing human reliability and human factors. The programme is planned to be completed by 1989.

One of the projects, Optimisation of Technical Specifications by Using Probabilistic Methods (RAS-450), is directly related with human errors in nuclear power plants (NPPs). The project aims at developing the technical specifications and safety philosophy from the risk point of view. In this context, probabilistic methods are utilized to establish safety criteria as a basis for the specifications. The objective here is to apply the findings and the methods of Finnish and Swedish PRAs in development of plant practices [1].

The human factors coupling has become salient via applications in the following areas:

- reconsideration of plant shutdown requirements during specific safety system failure situations
- analysis of efficiency and coverage of test arrangements in standby safety systems
- evaluation of impact of planned maintenance activities in standby safety systems.

In addition to the positive effects of normal test and maintenance, human activities may also degrade system operability. The degradation happens via small deviations of human behaviour called slips. As an example, forgetting of tightening the bolts may cause a seal to leak. An another kind of process is represented by mistake type errors, which refer to more stable deficiencies in man machine interface [2]. Mistakes as cognitive errors can cause common cause failures (CCFs) and paralyze redundant systems. Since nuclear systems are generally equipped with redundant circuits, it is the CCFs and latent system interactions which are the most hazardous phenomena to appear suddenly in a nuclear event sequence. In the NKA/RAS-450 project, it has become clear that possible paths to CCFs have to be investigated efficiently. One branch here are the testing and maintenance activities.

In order to identify CCFs originated in test and maintenance, VTT and TVO have been working in close co-operation. The objective was to develop a simple and effective tool to help the identification. As a result, a method for practical analysis purposes was created and tested. In the following, the principles and the use of the method are described.

Main principles of the method

In the identification of human related CCFs (HCCFS), there are two possible starting points: man and machine (or technical system). Starting purely from internal human processes would have required more expertise and resources than were available. However, such procedure is suggested for operation tasks and in case of a very limited object. In consideration of test and maintenance, starting from technical system failures and taking into account inherent human behaviour characteristics is, however, natural. Thus, we decided to start from the technical system side.

Our basic principle of the identification is simply: human errors cannot cause a system to fail in a new way. This means system failures can only exist due to technical reasons and it is always possible to create check-lists for system failures. Organisational liability or human errors such as wrong or missing lubricant may appear as direct causes of the failures, but even human errors cannot create impossible paths to a failure.

CCFs are more or less related with the pre-existing hazards in man-machine systems. This means that if a human error causes a redundant system to fail, there has to be a systematic misunderstanding in human behaviour or exist latent interactions between technical systems. Therefore, simple human slips do not usually cause CCFs and can be screened out during the identification task.

Another starting point of our method is that team work techniques general in process industry hazard identification can as well be used on the nuclear side to conduct a task known as "talk-through" or "task analysis". We decided to modify the principles of HAZOP (Hazard and Operability Study) and FMEA (Failure Mode and Effects Analysis) to be applicable in the identification of human errors. After considering carefully the properties needed to identify human errors and especially HCCFs, a satisfactory solution could be found. From this on, we call our result the HCCF Analysis of Test and Maintenance.

The method relies on the use of representatives of plant maintenance and operation to form the identification team. Via systematic use of plant experience, PSAs can be completed and new sights on safety gained. The work is led by a chairman, who gives ideas for possible errors and takes care of the quality of the work including the time spent for discussions. Typically the team also needs a secretary to make the paperwork. Other members needed are shift supervisors, maintenance technicians and engineers. The suitable total size of an identification team has proved to be 4-5 members.

The structuring of the identification is performed by using a form illustrated in Figure 1. The form includes columns for redundant component groups; maintenance tasks with their error characteristics; detection factors; risk classification; measures to be taken and important remarks. The form can be divided into three parts in respect of the error causation, the error revelation and additional information. Possible errors and their detection characteristics are weighted in respect of the risk they are considered to cause and classified into risk classes respectively. An another aim of the form is to yield conversation and information exchange between different groups on plant operation and maintenance, which may reveal important problems, e.g., in work delegation otherwise remaining unknown.

In addition to the form, auxiliary documents are needed. A FMEA or systematic maintainability review documentation if available is an excellent aid to give ideas of possible failure mechanisms [3]. A list of usual CCF modes is easy to make and it can be completed during the sessions. A PI-diagram of the system under investigation is necessary to guarantee all the components are considered. Furthermore, scheduled maintenance and test statistics with the tasks performed are needed to check the task intervals etc. However, the main information source is the team knowledge.

Analysis Flow

The identification begins by choosing the first component group of a certain safety related system. Here, FMEA documents, if available, and system PI-diagrams are utilized. All the maintenance tasks of interest are then taken into consideration and listed on the form with their frequencies. This is performed separately for the mechanical, electrical and instrument maintenance. The chairman takes care that all the relevant errors are discussed and impossible CCF sources are screened out. A similar procedure is also performed for testing of certain components or systems. To invent possible CCF mechanisms, lists of general fault and specially CCF causes can be used and the chairman leads the discussion by presenting new error types. The first part of the form is thus called the error section.

System:650	Analysed by: PP, TS	Date:15.4.1987	Page : 1(3)	Revision date:20.5.1988 PP				
	HCCF ANALYSIS FOR TEST AND MAINTENANCE							
	THE ERROR SECTON		THE DETECTION SECTION					
COMPONENT GROUP	TASK; CCF SOURCE	TASK FREQUENCY	CONSEQUENCES	DETECTION PROCEDURE	T&I FREQ.	CCF CLASS	MEASURES	REMARKS
DIESEL AGGREGATE				Oil level Air leakages Oil sample Vibration test Start test Load test Trial run	1/w 1/w 1/6m 1/8w 1/2w 1/m after outage			
	A: FILLING THE FUEL RESERVOIR 1. Wrong fuel	A:WHEN NEEDED	1. Diesels don't start or they stop in demand	1. Eventually detected in load test or in trial run		B(C)	1. A study on the fuel quality assurance	Are samples taken ?? A common tank for all the diesels
	B: CHANGING OF THE OIL AND THE FILTER 1. Wrong oil	B: 1/2y	1. Diesels stop after a while	1.It is evident that wrong lubricant is not detected in start tests and only maybe in load and vibration tests. Samples and trial run should reveal the error after the outage		B(C)	1. Diesel PI-diagrams should be updated!	How sensitive the diesels are to the oil quality?
	2. Omission of changing filters or wrong filters		2. Usually no harm	2. Detected, if blocked then no start	See above	C	1. Uniform oil filters used	

Figure 1. A filled HCCF Analysis form. All the relevant tests are listed at the beginning of the column with their frequencies. The tests which could reveal an error are mentioned again after the appropriate error mode.

After the possible HCCF candidates are booked, the detection factors are considered to screen the amount further. The other important function is to make clear the consequences of a certain CCF, for which a certain column is addressed. Columns are also reserved for indications or inspections which could reveal the CCF with their frequency. The part is called the detection section since its function is to illustrate, whether a certain HCCF really can remain undetected over a significant period of time.

According to the results of the error and the detection sections, the HCCFs are classified into three classes. The classes represent the risk contribution of the remaining HCCFs respectively. If needed, more accurate classification or quantitative values can be used. The flow diagram of the analysis is shown in Figure 2.

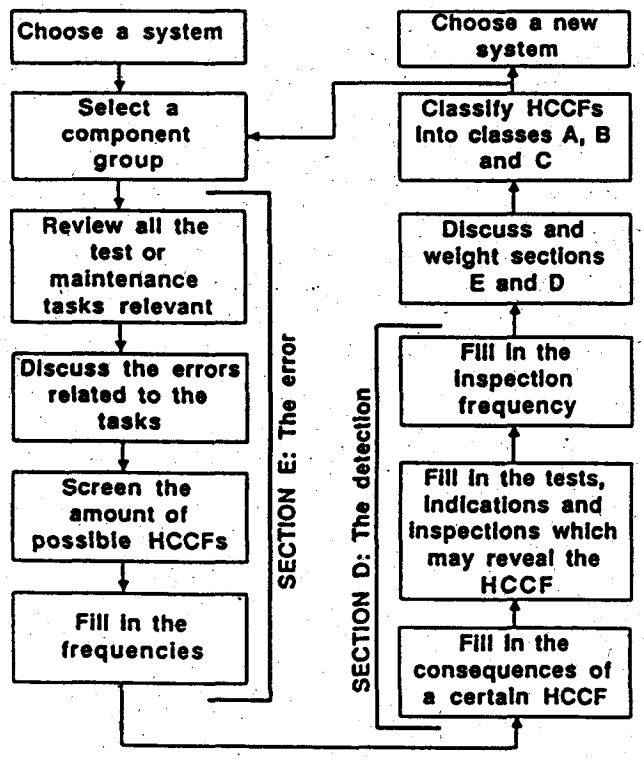


Figure 2. HCCF Analysis flow diagram.

Filling the form

In the following, there is a more precise description of what should be filled in each column of the form in Fig. 1. The instructions given should only be seen as guidelines and they can be modified, if needed.

Component Group: Here, codes of redundant components or systems addressed are expressed. The components do not necessarily have to be redundant, if they are similar in respect of the detection factors and the maintenance activities performed . Also single components can be analysed, if their reliability performance is vital because of the couplings between systems.

Task, CCF Source: Systematic preventive maintenance and tests are booked here. Capital letters can be used to distinguish different maintenance tasks. Possible errors causing CCFs are numbered running from No. 1 per component group. Thus, the consequences, the risk class and the measures taken associated with a certain CCF are easy to find. If a test/inspection does not include special operations which could introduce more CCFs, the test is only regarded as revealing action and written down in the inspection procedure column. "No activities" means the component group does not belong to the preventive maintenance program. These component groups are not studied further, since only random failures and errors are possible, if the experience does not show high human error frequency. Likewise, very improbable error modes are screened out already in the initial phase.

Task Frequency: The frequency of a test or maintenance, which also means the frequency to possibly cause a CCF. Abbreviations are used here.

Consequences: The consequences of a certain HCCF from the component group, system function or plant survival point of view. It has to be emphasized here that the consequences listed here are only the opinion of the identification team for further investigation. Also couplings between systems should be mentioned. A thorough thinking is suggested here since all the consequences may not be salient in the beginning.

Detection Procedure: Control room indications, alarms, functional tests and inspections, which may reveal the CCFs are listed here. If it is questionable whether a certain test is valid to reveal real hazards in demand situation, it can be referred here and described in detail in the following columns.

T&I Frequency: The frequency of a certain test or inspection using the same abbreviations as earlier.

CCF Class: The CCFs are classified into three risk classes. Here, the interpretation of risk is the following:

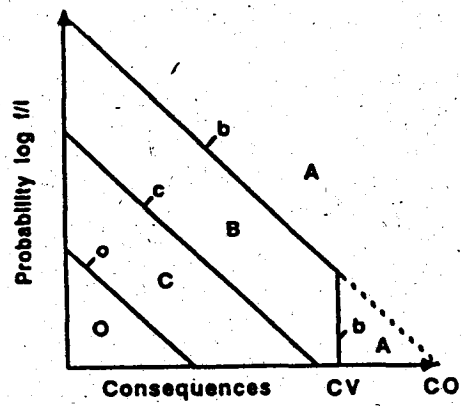
$$R = (f / i) * c \qquad (1)$$

, where:

R = Risk
f = task frequency
i = inspection frequency
c = consequences

The proportion f/i expresses the frequency weighting factor (which is also the probability of a component group being failed if i >> f). If the factor value approaches 1 or more, and the frequencies of both f and i are low, it is necessary to consider closer the period of time errors may remain undetected. If that is considerable, the risk class has to be raised.

It has to be pointed out that Equation (1) holds for credible error modes. This means no exact classification in respect of the error probabilities is needed, and the risk induced by the incredible HCCFs screened out during the work is assumed to be approximately 0. However, no exact values to the equation variables has been given in the identification sessions, but it is possible in future applications. The illustration of Equation (1) is however used during the sessions to help the risk classification. The illustration is presented in Figure 3. As seen, more weight is given to severe consequences.



CV = cut - off value for weighting of major risks

O, C, B = Risk classes remaining under respective equivalent risk curves o, c and b.

A = Risk larger than curve b indicates.

CO = Consequences

f/l = Expression of the probability of an error remaining latent (especially when l > > f)

Figure 3. Illustration of risk classess induced by the HCCFs. Severe consequences are weighted.

We have in our applications emphasized the subjective classification into classes A, B and C, where A stands for the highest risk. In some arguable cases, also interim classes, e.g., A(B) are used (read: A to B direction). Impossible and negligible HCCF modes are left outside the classification. The ranking expresses the identification team view on the proportional risk the CCF is perceived to introduce into the plant.

Measures: The measures taken or to be taken to hinder a certain CCF or to mitigate its consequences. One function of the identification sessions is to serve as forums where plant operation and maintenance practices are evaluated and modifications suggested.

Remarks: Other remarks of importance. Includes mainly information based on the plant staff experience about the failures, maintenance and operating conditions, opinions on the validity of tests, reasons for the classification and problems detected. The role of this column could not be emphasized too much, since it gives an idea what the plant staff really wants and needs.

An example of a filled form is given in Fig. 1, which demonstrates the way the method yields HCCFs quantified on a coarse level in respect of their risk contribution. This provides a good basis for further quantification and in-depth evaluation of human errors.

Experience from testing the method

The method has been tested at the TVO nuclear power station in Olkiluoto. The testing was performed in March and April 1987 in several group sessions, where safety related systems were investigated. The participants were maintenance technicians from different maintenance fields, a former shift supervisor and a chairman from VTT.

The sessions yielded about 20 possible test and maintenance originated HCCFs classified into the two highest risk classes A and B. In addition several HCCFs were classified into category C and suggestions to improve the situation were given. The ways the plant is maintained and operated were discussed eagerly resulting in several remarks useful in future e.g. suggestions of maintenance program extension to new devices and ideas to modify some tests.

The personnel participating took their task seriously and a positive attitude towards the method could be observed. They felt that when people try to think how a system can be made to fail, new things occur to them since normally the staff only tries to think how to make things go well. The selection of the participating people was thus successful.

It could be proved that a system can be analysed in a limited time on a general level of accuracy. This means a medium size system requires about one hour for each maintenance group (mechanical, instrumentation, electrical and tests), which results in about 3-4 hours per system if all the types mentioned are considered. The method is flexible in modifying the level of analysis detail, but it must be taken into account that it becomes time consuming if the level is increased too much. Here, a FMEA performed beforehand proved to be a valuable aid.

Discussion and conclusions

The identification of hazardous human errors has often been mentioned to be very difficult. It is true that the search for root causes and psychological mechanisms can be endless and frustrating. However, there are ways to perform the identification within a limited time and with limited resources. This paper illustrates a possible procedure proved to be useful in practice.

One often observed deficiency in PSAs is the lack of operational experience used. The method presented can yield a remarkable amount of new information on the CCFs and plant properties. Here, two basic needs have to be satisfied: the system and the maintenance documents have to be available (a FMEA helps the work), and the correct people have to be found to create a good team. There exist needs to identify and reduce risks and maybe there are also methods, e.g., HAZOP and the HCCF analysis described here to do that, but how to motivate and organize the real work? The organisational factors have proved to be difficult not only in hazard identification but everywhere in industry and work life. It is suggested that more time should be spent to consider these tasks when performing analyses, since the result is directly proportional to the motivation [4].

The method presented can also be modified and used in other contexts. As an example, plant operating tasks could be analysed by substituting component groups by different goals and objectives of operators when performing a certain task. Hence, the internal goal-oriented structure of human behaviour can be taken into account in human error identification. Because of its properties, the method is recommended to be used extensively to widen the coverage of safety studies, and in NKA/RAS-450 project new applications including further method development are prepared.

References

[1] K.J. Laakso (ed.), NKA/RAS-450 Optimization of Technical Specifications Using Probabilistic Methods - A Nordic Perspective. NKA/RAS-450-(88)1. Summary Report 1985-1987. Nordic Liaison Committee for Atomic Energy (NKA), Espoo, April 1988.

[2] D.A. Norman, "New views of information processing: Implications for intelligent decision support systems," in Hollnagel et al: Intelligent Decision Support in Process Environment. Springer Verlag, Heidelberg, NATO ASI Series, 1986.

[3] K.J. Laakso and D. Burns, "Systematic Maintainability Review for Plant Design," presented at the Second European Logistics Symposium, Växjö, Sweden, June 1985.

[4] P. Pyy and J. Suokas, "Identification of accident sequences with human contribution in the process industries," presented at the 8th Society of Reliability Engineers Scandinavian Chapter Symposium, Helsingör, Denmark, October 5-7 1987.

COMMON CAUSE FAILURE

COMMON CAUSE FAILURES (CCF) ARE FAILURE CAUSES OR MECHANISMS WHICH RESULT OR CAN RESULT IN MULTIPLE FAILURES IN REDUNDANT COMPONENTS ON REAL DEMAND SITUATIONS.

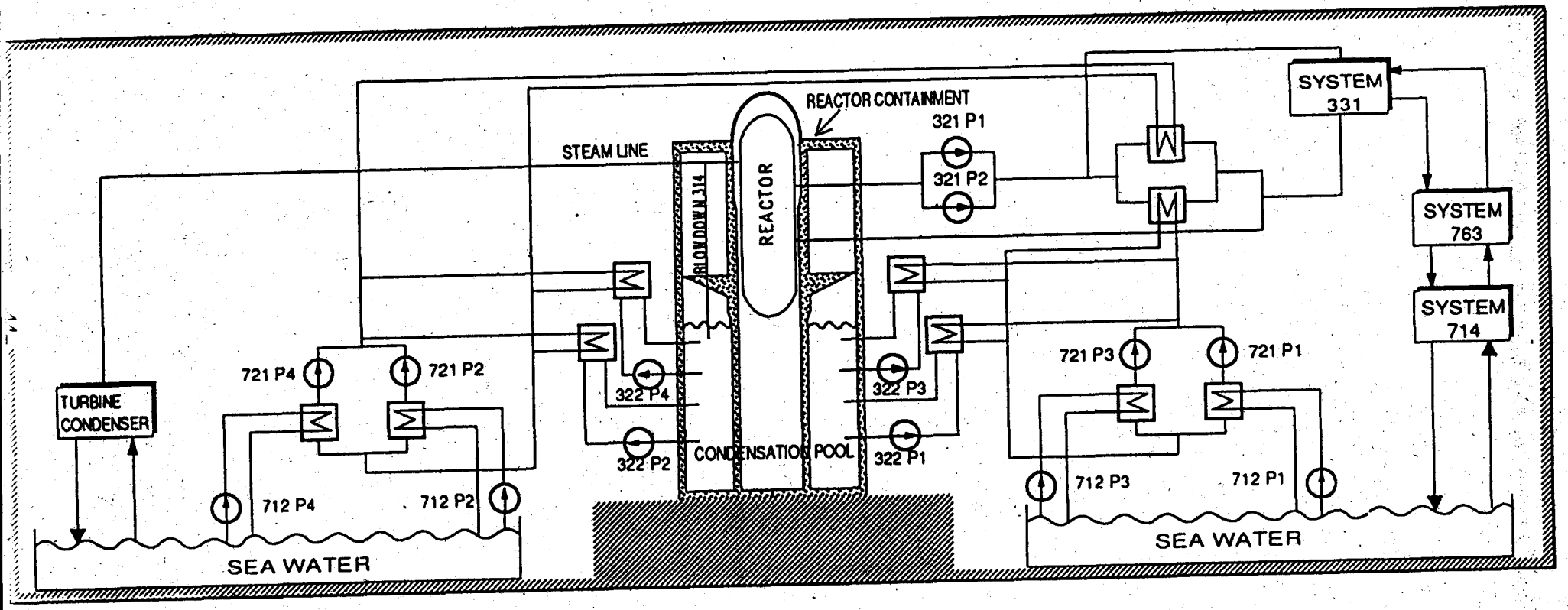
THE FAULTS ARE USUALLY REGARDED AS CCF WHEN THEY HAVE BEEN DETECTED:

- ON STANDBY COMPONENTS WITHIN THE TIME FRAME OF THE SURVEILLANCE TEST INTERVAL, AND

- ON CONTINUOUSLY RUNNING COMPONENTS WITHIN TWENTY-FOUR HOURS.

OBS. LONGER TIME FRAMES MUST BE CONSIDERED WHEN FAILURES ARE NOT DETECTED IN PERIODIC TESTS OR OTHER PLANNED CHECKS

saved 13.2.95 by klj as d:\teksti\hccf\defccf.doc


REACTOR CONTAINMENT
STEAM LINE
BLOW DOWN 314
REACTOR
321 P1
321 P2
SYSTEM 331
SYSTEM 763
SYSTEM 714
TURBINE CONDENSER
721 P4
721 P2
322 P4
322 P2
CONDENSATION POOL
322 P3
322 P1
721 P3
721 P1
712 P4
712 P2
712 P3
712 P1
SEA WATER
SEA WATER

The subsystems are separated physically from each other and each subsystem has a separate electrical supply bus. The system capacities were originally dimensioned to be 4 x 50 % subsystems according to design criteria. This creates an excess margin to the single failure criterion, which makes it possible to justify power operation during a limited time with one subsystem unavailable due to planned maintenance actions or a repair of a fault. Furthermore, according to renewed and more realistic thermo-hydraulic calculations of Design Basis Accident events, the system capacities are in most cases 4 x 100 %.

HCCF

HUMAN-INTERACTION DEPENDENCE

DEPENDENCIES INTRODUCED BY HUMAN ACTIONS, INCLUDING ERRORS OF OMISSION AND COMMISSION.

THE PERSONS INVOLVED CAN BE ANYONE ASSOCIATED WITH PLANT-LIFE-CYCLE ACTIVITY, INCLUDING DESIGNERS, MANUFACTURERS, CONSTRUCTORS, INSPECTORS, OPERATORS AND MAINTENANCE PERSONNEL.

A DEPENDENT FAILURE OF THIS TYPE OCCURS, FOR EXAMPLE, WHEN AN OPERATOR TURNS OFF A SYSTEM AFTER FAILING TO CORRECTLY DIAGNOSE THE CONDITION OF THE PLANT - AN EVENT THAT HAPPENED DURING THE THREE MILE ISLAND ACCIDENT WHEN AN OPERATOR TURNED OFF THE EMERGENCY CORE COOLING SYSTEM.

saved 11.2.95 by kjl as d:\teksti\hccf\termhid0.doc

FOCUS IN IDENTIFICATION AND ANALYSIS OF DATA

DEPENDENCES WITH SPECIFIC EMPHASIS :

- ON COMMON CAUSE FAILURES, AND
- ON HUMAN INTERACTIONS

FOCUS ON ANALYSIS OF FAILURES WHICH HAVE NOT BEEN INVESTIGATED IN THE LICENSEE EVENT REPORTS.

THE EXTENSIVE REPORTING IN THE COMPUTERIZED MAINTENANCE HISTORY DATA SYSTEM OF THE TVO PLANT WAS USED AS DATA SOURCE.

saved 14.2.95 by kjl as d:\tekst\hccf\ident0.doc

VTT

CONTENT OF FAILURE REPORT

- Report type and no
- Station code
- Unit code
- System and component code
- Failure data codes (see Appendix 2)
- Points of time
  - Time of failure detection
  - Start of unavailability
  - Start of repair *)
  - Available after repair
- Repair effort
  - man-hours
  - average number of men
- Waiting time and cause *)
- Component category (see Appendix I)
- Description in plain language for
  - failure observation
  - failure type and cause
  - action taken

*) optional

FAILURE DATA CODES

In this paper has an approximate translation been made of the TUD-systems classification of the failure information.

A FAILURE DETECTION

A	Alarm
B	Operation Supervision and Service Observation in controlroom
H	Operation Supervision and Service Observation otherwise
C	Preventive maintenance
D	Testing and Preventive maintenance
E	Inspection
G	Real demand

B EFFECT OF FAILURE ON ITEM

A	Won't close/stop/disconnect (on order)
B	Won't open/start/connect (on order)
C	Spurious closing/stop/disconnection
D	Spurious opening/start/connection
E	Signal (measuring value) fails to appe
F	Spurious signal
G	Faulty measuring value (signal)
H	Faulty regulation (governing)
K	Other functional obstructions
L	None or a minor functional obstruction

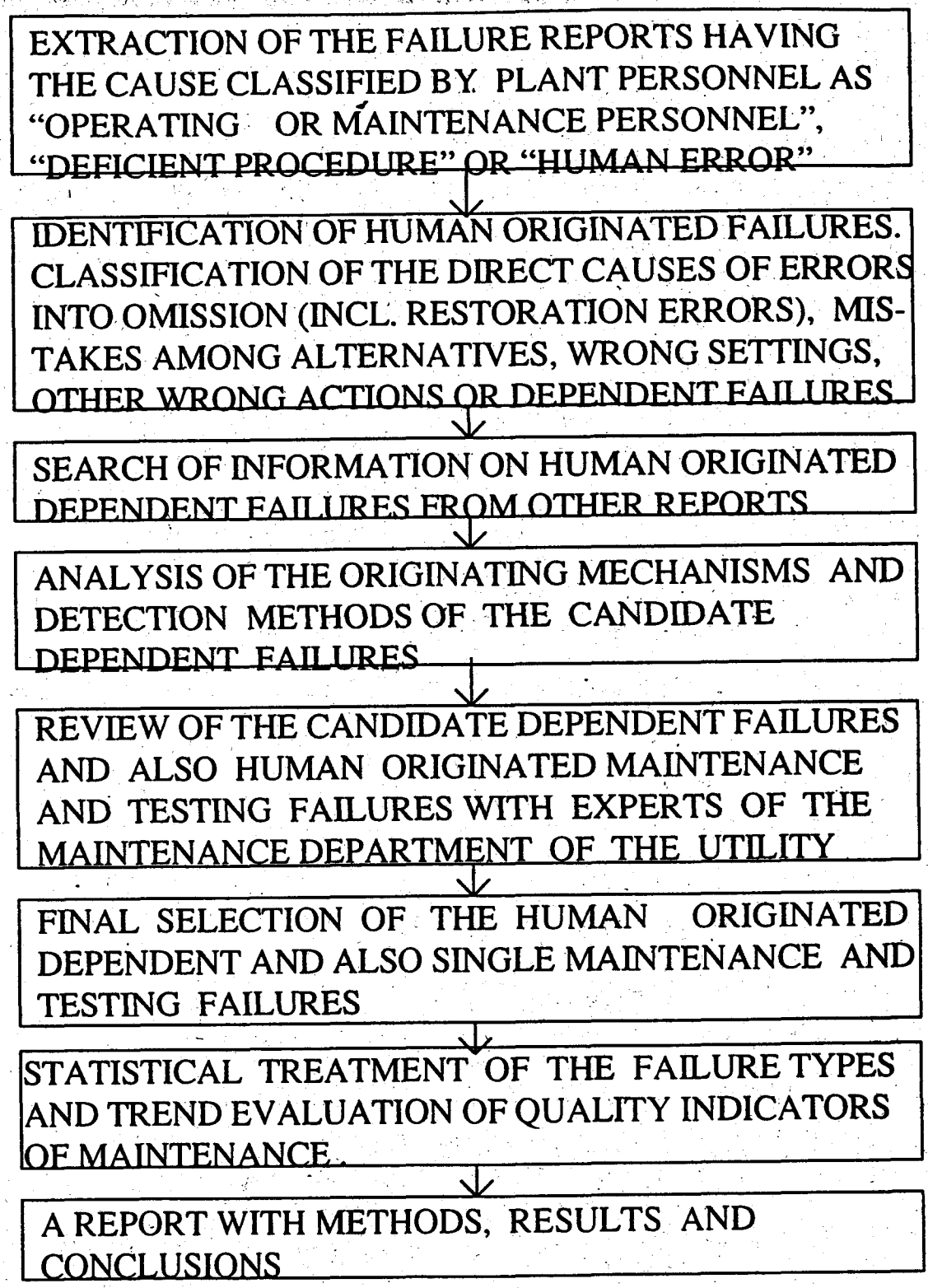
Note that all codes BA to BK are functionally obstructing failure w.r.t. the desired function and therefore disturbing the operation of the item which should not be the case for failures coded BL .

E ACTION TAKEN

H	Replacement of component with new engineering data
B	Replacement of component with same engineering data
C	Repair/adjustment (no replacement of component)
D	Replacement of part of component
Z	Other (e g cleaning, lubrication)

D TYPE OF FAILURE

A	Fracture/Crack
D	Internal tube leakage
E	External sealing leakage
F	Internal sealing leakage
G	Deformation, displacement
H	Vibration, noise
I	Deposit, blockage
J	Biting, seizure
L	Bad contact
M	Open circuit
N	Ground fault, insulation fault
O	Short circuit
P	Out of adjustment
R	Base program fault
S	Applikation program fault
T	Database fault
U	Corrosion, erosion, wear
X	Temporary or unidentified fault
Y	Control equipment fault
W	Operating error/wrong base position
Z	Other



FLOW DIAGRAM OF HUMAN CCF ANALYSIS

VTT AUTOMAATIO
Teollisuusautomaati

TVO I II EQUIPMENT PLACE IDENTIFICATION NUMBER_____
WORK NUMBER_____ YEAR:_____
DATE (fault detected) _____ time: _____ DATE (repair started): _____
time:_____ Date (work finished):_____ time:_____

The written text in the failure report of the plant (description of fault and corrective actions):

The cause classification in the failure report (1-2 squares): A B C D W

Complementary information (possible time relation or functional connections to other failures, conflicting information, etc)

..(The information under this line was prepared by follow-up analysis of the reporting).....

I INFORMATION ON THE WORK TASK WHERE THE DEVIATION OCCURRED

Cause of the deviation unclear Deviation possibly caused in Deviation certainly caused in the action:

The action was (1-2 squares): repair preventive maintenance periodic test interval _____weeks
modification functional test date (possible or certain) _____
Complementary information: _____

The caused action occurred during (1-2 crosses) : cold shutdown of reactor refuelling hot shutdown of reactor nuclear heating hot readiness of reactor power operation start-up shutting down

Complementary information (e.g. how the failure occurrence could have been avoided):

_____

_____

.....

(The information under this line will be surveyed, if the error involved as candidate on dependent failure)

II INFORMATION ON THE TASK BY WHICH THE DEVIATION WAS DETECTED

Detection method unclear Deviation possibly detected in certainly detected in the task:

The detection method was: alarm operation supervision in control rooms, how _____
preventive maintenance periodic testing (e.g acc. to technical specifications) other authority inspection (e.g. NDT) equipment worked not on demand other supervision of operation (e.g. shift walk-around, alignment) functional test repair other check , which_____ date_____interval _____

Detected in plant state (1-2 crosses): cold shutdown of reactor refuelling hot shutdown of reactor nuclear heating hot readiness of reactor power operation start-up shutting down
Complementary information (e.g. identification number of techspec test or preventive maintenance action):

_____ _____

Deviation not detected in the operative check (check following after the work action, 1-2 crosses): preventive maintenance functional test alignment adjusting start-up test periodic test interval _____ other check which_____ date_____ plant state, which _____
Complementary information (e.g. identification number of tech spec test or preventive maintenance task or explanation, if checking task existed ?): _____

Deviation was not detected in organizational check (independent QA and QC, performed prior to or during the the work task): Deficient review of: design work planning start-up testing program deficient acceptance inspection other review or inspection, which_____
Complementary information (e.g. which possible other review or check actions could have detected the deviation): _____

III THE TYPE; ORIGIN AND DEPENDENCE OF THE DEVIATION

Deviation type(1-2 types): omission (also restoration errors) mistakes among alternatives wrong settings other wrong action, e.g. due to human variability dependent failure (put together all dependent failures and give the following information on the dependent failures and only once) Other connected dependent failures are: _____

The originating mechanism of the deviation and dependence is deficient (1-2 types): design work planning procedure organisation (e.g. definition of work scope or information transfer) supervision of subcontractors same group , training , tools (selection, maintenance or QC) other . , which (or complementary information, e.g. which organizational unit or personnel category): _____

The deviation was additionally caused by: equipment close to each other(e.g. same room) administrative easiness (e.g. sequential tasks feasible soon after each other)
Complementary information: _____

Consequences of the deviations (e.g. unavailiability time of equipment or system):
Consequence classification in failure report: A B C D E F G H I
Delay time (from originating work task until fault detection): _____ hours.
Total unavailability time: _____ hours
Complementary information (e.g description of consequences): _____

IV NOTES ON ALTERNATIVE CORRECTIVE ACTIONS

The problem can be corrected (or already corrected) by:

VTT AUTOMAATIO
Teollisuusautomaati

TVO I II EQUIPMENT PLACE IDENTIFICATION NUMBER: 531K 951_____
WORK NUMBER: 5003032__ YEAR:1994_____
DATE (fault detected): 05.06.94____ time: 11.16_ DATE (repair started): 05.06.94____ time: 11.30____
Date (work finished): 05.06.94_____ time: 13.00_____

The written text in the failure report of the plant (description of fault and corrective actions):
531K951 alarmed inadvertently. Check of the measurement point. Measurement points 531K952,K953, K954 must also be checked. Subcondition on trip of of 531K951 H6 SS10 blocked. The trip limits of 531K951-K954 were set 60%. The limits had remained after the power raising test at this lower level. The restoration order was given, but the control room had interrupted the the actions. H7 limits have then been raised to 118 % and H8 limits to 125 %.

The cause classification in the failure report (1-2 squares): A B C D W

Complementary information (possible time relation or functional connections to other failures, conflicting information, etc)

(The information under this line was prepared by follow-up analysis of the reporting).....

I INFORMATION ON THE WORK TASK WHERE THE DEVIATION OCCURRED

Cause of the deviation unclear Deviation possibly caused in **Deviation certainly caused in the action:**
The trip limits on neutron flux of the reactor protection system had been lowered to 60 % in order to facilitate the special flow capacity test of the main steam isolation valve 311V004 24.05.94 before shutdown to refuelling outage.

The action was (1-2 squares): repair preventive maintenance periodic test interval _____weeks
modification **functional test** date (possible or certain): **24.05.94**_____
Complementary information: **Special isolation capacity test to check the limitatation of the valve's capacity when possible power plant power capacity increase is introduced in the future.**

The caused action occurred during (1-2 crosses) : cold shutdown of reactor refuelling hot shutdown of reactor nuclear heating hot readiness of reactor **power operation** start-up **shutting down**

Complementary information (e.g. how the failure occurrence could have been avoided):
If the neutron flux trip limits would have been restored from 60% to basic levels prior to start-up after refuelling outage_____
.....
(The information under this line will be surveyed, if the error involved as candidate on dependent failure)

II INFORMATION ON THE TASK BY WHICH THE DEVIATION WAS DETECTED
Detection method unclear Deviation possibly detected in **certainly detected in the task:**
Trip of one neutron flux monitoring channel in the reactor protection system four times at the 52 % power level during four successive reactor power raising attempts after the refuelling outage.

The detection method was: **alarm** operation supervision in control rooms, how _____
preventive maintenance periodic testing (e.g acc. to technical specifications) other authority inspection (e.g. NDT) equipment worked not on demand other supervision of operation (e.g. shift walk-around, alignment) functional test repair other check , which____ _____ date: **05.06.94**_____interval _____

Detected in plant state (1-2 crosses): cold shutdown of reactor refuelling hot shutdown of reactor nuclear heating hot readiness of reactor **power operation** **start-up** shutting down
Complementary information (e.g. identification number of techspec test or preventive maintenance action):

Deviation not detected in the operative check (check following after the work action, 1-2 crosses): preventive maintenance functional test alignment adjusting start-up test **periodic test** interval : **3 months**
other check which_____ date_____ plant state, which _____
Complementary information (e.g. identification number of tech spec test or preventive maintenance task or explanation, if checking task existed ?): _____

Deviation was not detected in organizational check (independent QA and QC, performed prior to or during the the work task): **Deficient review of**: design **work planning** start-up testing program deficient acceptance inspection other review or inspection, which_____
Complementary information (e.g. which possible other review or check actions could have detected the deviation): **Foreman signed the work order because he believed that the trip limits had been restored by the instrument technician to the basic levels, but no specific cross for checking of this detailed step existed in the work order.**_____

III THE TYPE; ORIGIN AND DEPENDENCE OF THE DEVIATION

Deviation type(1-2 types): **omission (also restoration errors)** mistakes among alternatives wrong settings other wrong action, e.g. due to human variability **dependent failure** (put together all dependent failures and give the following information on the dependent failures and only once) Other connected dependent failures are: **The trip limits not restored on the three other channels 531K952, K953 and K954 either, but the setpoints were slightly higher than ca. 52 %.** _____

The originating mechanism of the deviation and dependence is deficient (1-2 types): design **work planning** procedure **organisation** (e.g. definition of work scope or **information transfer**) supervision of subcontractors same group , training , tools (selection, maintenance or QC) other , which (or complementary information, e.g. which organizational unit or personnel category): _____

The deviation was additionally caused by: equipment close to each other(e.g. same room) administrative easiness (e.g. sequential tasks feasible soon after each other)
Complementary information: _____

Consequences of the deviations (e.g. unavailiability time of equipment or system):
Consequence classification in failure report: A B C D E F G H I
Delay time (from originating work task until fault detection): **288**_____ hours.
Total unavailability time: _____ hours
Complementary information (e.g description of consequences): _____

IV NOTES ON ALTERNATIVE CORRECTIVE ACTIONS

The problem can be corrected (or already corrected) by:
A root cause analysis is going on at the utility. The neutron flux trip limit setpoints will be verified (by simulation tests) in the future as a part of the RPS (reactor protection system) tests prior to start up at the end of the refuelling outages.

DEVIATION TYPES (1-2 TYPES)

FAILURE REPORTS HAVING THE CAUSE CLASSIFIED BY PLANT PERSONNEL AS "OPERATING OR MAINTENANCE PERSONNEL", "DEFICIENT PROCEDURE" OR "HUMAN ERROR"

IDENTIFICATION OF HUMAN ORIGINATED FAILURES.

CLASSIFICATION OF THE DIRECT CAUSES OF ERRORS INTO :

- OMISSION (INCL. RESTORATION ERRORS),
- MISTAKES AMONG ALTERNATIVES,
- WRONG SETTINGS,
- OTHER WRONG ACTIONS, OR
- DEPENDENT FAILURES.

Saved 14.2.95 by kjl as d:\tekstit\hccf\devtyp0.doc

VTT AUTOMAATIO
Teollisuusautomaati

TVO I II EQUIPMENT PLACE IDENTIFICATION NUMBER: **656 T003**

WORK NUMBER: **45738** YEAR: **1992**

DATE (fault detected):**26.08.92** time: **11.15** DATE (repair started): **26.08.92** time: **13.00**

Date (work finished): **26.08.92** time: **17.36**

The written text in the failure report of the plant (description of fault and corrective actions):

656 K433 L2 T3 low level alarm. T3 will not be filled. The power cabling to the outdoor pump cut at the erection work place of the start-up transformers.

The cause classification in the failure report (1-2 squares): A B C D W

Complementary information (possible time relation or functional connections to other failures, conflicting information, etc)

The power supply cables cut to the fuel fuel supply pumps 656 P011 and 656 P012 of the two day fuel tanks of the emergency diesel generators.

..(The information under this line was prepared by follow-up analysis of the reporting).....

I INFORMATION ON THE WORK TASK WHERE THE DEVIATION OCCURRED

Cause of the deviation unclear Deviation possibly caused in **Deviation certainly caused in the action:**

Own maintenance worker cut as ordered the 380 V cables at the work place of the 612 start-up transformers in order to facilitate erection of 110 kV cabling.

The action was (1-2 squares): repair preventive maintenance periodic test interval _____weeks **modification** functional test date (possible or certain) _____

Complementary information: **The power cables were thought to be unnecessary cables. No voltage due to standstill fuel supply pumps**

The caused action occurred during (1-2 crosses) : cold shutdown of reactor refuelling hot shutdown of reactor nuclear heating hot readiness of reactor power operation start-up shutting down

Complementary information (e.g. how the failure occurrence could have been avoided):

_____

_____

.....

(The information under this line will be surveyed, if the error involved as candidate on dependent failure)

II INFORMATION ON THE TASK BY WHICH THE DEVIATION WAS DETECTED

Detection method unclear **Deviation** possibly detected in **certainly detected in the task:**

Periodic loading and operation test of diesel genearator.

The detection method was: **alarm** operation supervision in control rooms, how _____ preventive maintenance **periodic testing (e.g acc. to technical specifications)** other authority inspection (e.g. NDT) equipment worked not on demand other supervision of operation (e.g. shift walk-around, alignment) functional test repair other check , which _____

date_____interval 4 (?)weeks__ 56

Detected in plant state (1-2 crosses): cold shutdown of reactor refuelling hot shutdown of reactor nuclear heating hot readiness of reactor **power operation** start-up shutting down
Complementary information (e.g. identification number of techspec test or preventive maintenance action):

Deviation not detected in the operative check (check following after the work action, 1-2 crosses): preventive maintenance functional test alignment adjusting start-up test periodic test interval _____ other check which_____ date_____ plant state, which _____
Complementary information (e.g. identification number of tech spec test or preventive maintenance task or explanation, if checking task existed ?): _____

Deviation was not detected in organizational check (independent QA and QC, performed prior to or during the the work task): **Deficient** review of: design **work planning** start-up testing program deficient acceptance inspection other review or inspection, which_____
Complementary information (e.g. which possible other review or check actions could have detected the deviation): _____

III THE TYPE; ORIGIN AND DEPENDENCE OF THE DEVIATION

Deviation type(1-2 types): omission (also restoration errors) mistakes among alternatives wrong settings **other wrong action**, e.g. due to human variability **dependent failure** (put together all dependent failures and give the following information on the dependent failures and only once) Other connected dependent failures are:

The originating mechanism of the deviation and dependence is deficient (1-2 types): design work planning procedure organisation (e.g. definition of work scope or information transfer) supervision of subcontractors same group , training , tools (selection, maintenance or QC) other , which (or complementary information, e.g. which organizational unit or personnel category): _____

The deviation was additionally caused by: **equipment close to each other**(e.g. same room) administrative easiness (e.g. sequential tasks feasible soon after each other)
Complementary information: **Cable charts outside not updated.**_____

Consequences of the deviations (e.g. unavailiability time of equipment or system):
Consequence classification in failure report: A B C D E F G H I
Delay time (from originating work task until fault detection): **2 weeks**__ hours.
Total unavailability time: _____ hours
Complementary information (e.g description of consequences): _____

IV NOTES ON ALTERNATIVE CORRECTIVE ACTIONS

The problem can be corrected (or already corrected) by:
Cable charts outside updated. Procedure for cutting of power cables prepared and in use.

France

OECD/NEA PRINCIPAL WORKING GROUP N°1
EXPANDED TASK FORCE ON HUMAN FACTEUR

TASK 4

"HUMAN FACTOR RELATED TO COMMON CAUSE FAILURES"

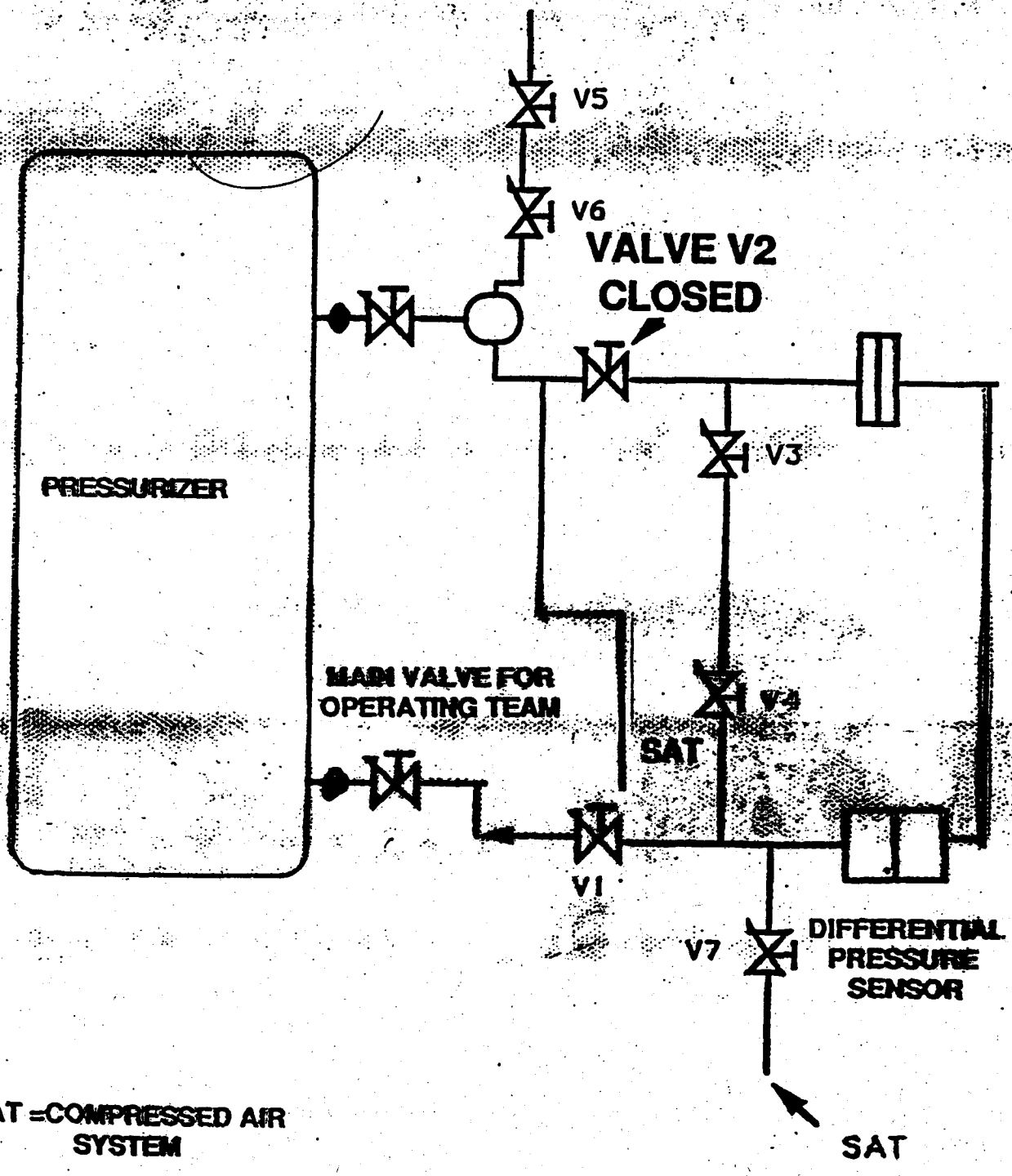
FRANCE CONTRIBUTION

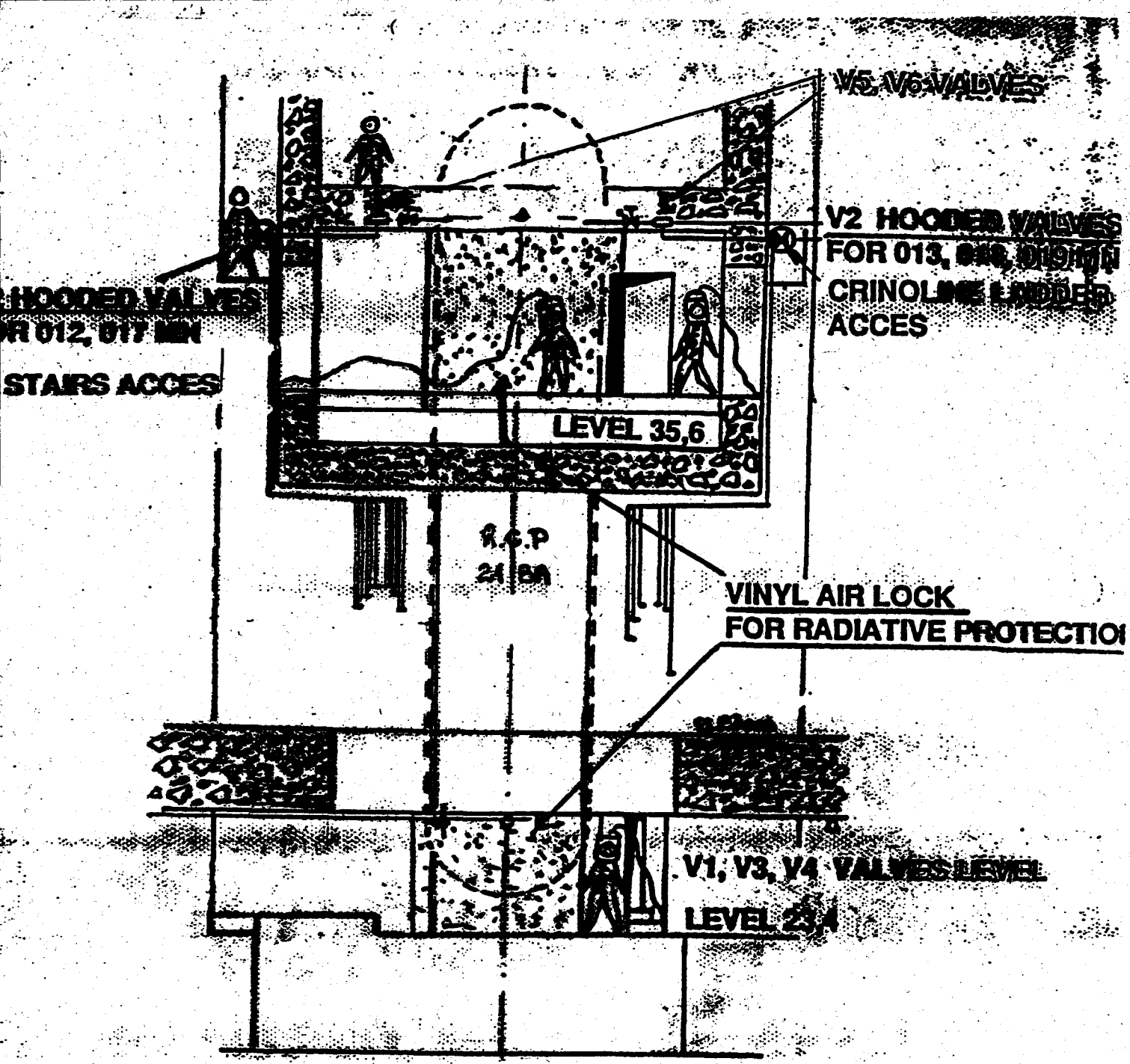
AFTER GRAVELINES INCIDENT IN SUMMER 1989

REGULATORIES REQUIERE TO STUDIE PARTICULAR IMPROVEMENT DURING OUTAGE IN THESE CASES

- **WHEN COMMON WORK IS PERFORMED ON SIMILAR COMPONENT ON REDONDANT SYSTEM**
- **WHEN WORK NEED TO USE SPECIAL PIECES OR TOOLS, MODIFYING SYSTEM,**
- **WHEN ELECTRICAL BY-PASS ARE USED**

LEVEL SENSOR SYSTEM DESIGN

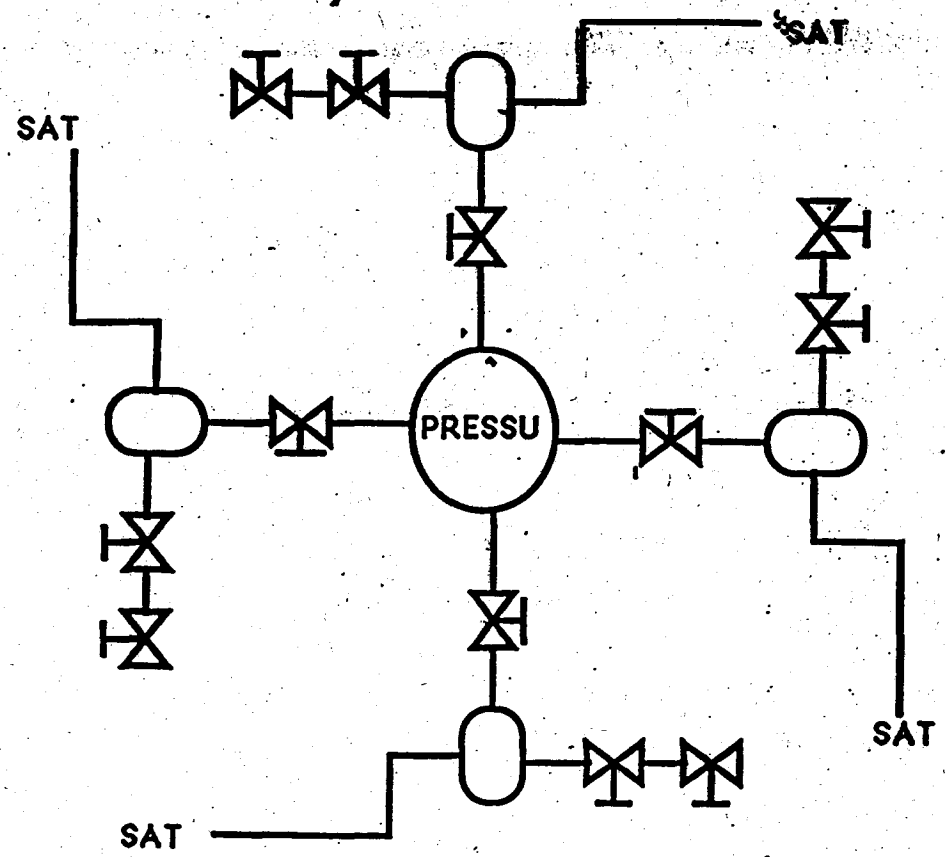




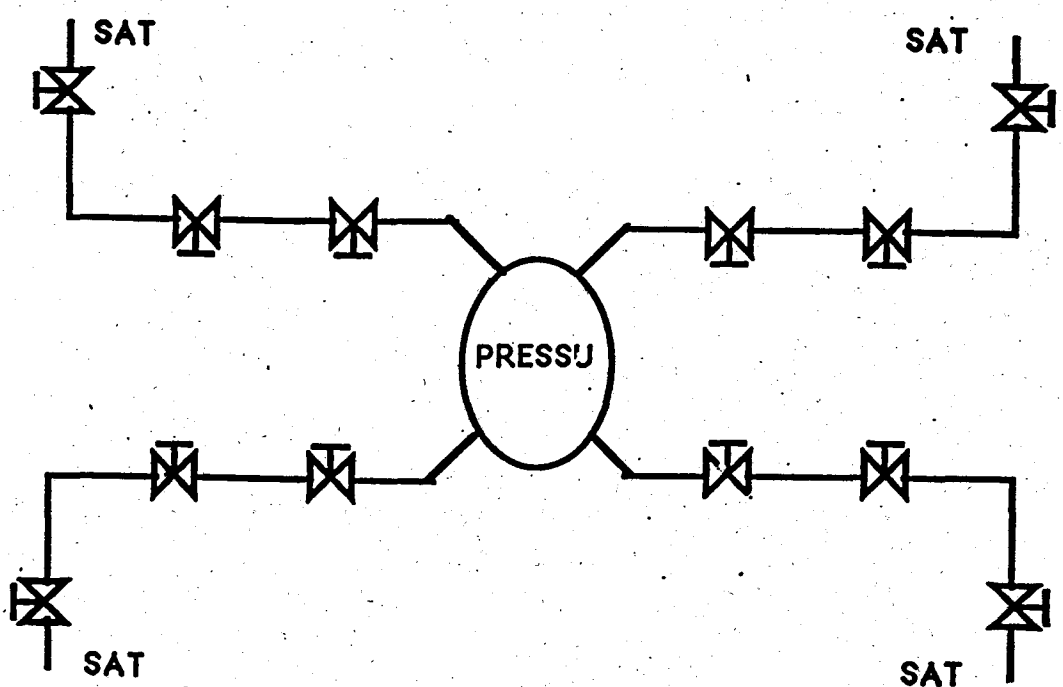
CONSTRAINTS ON SITE

- LACK OF KEY NUMBERS ON ALL THE VALVES
- SPATIAL ARRANGEMENT OF SYSTEMS IS COMPLEX
- RADIATION PROTECTION CLOTHES MUST BE USED IN THE VINYL AIRLOCK
- WATER AND COMPRESSED AIR SPRINGS ARE IN THE LOW LEVEL

PERCEPTION OF SYSTEMS BY OPERATORS ON HIGH LEVEL

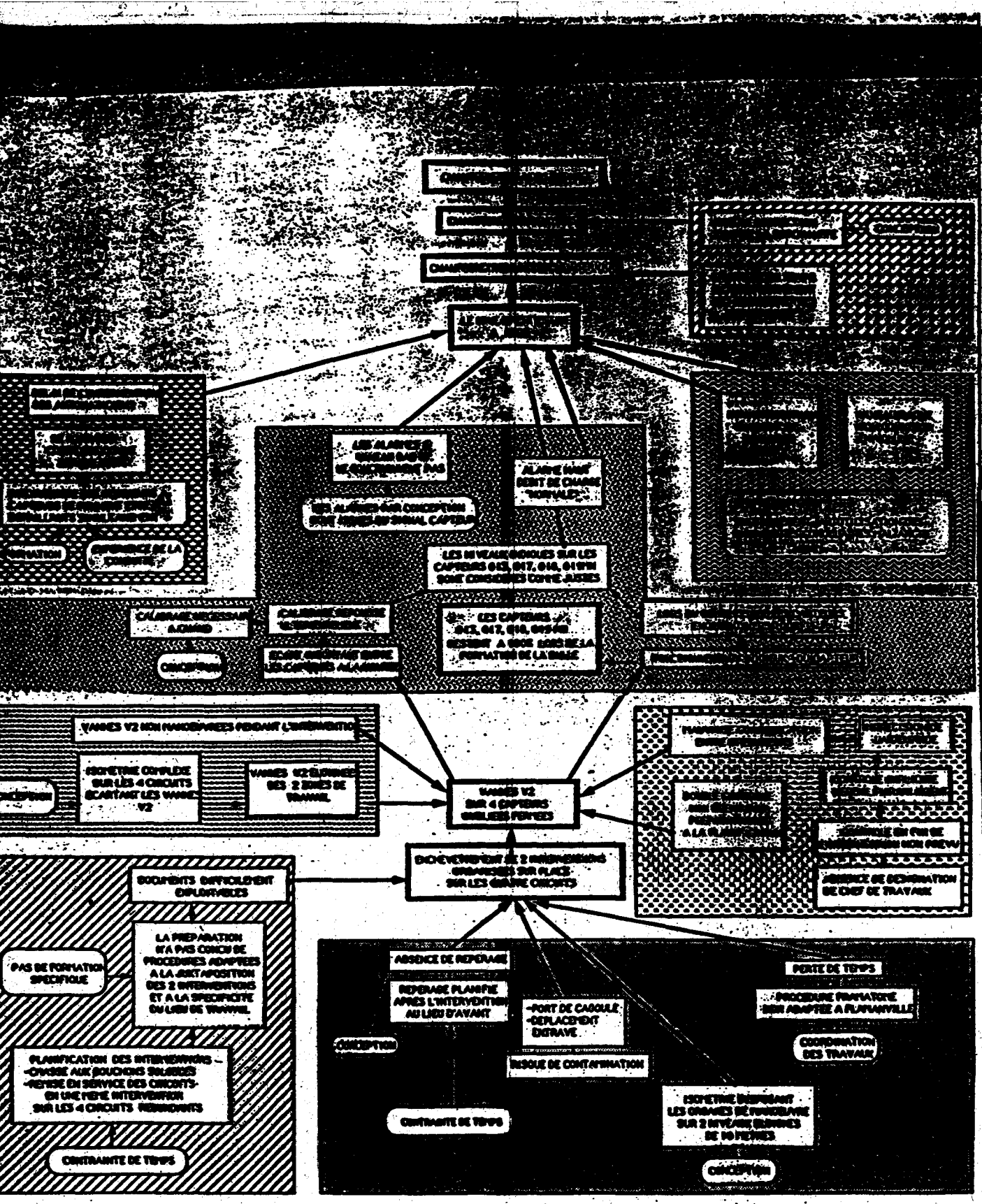


PERCEPTION OF SYSTEMS BY OPERATORS ON THE LOW LEVEL



SAT IS A COMPRESSED AIR SYSTEM

LARGE SIGHT OF SYSTEMS AND OF THEIR FUNCTIONS IS LOST



DIAGNOSTIC

CAPTEUR 012 MN

CONDITIONS PARTICULIERES DE L'INTERVENTION

TRAVAUX PREALABLES A L'INTERVENTION

INFORMATION EN SALLE DE COMMANDE

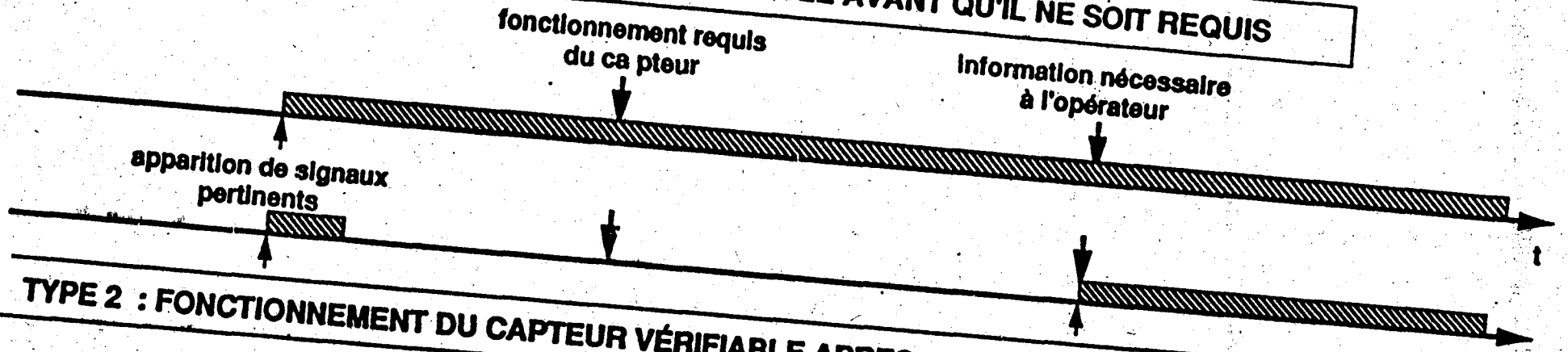
CHAUFFERETTES

CONTROLE

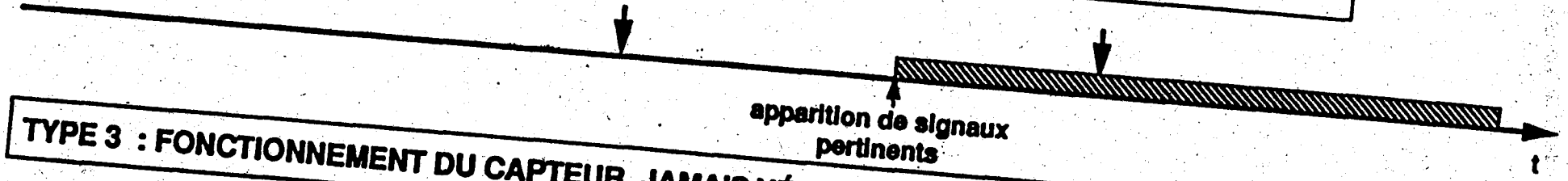
CONTRAINTE SPECIFIQUE AUX VANNES V2

QUAND VERIFIER LE CARACTERE OPERATIONNEL DES CAPTEURS ? : TROIS TYPES DE CAPTEURS

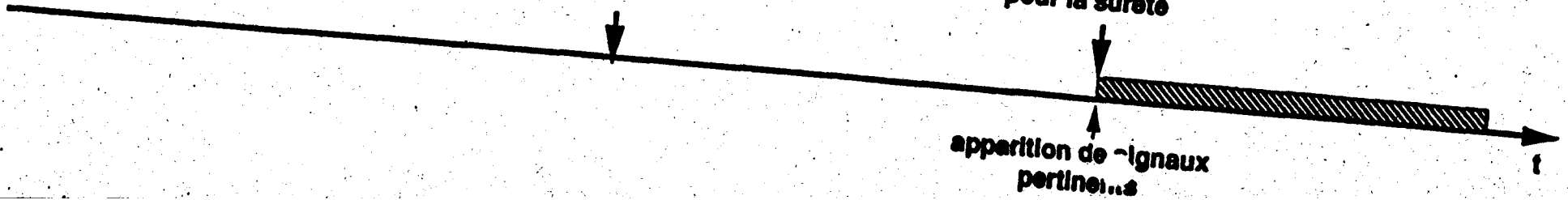
TYPE 1 : FONCTIONNEMENT DU CAPTEUR VÉRIFIABLE AVANT QU'IL NE SOIT REQUIS



TYPE 2 : FONCTIONNEMENT DU CAPTEUR VÉRIFIABLE APRES QU'IL SOIT REQUIS



TYPE 3 : FONCTIONNEMENT DU CAPTEUR JAMAIS VÉRIFIABLE



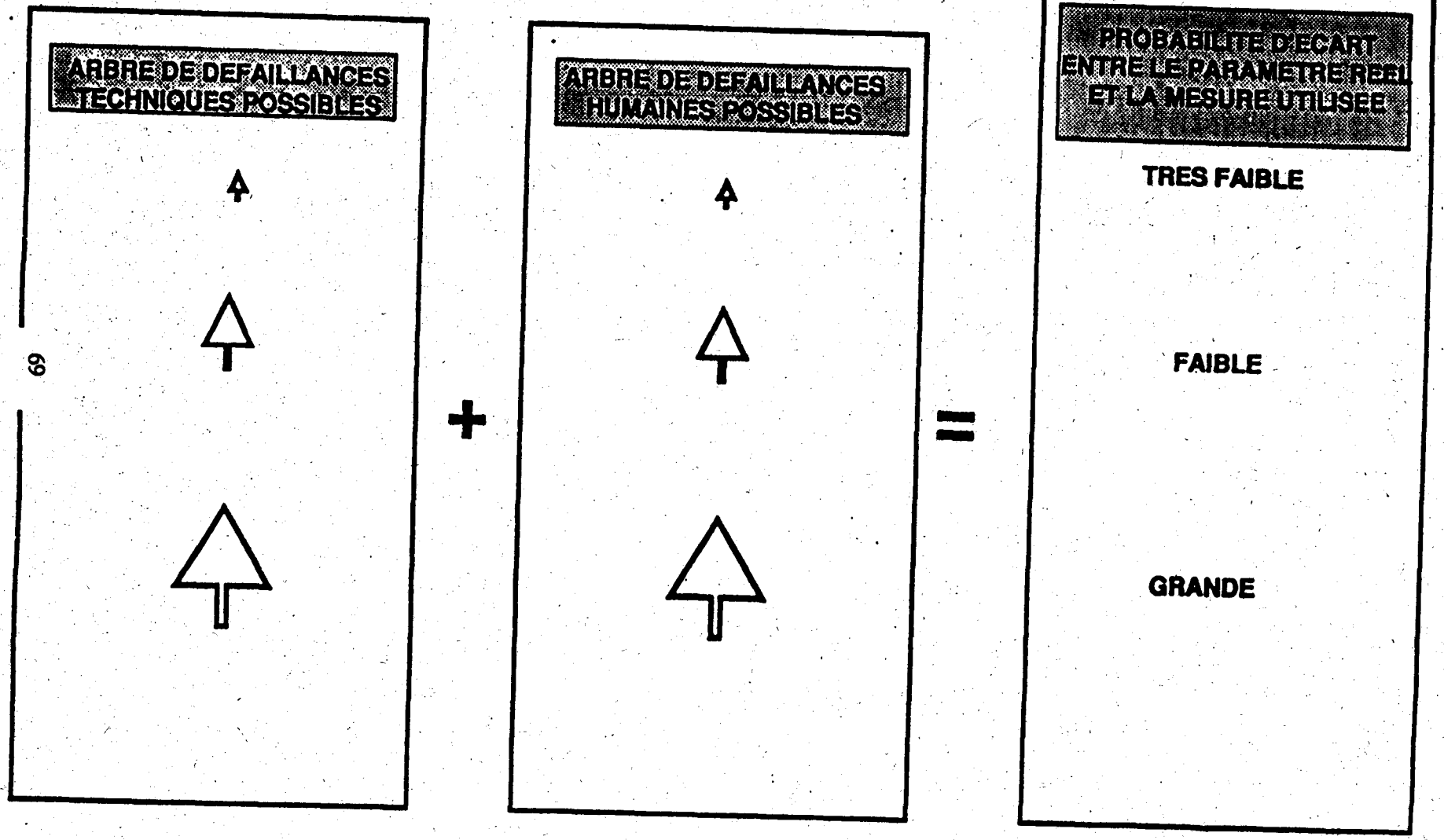
LES DIFFERENTES CATEGORIES DE CIRCUITS DE CAPTEURS / CONCEPTION

TYPES DE CIRCUITS DE MESURES	PARAMETRES PHYSIQUES	TRANSFORMATIONS AVANT SIGNAL	ARBRE DE DEFAILLANCES TECHNIQUES POSSIBLES
1 POINT DE PRISE DE MESURE	P	SIMPLE	
2 POINTS PROCHES CIRCUITS SIMPLES	P' P''	RELATIVEMENT SIMPLE	
2 POINTS ELOIGNES CIRCUITS COMPLEXES PARAMETRES INFLUANTS MULTIPLES	P'_1 P'_2 P'_3 P''_1 P''_2 P'_3	COMPLEXE	

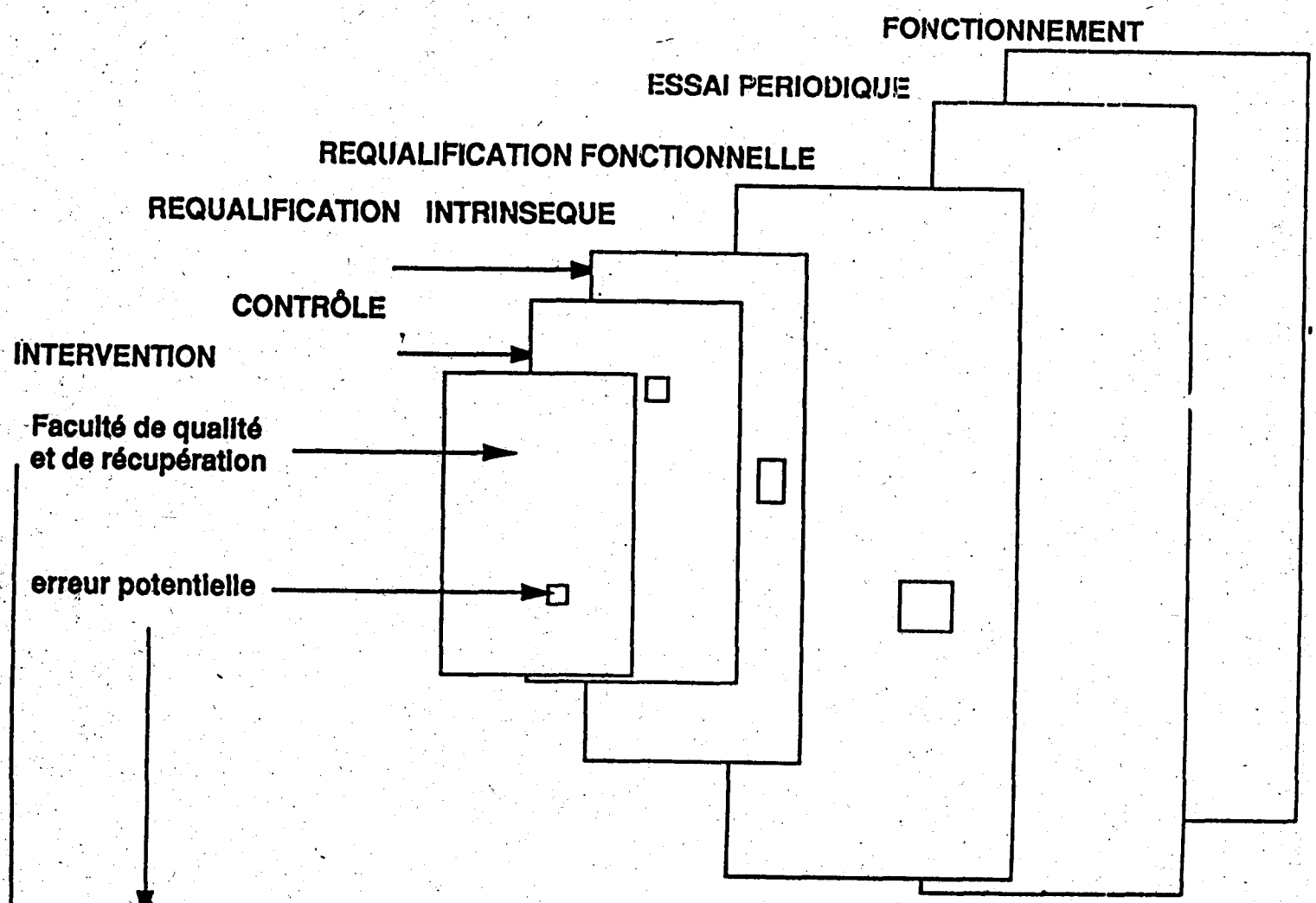
INFLUENCE DE LA CONCEPTION DES DIFFERENTES CATEGORIES DE CIRCUITS SUR L'ACTIVITE HUMAINE

TYPES DE CIRCUITS DE MESURES	CONSEQUENCES SUR L'ACTIVITE HUMAINE	ARBRE DE DEFAILLANCES HUMAINES POSSIBLES
1 POINT DE PRISE DE MESURE	PEU DE MAINTENANCE PAS DE LIGNAGE SIGNAL NON ENTACHE D'INCERTITUDE : OPERATEUR CONFIANT → PROBABILITE DE DEFAUTS INFIME	
2 POINTS PROCHES CIRCUITS SIMPLES	MAINTENANCE SIMPLE LIGNAGE SIMPLE SIGNAL FIABLE → FAIBLE PROBABILITE DE DEFAUTS OPERATEUR CONFIANT	
2 POINTS ELOIGNES CIRCUITS COMPLEXES PARAMETRES INFLUANTS MULTIPLES PLAGE DE LECTURE LIMITEE	MAINTENANCE COMPLEXE NOMBREUX LIGNAGES SIGNAL RELATIVISABLE → PROBABILITE DE DEFAUT IMPORTANTE : L'OPERATEUR L'INTERPRETE	

PROBABILITE D'ECART ENTRE LE PARAMETRE REEL ET LA MESURE UTILISEE



MECANISME DE CONSTRUCTION DE LA DISPONIBILITE DES SYSTEMES



Les erreurs potentielles sont reliées aux conditions d'intervention et de coordination

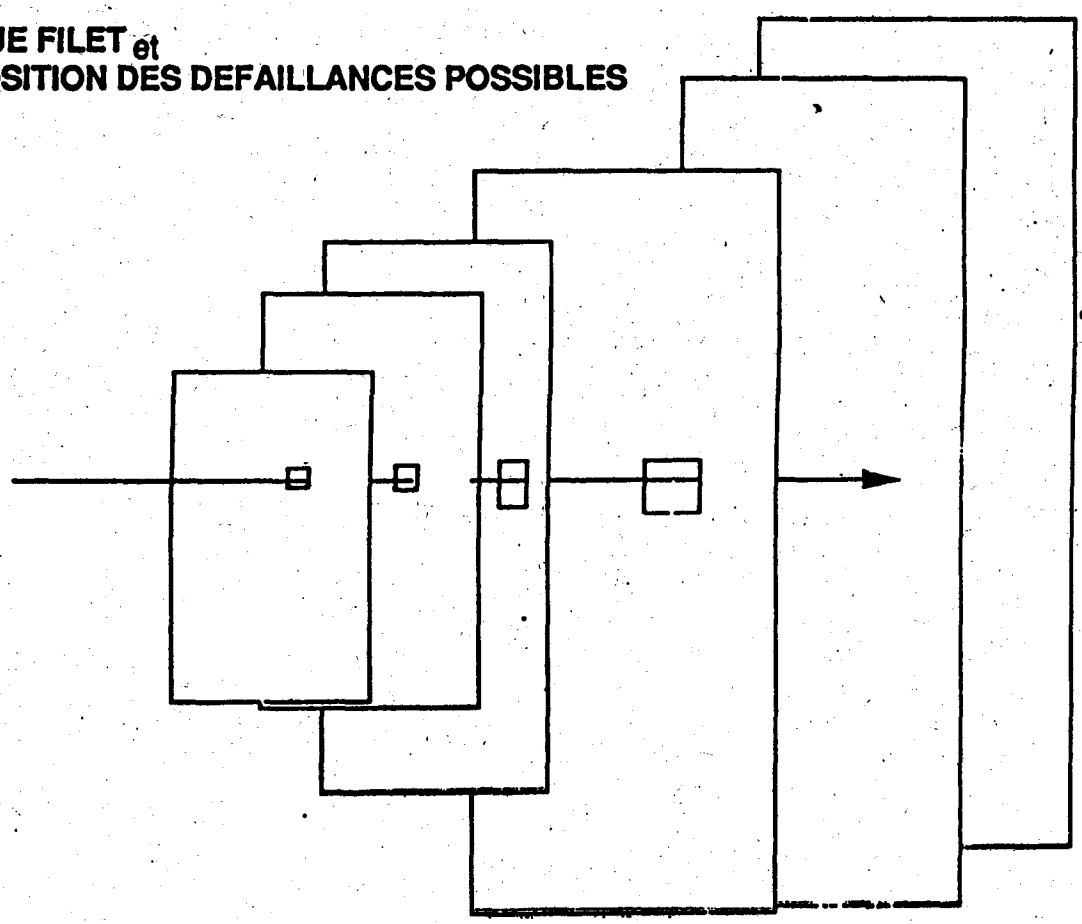
Les facultés de qualité et de récupération sont liées à l'expérience, aux connaissances des autres activités

SEFH/GB

FIABILITE D'UN SYSTEME ORGANISATIONNEL

PROBABILITE DE DEFAILLANCES DES FILETS ORGANISATIONNELS LIEE A LA QUALITE DE CHACUN DES FILETS

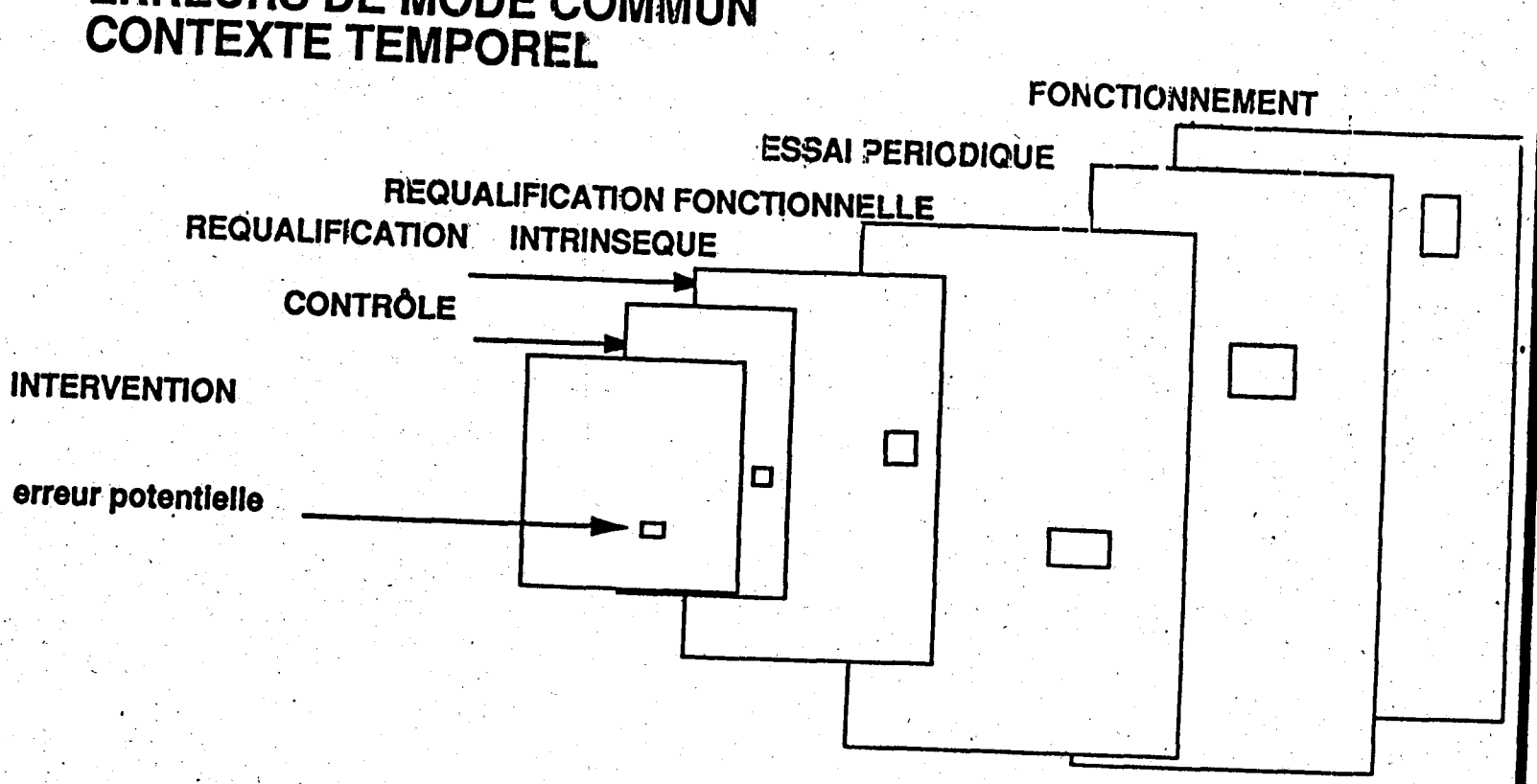
QUALITE DE CHAQUE FILET et MODE DE SUPERPOSITION DES DEFAILLANCES POSSIBLES



Certaines conditions semblables pour différentes activités, accroissent le risque de superposition des erreurs.

SEFH/GB

ERREURS DE MODE COMMUN
CONTEXTE TEMPOREL



- Le temps imparti est court, le délai disponible conduit à réduire le niveau de vérification de chacun, et le niveau de qualité de chaque action.

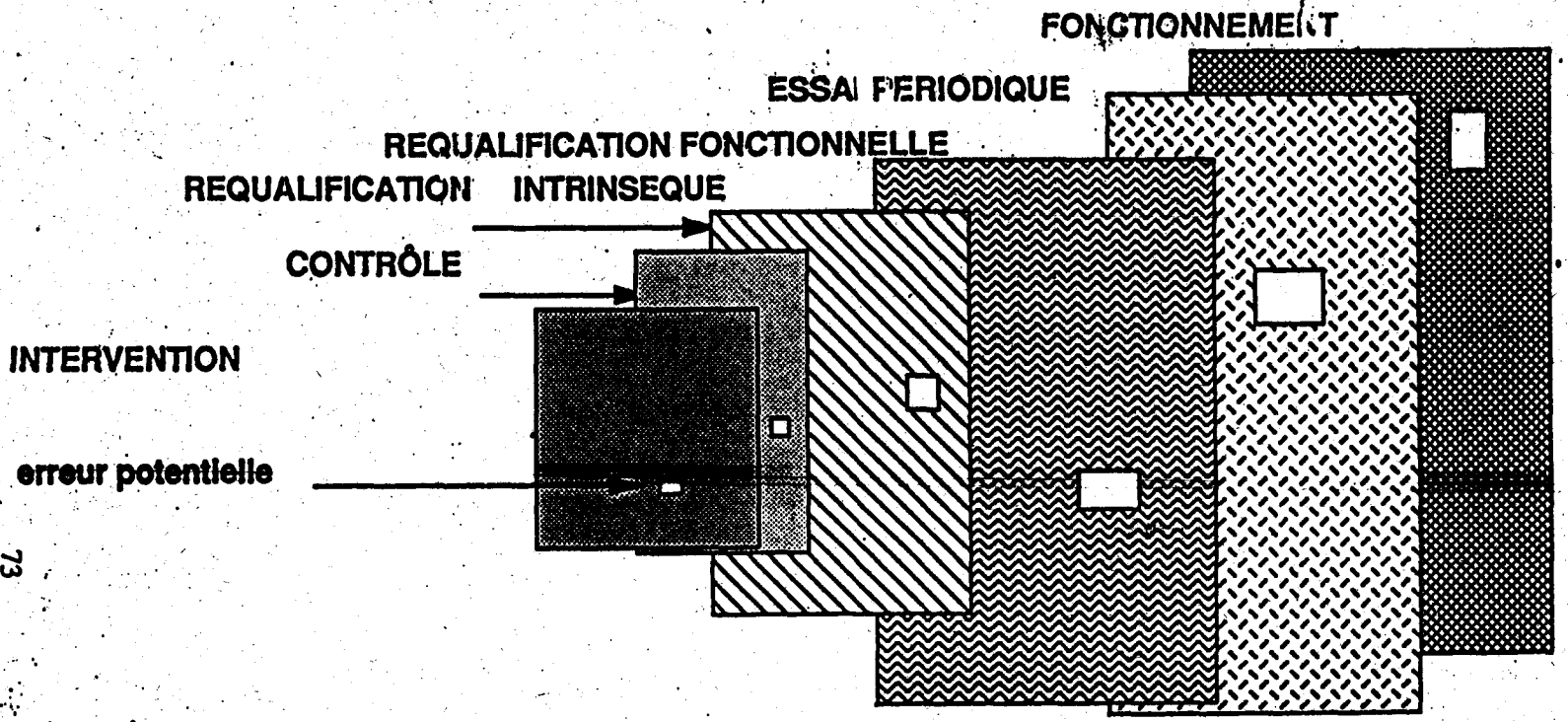
- Il n'y a pas de temps disponible pour la coopération avant la date limite

- La date limite représente un événement social pour tous.

- l'ensemble des acteurs se focalise sur un objectif temporel.

- Fatigue de l'ensemble des acteurs liés à l'organisation temporelle

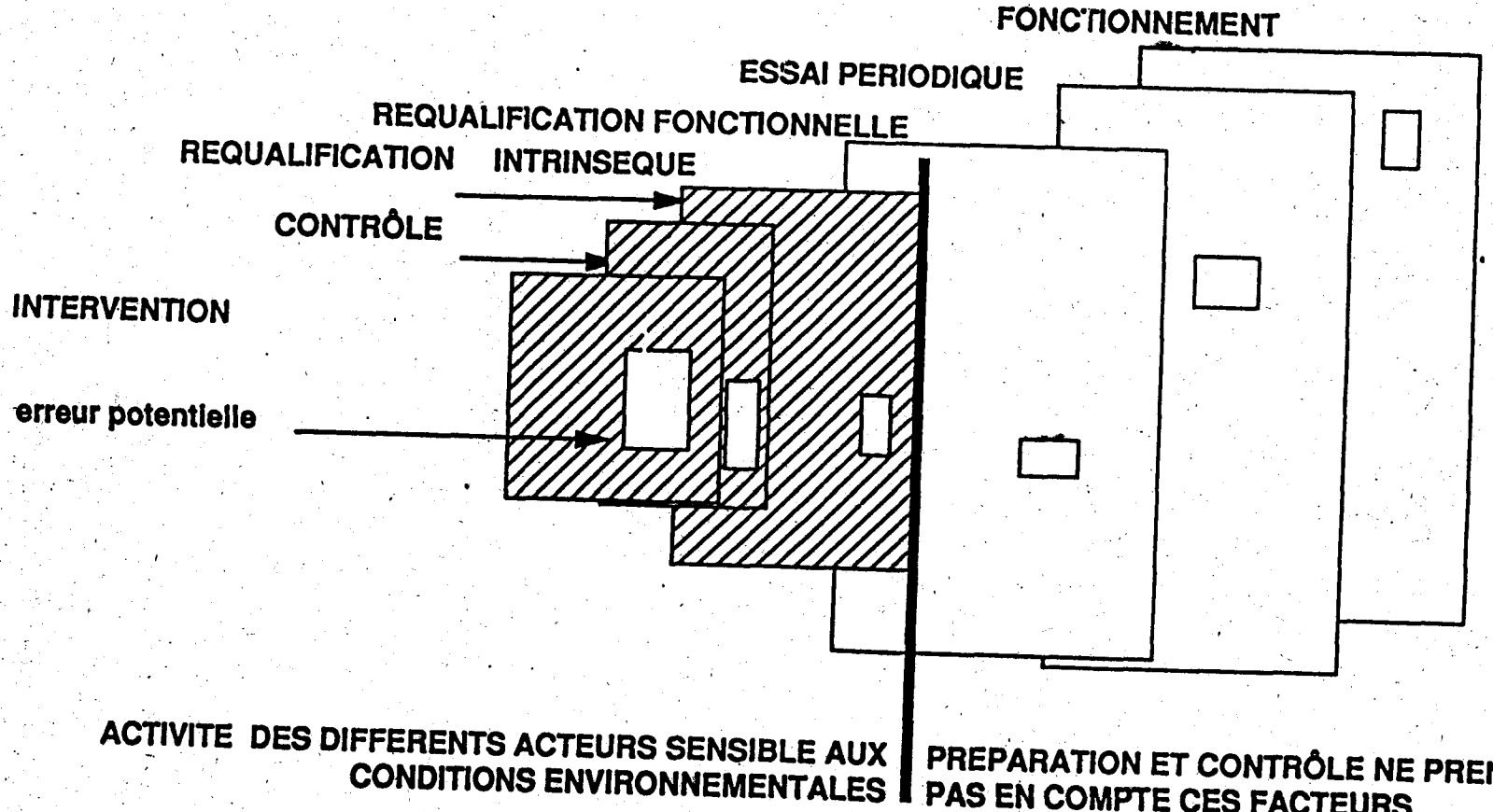
ERREURS DE MODE COMMUN
CONTEXTE ORGANISATIONNEL



_ répartition des activités à différentes fonctions de logiques différentes qui ne communiquent pas.
- absence de recouvrement dans la connaissance des éléments de diagnostic de chaque fonction.
- les éléments de l'arbre de défaillance n'ont pas été reliés a priori
Les contrôles se s'articulent pas sur cette logique.
Les difficultés de l'intervention ne peuvent pas être décodées en risques potentiels

ERREURS DE MODE COMMUN
CONTEXTE ORGANISATIONNEL

RELATION PRESTATAIRE SITE



SEFH/GB

FONCTIONNAL ANALYSIS OF THE REDONDANT SYSTEMS

IN PARTICULAR :
- WHAT INPUT AND OUTPUT OF THE SYSTEME
- INTERACTION WITH THE DIFFERENTS VARIABLE
- WHAT ELECTRICAL, GAZ OR LIQUID SOURCES IS USED

ERGONOMIC ANALYSIS

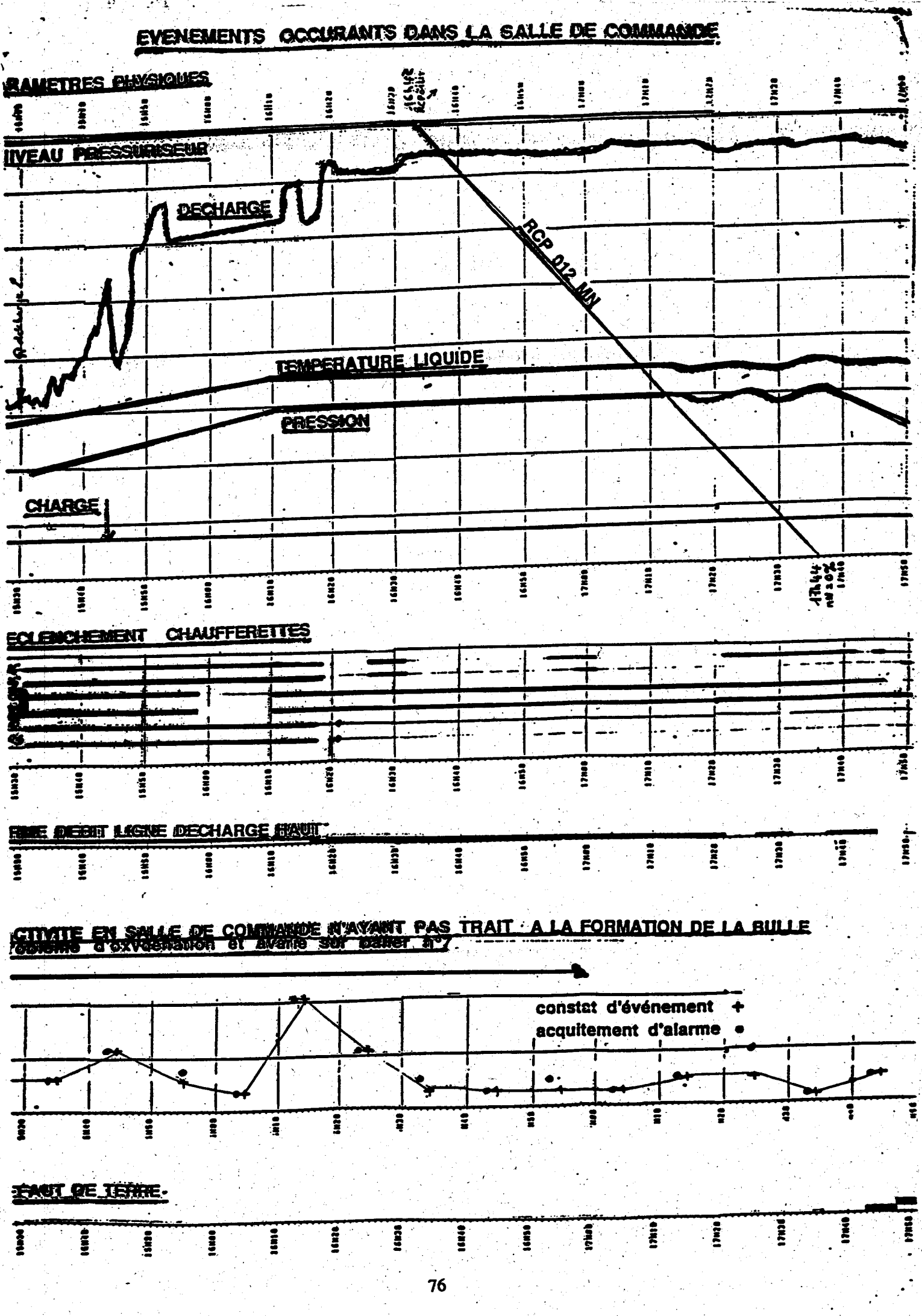
- WHAT KIND OF ACTIVITIES FOR MAN
  + WHAT PROCEDURES ,
  +WHAT TOOLS,
  +WHAT ACTIVITIES ON SOURCES

-WHICH CONSTRAINTS
-WHICH INTERFACES
-WHICH REGULATION CRITERIUM

- WHICH NEED TO OPTIMIZE ACTIVITIES

- WHEN THE RESULT OF ACTIVITY IS KNOWN

- WHAT TEST CAN BE PERFORMED
- ANALYSIS OF DETECTION, DIAGNOSTIC, TREATMENT, ACTION, AFTER WORK


EVENEMENTS OCCURANTS DANS LA SALLE DE COMMANDE
RAMETRES PHYSIQUES
IVEAU PRESSURISEUR
DECHARGE
RCP 012 MN
TEMPERATURE LIQUIDE
PRESSION
CHARGE
ECLENCHEMENT CHAUFFERETTES
DEBIT LIGNE DECHARGE HAUT
CLIMTE EN SALLE DE COMMANDE N'AYANT PAS TRAIT A LA FORMATION DE LA BULLE
Système d'extraction et alarme sur palier n°
constat d'événement +
acquitement d'alarme •
FAUT DE TERRE.

FONCTIONNAL ANALYSIS OF THE REDONDANT SYSTEMS

IN PARTICULAR :
- WHAT INPUT AND OUTPUT OF THE SYSTEME
- INTERACTION WITH THE DIFFERENTS VARIABLE
- WHAT ELECTRICAL, GAZ OR LIQUID SOURCES IS USED

ERGONOMIC ANALYSIS

- WHAT KIND OF ACTIVITIES FOR MAN
  + WHAT PROCEDURES ,
  +WHAT TOOLS,
  +WHAT ACTIVITIES ON SOURCES

-WHICH CONSTRAINTS
-WHICH INTERFACES
-WHICH REGULATION CRITERIUM

- WHICH NEED TO OPTIMIZE ACTIVITIES

- WHEN THE RESULT OF ACTIVITY IS KNOWN

- WHAT TEST CAN BE PERFORMED
- ANALYSIS OF DETECTION, DIAGNOSTIC, TREATMENT, ACTION, AFTER WORK

CAUSAL ANALYSIS OF CRITICAL FAILURE

- DEGREE OF ROBUSTNESS AND RELIABYLITY OF THE SYSTEM
- TYPE OF FAILURE
- SCENARIO TO GO TO FAILURE
-IMPORTANCE OF THE DIFFERENT ELEMENTS OF THE SYSTEM TO GO TO A FAILURE

ERGONOMIC ANALYSIS

- IMPORTANCE AND ROLE OF OPERATOR IN THESE SCENARIO
- IDENTIFICATION OF CAUSES (ERGONOMIC, TECHNICAL, ORGANISATIONNAL, COGNITIVE) WHICH CREATE FAILURES
- ANALYSIS OF DETECTION, DIAGNOSTIC, TREATMENT, ACTION, AFTER FAILURE
- WHICH KIND OF TOOLS ARE NEEDED FOR
- ERGONOMICS CONSTRAINT IN THESE WORKS

ETAPE / Domaine d'analyse	1. Analyse fonctionnelle		2. Analyse de disponibilité		3. Identification et classement des défaillances		4. Analyse causale des défaillances critiques		5. Propositions d'amélioration et validation	
	Objectifs	Méthode et/ou outil	Objectifs	Méthode et/ou outil	Objectifs	Méthode et/ou outil	Objectifs	Méthode et/ou outil	Objectifs	Méthode et/ou outil
Analyse de fiabilité	• Structure fonctionnelle du système • Différentes fonctions et leurs interactions • Mission du système, entrées et sorties • Variables du process et leurs interactions • Interfaces d'information et de commande • Répartition de la gestion des variables entre (automatisme-machine-opérateur)	• Diagrammes blocs • Graphes de fluence	• Pourcentage des différentes configurations de fonctionnement • Temps de disponibilité d'un composant et la probabilité de passage d'un état disponible à un état indisponible et vice-versa	• Arbre d'événements • Graphe de Markov	• Calcul et analyse des conséquences d'un événement initiateur (d'un système séquentiel) • Liste hiérarchisée (disponibilité, fréquence, gravité) des différents modes de défaillance pouvant l'affecter	• Arbre d'événements • Analyse des modes de défaillance et de leurs effets	• Mise en évidence du degré de fragilité du système • Combinaisons des pannes • Différents scénarios aboutissant à l'apparition d'un événement donné • Mise en évidence de la place des différents éléments du système dans l'apparition de l'ENS	• Arbre de défaillance	• Amélioration de la fiabilité et de la disponibilité du système socio-technique • Evaluation coût-efficacité des améliorations	• Analyse de sensibilité (simulation d'AdD en fonction des différentes hypothèses suggérées par les résultats précédents
Analyse ergonomique	• Description des tâches prescrites • Description des activités réelles • Identification des : ◆ contraintes ergonomiques ◆ différents interfaces existants ◆ critère de régulation • Mise en évidence place de l'opérateur dans le système • Classement des interfaces en fonction de leur degré d'utilisation et de pertinence par rapport à l'activité • Recensement des besoins pour une réalisation optimale de l'activité • Gestion des aléas	• Analyse documentaire et interview • Observation systématique de l'activité à l'aide de : ◆ camescope ◆ magnétophone ◆ interview et auto-scopie	• Taux d'occupation de l'opérateur • Planification temporelle des opérateurs selon les phases du travail et les situations	• Analyse (par observation, interview...) des activités spatio-temporelles des opérateurs	• Impact des dysfonctionnements sur l'activité des opérateurs et sur le système • Place de l'opérateur dans la performance du système • Typologie des erreurs • Recensement des moyens de compensation technique et/ou humain	• Analyse des activités centrée sur les dysfonctionnements (nature, genèse, impact) • Analyse des erreurs et des activités mises en jeu	• Mise en évidence du rôle et place de l'opérateur dans l'apparition d'un événement critique donné • Identification de l'ensemble des causes (d'origine technique, ergonomique, organisationnelle, cognitive) générants des erreurs, dysfonctionnements et/ou perturbant la mission du système) • Analyse des activités de récupération (détection, diagnostic, traitement, action...) • Stratégie de conduite en temps partagé • Identification des différents moyens (matériels et informationnels) nécessaires à ces activités • Evaluation du temps de ces activités • Dégager les contraintes ergonomiques générées par ces activités	• Arbre de défaillance • Simulation in situ de certains dysfonctionnements critiques et observation centrée sur l'analyse des activités de récupération	• Adaptation optimale du système homme-tâche-système technique • Evaluation coût-efficacité des améliorations	• Analyse de sensibilité (simulation d'AdD en fonction des différentes hypothèses) suggérées par les résultats précédents

COMMON MODE INCIDENTS CAUSED BY THE USE OF MEASURING AND CALIBRATION INSTRUMENTS

1. INTRODUCTION

The use of measuring and calibration instruments is the root cause of a number of incidents. Anomalies associated with such instruments or their use may indeed result in common mode failures affecting redundant equipment or items of equipment ensuring the same function.

2. INCIDENT ANALYSES

2.1 CHOOZ A - 19 JULY 1988

2.1.1 Development of the incident

On 19 July 1988, investigations in progress for a week following unusual openings of the pressurizer relief line isolation valves were being carried out on the reactor coolant pressure control while the unit was operating at 100% of the rated power. The pressure control channel of the pressurizer at the Chooz plant is made up, besides safety valves, of two relief lines each comprising an isolation valve and a relief valve intended to avoid opening safety valves. The operator who has not found the root cause of the problem decided to measure the reactor coolant pressure and to that end connected a previously tested standard sensor with an instrument tap provided for this purpose. Nine pressure sensors in the reactor coolant system, seven of them involved in the development of certain reactor protective devices, then revealed a standardization defect which led them to give a pressure 3 bar higher than the actual reactor coolant pressure.

2.1.2 Analysis of consequences

This incident was without direct consequence for safety but would have resulted in a delay of the order of a few seconds when operating the protective devices during a pressure drop. However, if the discrepancy had been more significant, the situation would not have been covered by accident studies.

2.1.3 Analysis of causes

This defect is due to the use *in situ* of a portable pressure generator unsuitable for checking these sensors, at unit startup in April 1988. Indeed, the sensors had been tested, as usual, on a calibration bench in hot shop after removal, during the annual shutdown in May-June 1987. In this specific case, it was an additional check before startup, without removing the sensors, as the unit shutdown had been prolonged for several months. After detection of the incident, a verification of the portable pressure generator manometer evidenced a 3-bar discrepancy throughout its measuring range.

This incident shows a typical case of lack of functional requalification after maintenance work in April 1988. Installation of a standard manometer following a phenomenon not directly related to the anomaly (an incorrect cross-calibration of the sensors does not mean necessarily an incorrect standardization of the latter) enabled the anomaly to be immediately detected.

2.2. GRAVELINES 6 - 31 MAY 1990

2.2.1 Development of the incident

On 31 May 1990, during the performance of a periodic test on the Unit 5 nuclear power measuring channels, the foreman who suspected the ramp generator he was using as a test equipment of yielding wrong values decided to check it. This check confirmed his suspicions. The intrument did not comply with the manufacturer's specifications.

This instrument which had however been checked on 7 May 1990 by a subcontractor approved by the National Office of Metrology was used on 22 May 1990 to perform the same type of test at Unit 6 and was the root cause of readjustments on the four nuclear power measuring channels. On checking with an instrument complying with specifications, the operator noticed that the adjustments of power channels at unit 6 were not correct and that the unit had been operating for 9 days with this anomaly.

2.2.2 Analysis of consequences

The incident was without direct consequence for safety. However, an assessment of the potential consequences of these misadjustments was carried out by EdF. The adjustments of the reactor protective devices on neutron flux variation were affected but the available margins for the core which had just undergone refuelling, with respect to generic assumptions of accident studies were sufficient to ensure that the reactor safety would not have been jeopardized, in the event of an accident, during this period.

2.2.3 Analysis of causes

The root cause of this incident was the use of a calibration instrument not properly standardized by the subcontractor and not checked on its return to the site to make sure it was in compliance with specifications.

Moreover, the lack of questioning attitude from the worker who carried out readjustments at unit 6 without raising issues as well as the absence of initial and final readings in the test performance procedure favoured this incident.

An early detection of this anomaly was not possible because of the impossibility of carrying out a fonctional requalification test under real conditions .

2.3. DAMPIERRE 1 - 21 NOVEMBER 1990

2.3.1 Development of the incident

On 21 November 1990, the chemists noticed that the measured value of the mean pressure safety injection accumulator boron concentration did not comply with technical

specifications (value measured : 2560 ppm for a required value between 2325 and 2475 ppm). This value was questioned since the previous measurement carried out on 11 October 1990 complied with specifications (2410 ppm) and there had been in the meantime no water movement likely to modify the boron concentration. After investigations, it has been found that the error was due to the titrimeter (instrument used to determine the boron concentration) which overestimated the boron concentration value of about 5.6%.

After rectification of the error and checking of the other tanks containing borated water, two tanks proved to have boron concentrations which did not comply with technical specifications. The boron content was altered which made it possible to get back to the values required by technical specifications on 22 November 1990.

2.3.2 Analysis of consequences

The incident was without direct consequence for the safety of the installation. However, this anomaly led to a common mode failure likely to affect all of the borated water tanks at unit 1 since the analyser is used to measure the boron concentration of eight tanks and to a defect at unit 2 as a tank is common to units 1 and 2.

2.3.3 Analysis of causes

The incident is due to an improper use of a measuring instrument. Indeed, the value of the strength of the soda used for dosing boric acid was not consistent with the value to be found in the memory of the titrimeter computer. In fact, when the standard soda solution was replaced on 11 November 1990, the operative did not validate the strength of the solution and the instrument stored the value of the previous strength.

The absence of validation of the measurement given by the titrimeter by another measurement favoured the incident. The operator decided in this respect to check the measuring channel, before use, by an analysis of a known boron solution used as a standard.

3. INCIDENTS OR SIMILAR EVENTS

Following the degradation in offsite power supplies which occurred on 12 January 1987 (refer to IRS no 09.13.00), an error in setting the rotor overvoltage protection relays caused the spurious startup of the Chinon 3 turbine generator. The back-up diesel generators which started when the power source switched were not automatically connected to the 6.6 kV redundant trains A and B switchboards owing to the fact that the undervoltage protection relays had been set at 0.6 times the rated voltage instead of 0.7 times the rated voltage and the voltage, when it dropped, remained between 0.6 and 0.7 times the rated voltage. This setting error is due to the failure of the calibration bench used to set the relays. Furthermore, this bench which was made locally was used for the whole site of Chinon.

On 18 August 1987, the Nogent 1 unit was being pressurized at the beginning of precritical hot tests. The pressure was being monitored in the control room on the readouts for the four pressure sensors in the reactor coolant system and the inhibition order for the closure of isolation valves was given at 140 bar instead of 145 bar (expected value). As a matter of fact, some time before, the manufacturer had adjusted the internal frequency of the sensors so as to limit chatters on the pressurizer spray valves which are set based on the information from these sensors. This operation which should have had no effect on the adjustments of the sensors in fact shifted the sensors from the zero value. The anomaly was corrected by cross-calibration of

the sensors with the sensor for measuring pressure in the reactor coolant system at the coolant system spray inlet during reactor shutdown, using a precision measuring instrument.

A maintenance-related human error which resulted in an incorrect set pressure of a steam generator mechanical safety valve caused the opening of the valve at 76.2 bar on 4 July 1988 at the Paluel 3 unit.

In the same way, the malfunction of a recorder used during the set pressure test of the steam generator power-assisted protection valves on 30 March 1990 was the root cause of an error in setting the power-assistance panels which resulted in the opening of several valves on 23 and 25 July 1990 at the Fessenheim 2 unit.

On 16 September 1991, a discrepancy between theoretical critical boron concentrations - with all rod clusters removed and the rod bank used for the primary system temperature control inserted - and the same values measured on the site using a measuring instrument (titrimeter) was highlighted during core conformity physics tests during startup at the Chinon 2 unit. An error, during dosing, in determining the strength of the soda used for measuring the boron concentration is the root cause of this discrepancy and distorted all the measurements performed at units 1 and 2 by reducing them of 5.5%. This led the operator to alter the boron content of borated water tanks as well as to calibrate automatic boron meters for measuring the boron concentration in the reactor coolant system of both units. After correction of the error, four tanks had boron concentrations which did not comply with technical specifications (the boron concentration was too high). The consequences of this incident were opposite to those of the Dampierre 1 incident (boron concentration too low) but the initiating cause was the same (strength of the soda). For its part, this incident affected two units in power (unit 1 at 100% power, unit 2 at 8% power at startup).

On 6 September 1992, at the Chinon B4 unit, the use of an erroneous software to calculate the reference nuclear power by thermal heat balance led to underestimate the nuclear power of 3% and calibrate all the nuclear power measuring channels. This error was without real consequence since the unit was operating at 75% nuclear power in extended cycle but it could have led, considering the adjustments performed, to exceed the fuel assembly design linear power density if the unit had been operating at full power.

On 7 September 1993, during an annual steam generator safety valve set pressure test at the Cruas 2 unit, the use of a test pressure sensor which affected considerably the measurement owing to an integrated response time of 0.56s not known by the worker led to underestimate the set pressure of these valves and therefore to set beyond their limits the first 9 valves tested before identification by the operator of the root cause of these excessive set pressures. Moreover, this sensor had been used on 25 May 1993 on unit 1 for the same test. A check performed by the operator revealed that 6 valves had a set pressure far beyond their tolerance limits.

4. MEASURES TAKEN BY EDF

The conclusions drawn by the EDF central services from the incident analyses led them to draw up a national directive (DI 061) entitled "Standardization and test of measuring instruments and standards" applicable on sites since 1 January 1992 which set out provisions

for measuring equipment as regards :

- management principle
- standardization or test operations
- control of these operations
- test at each use
- monitoring of each use.

5. LESSONS DRAWN FROM THESE INCIDENTS

Incidents of this type are various and many but trends can be derived from their analysis.

One of the characteristics of such incidents is the propagation of the adjustment defect to several items of equipment as a result of an incorrect standard or a human error when using a standard.

Indeed, such a defect then appears as a "virus" and the equipment or the operative involved is therefore likely to "contaminate" all the items of equipment on which both of them carry out work.

In fact, when an error detected on redundant items of equipment using the same instrument, involving systematically a similar modification in their adjustments, is not a common mode failure related to the design or ageing, it is highly likely that it is a common mode failure related to the instrument itself, its use or a previous maintenance work. The worker has therefore to question himself and adopt an attitude of "self regulation" as suggested by the Gravelines operator. **It is worthy of note that such an approach would have made it possible to detect more rapidly most of the above-mentioned anomalies.**

The analysis of these incidents leads to highlight three main initiating causes for such defects, namely the use of a faulty instrument, the use of an unsuitable instrument and the improper use of an instrument. It highlights that the workers are not sensitive enough to the common mode nature of these defects with respect to their behaviour.

1/ Use of a faulty instrument

This type of incident is mainly due to the fact that the conformity of a measuring instrument is not called into question after its standardization or test by a subcontractor or that there is no monitoring of its characteristics. The instrument may be defective as a result of an incorrect standardization or some type of degradation.

2/ Use of an unsuitable instrument

The absence or inadequacy of definition in the test range of characteristics for the measuring instrument to be used is often the root cause of such incidents. The instrument used is generally properly standardized but its accuracy is not always sufficient with respect to that required to ensure a measurement consistent with the criterion to be respected. In that case, it results in an error in the measurement which cannot be easily identified by the operative and varies according to the equipment to be tested. This is the case of the Chooz A incident for which the measuring instrument used was not accurate enough with respect to the equipment tested.

3/ Improper use of an instrument

In this case, the measuring or calibration instrument is properly standardized but not used properly by the worker. Incidents of this type due for most of them to a lack of training, information and experience will have the same consequences as in the previous case, apart from the fact that they will only depend on the user of the instrument. This is the case of the Dampierre 1 incident which, as one of the tanks has been designed to be common to two units, affected two units.

The main lines for improvements derived from the analysis of these incidents are as follows :

- **the questioning attitude from workers must be developed.** In particular, when the same correction is to be made systematically at least on two items of equipment, there is a significant risk of common mode due to the use of a measuring or calibration instrument and a specific analysis must be undertaken. This rule would avoid a good many of incidents. Its application would have made it possible to detect most of the anomalies set forth in this paper. This is developed in section 3.3 *Response of individuals* of the INSAG-4 IAEA Safety Report which explains that a questioning attitude together with a rigorous and prudent approach and good communication will considerably contribute to safety.

- **the national directive drawn up by EDF (DI 061) must be extended.** Indeed, although it constitutes an additional line of defense enabling the operators to better anticipate the common mode risks associated with the use of measuring instruments, it only applies to the use of a faulty instrument and does not take into account the use of an unsuitable instrument nor the improper use of an instrument which were also the root cause of common mode incidents.

- **the national directive (DI 061) must be thoroughly adopted by the sites.** The practical terms and conditions for implementation of the DI 061 directive are not indeed sufficiently formalized in the application notes of the different site units. As a matter of fact, when a national directive is drawn up, the usual procedure of the sites is to transcribe this directive in local application notes which themselves must be taken in by the workers to be able to bring about the changes required by the directive when performing their tasks and harmonize onsite practices between the different units of the site. This approach may take some time which explains that incidents occurred after the enforcement date of the national directive. Furthermore, the current management of measuring equipment does not make it possible to identify retrospectively and in an exhaustive way the equipment affected following work carried out with a faulty instrument.

- **the preventive measures against common mode risks aasociated with work carried out on redondant trains must be developed and improved, namely**

  . **maintenance work of a same nature on redundant items of equipment must be spread over time** when it is possible so as to avoid this type of defect, which constitutes an "upstream" protection system

maintenance work must be requalified in a functional way as far as possible so as to early detect this type of defect, which constitutes a "downstream" protection system.

Germany

DRAFT

German Contribution to

Task 4 of the Extended Task Force on Human Factors

(OECD/NEA/CSNI/PWG1)

"Human Factor Related Common Cause Failures"

Malfunction of the Thermal Actuation Mechanism of Fire Dampers

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Cologne, September 1994

Malfunction of the Thermal Actuation Mechanism of Fire Dampers

1 Background

The fire protection concept of modern German NPPs is based on a combination of structural, equipment-related, and administrative measures. Priority is given to the prevention of fires. This includes measures to minimize and encapsulate fire loads, and to avoid foreseeable ignition sources in the vicinity of combustible materials. An automatic fire detection system ensures the early detection of fires so that fire fighting can begin in an early stage of the fire by trained plant personnel. In areas with restricted access stationary fire suppression systems are used.

Of high importance within the fire protection concept are also measures to prevent the spreading of fires. This includes the implementation of areas separated by fire resistant structures. These measures are effective if early fire fighting is not successful. By the arrangement of redundant safety equipment in different fire zones with separated air supply it is ensured that even a developed fire affects only one redundancy. Long-term fire fighting is performed by the internal or external fire brigades.

Fire dampers in ventilation ducts are part of the structural fire protection measures. They prevent the spreading of fires through the ventilation system to other fire zones. Closing of fire dampers has to be regarded as a single measure within the fire protection concept. This concept includes also non-closing of individual fire dampers.

In German NPPs, on demand fire dampers are usually closed electrically remote-controlled, either actuated by the staff from the main control room or – in some cases – automatically by the central unit of the fire detection system. At all events described below the electrical actuation of the fire dampers worked properly. The thermal actuation by a fusible element is a diverse actuation mode, for which a high reliability is expected. It has to ensure the safe closing of fire dampers if the electrical mechanism was not actuated or failed.

It should be mentioned that structural fire protection components are not licensed and supervised by the nuclear regulatory authorities, but that authorities and testing facilities are involved which usually supervise the application of fire protection components in industrial plants and conventional buildings. Therefore the licensing process and

supervision is not equivalent to the procedure at safety systems of nuclear power plants.

2 Event Description

Malfunctions of the thermal actuation mechanism of fire dampers were detected in several German NPPs. The fire dampers have been of various designs and four manufacturers. The event analyzed here was the first one reported to the German national incident reporting system.

This first malfunction of the thermal actuation mechanism was detected during the annual inspection of fire dampers located in the ventilation system for controlled areas. During the inspection the function of the electrical remote actuation and the manual actuation were checked, and a visual inspection of the inner and outer parts of the dampers was performed.

The visual inspection revealed deficiencies at the thermal actuation mechanism of one fire damper. The lever of the thermal actuation mechanism was corroded. To prove proper function of the thermal actuation mechanism the fusible element was removed, but the damper disc did not close. The lever of the mechanism was jammed.

Subsequent evaluations showed that the bore hole of the lever was not deburred. The bearing bolt placed in this hole was too tight, so that the lever could not move. This condition lasted presumably since the initial installation of the fire damper more than 10 years ago. It seems that the function of the thermal actuation of the fire damper was not tested after the installation.

3 Systematic HF Analysis

The analysis was performed using an adopted Human Performance Evaluation System (HPES) method. At the analysis of this event by HPES some difficulties were encountered.

The sequence of the event is shown in fig. 1. The sequential tree is two-fold:

1. sequence of deficiencies in design, fabrication and installation

2. sequence of deficiencies in licensing of the fire dampers and maintenance program

Both sequences resulted in insufficient in-service inspections, which was the direct cause of the common cause failure of the fire dampers.

3.1 Deficiencies in Design, Fabrication and Installation

In the event discussed here, the screw through the lever bore hole performed as bearing bolt in the thermal actuation mechanism. For this purpose the bolt had a turned shoulder. The clearance for the lever was small (some tenth of a millimeter), if the bolt was fully screwed. This design feature did not meet the "robustness" concept which is normally applied to equipment used in NPPs. But, there was no general design requirement for robustness.

The bore hole in the lever was manufactured without being sufficiently deburred. This small thickness increase of the lever caused its jamming if the bearing bolt was completely screwed. The omission of the deburring seems to be an QA problem of the manufacturer. With respect to the long timespan since the manufacturing a detailed analysis was not possible.

During installation of the fire damper in the NPP the worker obviously fixed the bolt too tight. Whether subsequently a test of the thermal actuation had been performed, could not be evaluated due the long timespan. It may be assumed that during installation no sufficient functional test of the thermal actuation was performed. This deficiency can be assessed as a human factors problem.

During operation air-borne dirt deposited on the actuation mechanism. Additionally, slight corrosion occurred at the mechanism. Dirt and corrosion caused further motion hindrances of the thermal actuation mechanism. I.e., even if the thermal actuation had operated after the installation, these effects could have caused the jamming of the lever. Dirt deposits and corrosion were not expected in the ventilation ducts. Additionally, the damper internals have to be inspected via a handhole. Often ventilation ducts are installed at the ceiling of the rooms. Therefore, the access to the dampers is difficult. In some instances the internals can only be inspected visually using a mirror and lamp. It can be assumed that these difficult environmental conditions may have led to deficiencies or even to the omission of the checks.

3.2 Deficiencies in Licensing and Maintenance Program

Fire dampers are tested against conventional industrial standards. The most important examination is the diagnosis of the fire resistance time. Endurance tests are normally not performed, because it is not assumed that fire dampers are often closed during their life time. Therefore, the actuation mechanism is tested only about 50 times during the licensing tests. Ageing tests are not part of the examination.

The design is not explicitly evaluated whether minor tolerances in fabrication, installation or operating conditions could cause problems, i.e. "robustness" was no criterion in the examination.

An additional problem in the licensing of fire dampers resulted (and still results) from the fact that various testing facilities were involved in the licensing examination. None of these testing facilities performed a general examination of the design of the fire dampers.

The manufacturers of the fire dampers recommend yearly or half-yearly in-service inspections of the dampers. The in-service inspection should contain a visual inspection of the damper internals and a functional test of the actuation mechanisms. The German Nuclear Standards (KTA) requires yearly in-service inspections and proposed no detailed content of the inspection. There is a remark in the standard to follow the recommendations of the manufacturers. The in-service inspections were performed yearly in the NPPs, because some fire dampers are only accessible during shutdown.

The in-service inspection contained the functional test of the electrical remote and the manual actuation as well as the visual inspection of the damper internals. The thermal actuation was often not tested, resp. the fusible element was removed after the damper had closed by the diverse actuations. The movability of the thermal actuation mechanism was then checked. The evaluations performed after the events revealed that this kind of test may not detect every malfunction of the thermal actuation mechanism, because the friction conditions are different when the dampers are closed. Realistic tests with melting the fusible element using hot air have normally not been performed.

In some NPPs the in-service inspections obviously did not completely adopt the recommendations of the manufacturers regarding the content of the inspections. Three different causes may be assumed:

- safety significance:
  Fire dampers are usually closed in case of a fire by the remote electrical actuation. The thermal actuation has only back-up function. In the German incident reporting system no event has been reported that a fire damper has been closed by thermal actuation, and up to the event discussed here no malfunction of the thermal actuation mechanism had been reported. Therefore, the in-service inspection of the thermal actuation may be assessed as one of minor safety relevance.

- high reliability expected:
  The thermal actuation is a passive actuation. These actuations have normally a high reliability. The minor safety significance and the expected high reliability may have contribute to the omission of the functional test of the thermal actuation during in-service inspections.

- economical aspects:
  Detailed inspection of the internals is time consuming and in some instances difficult to perform (see chap. 3.1). The time to perform inspections of the internals is important for NPPs, because several hundred of these fire dampers are installed in each plant. Detailed inspections would cause additional work load during the refueling outage, which is normally avoided if the safety significance is assumed low.

The relevance of these three contributing factors cannot not be evaluated in detail. But, it may be assumed that these factors supported the deficiencies in the in-service inspection program.

3.3 Causal factor analysis

The HPES causal factor analysis is difficult to perform in this event, because organizational aspects are not adequately applicable. Some of the contributing factors relevant in this event are addressed to the licensing process and supervision. The root cause analysis tree is shown in fig. 2. Five different root causes resulted from the evaluation. The significance of these root causes is discussed above.

The causal factor analysis of these root causes did not reveal additional results. It is not worth to give the coding of the causes here. Recommended corrective actions are addressed in chapter 4.

4 Lessons Learned, Actions Taken

After the detection of the first malfunctions in one NPP it was recommended to check the function of the thermal actuation mechanism of fire dampers in safety relevant areas of all German NPPs and other nuclear installations.

Where failures occurred, short-term recovery actions were taken in co-operation with the manufacturers. Redesign of the affected types was recommended to eliminate the weak points and to find robust solutions. This is especially necessary as the thermal actuation mechanism is located inside the ventilation duct and therefore inspections are difficult to perform.

The procedures for in-service inspections of fire dampers will be changed. They will prescribe the check of the thermal actuation mechanism of a sufficient number of fire dampers in appropriate intervals.

5 General Conclusions

The malfunctions of fire dampers in German NPPs is a common cause failure problem. The root causes of this problems result from the complex licensing examinations, deficiencies in design and mainly deficiencies in the preventive maintenance program. Main contributors to these causes are deficiencies during fabrication and installation as well as the assumption that the thermal actuation has a minor safety significance.

These types of deficiencies may occur for any similar components, if these components have been developed for conventional applications and are only adopted for installation in nuclear facilities.

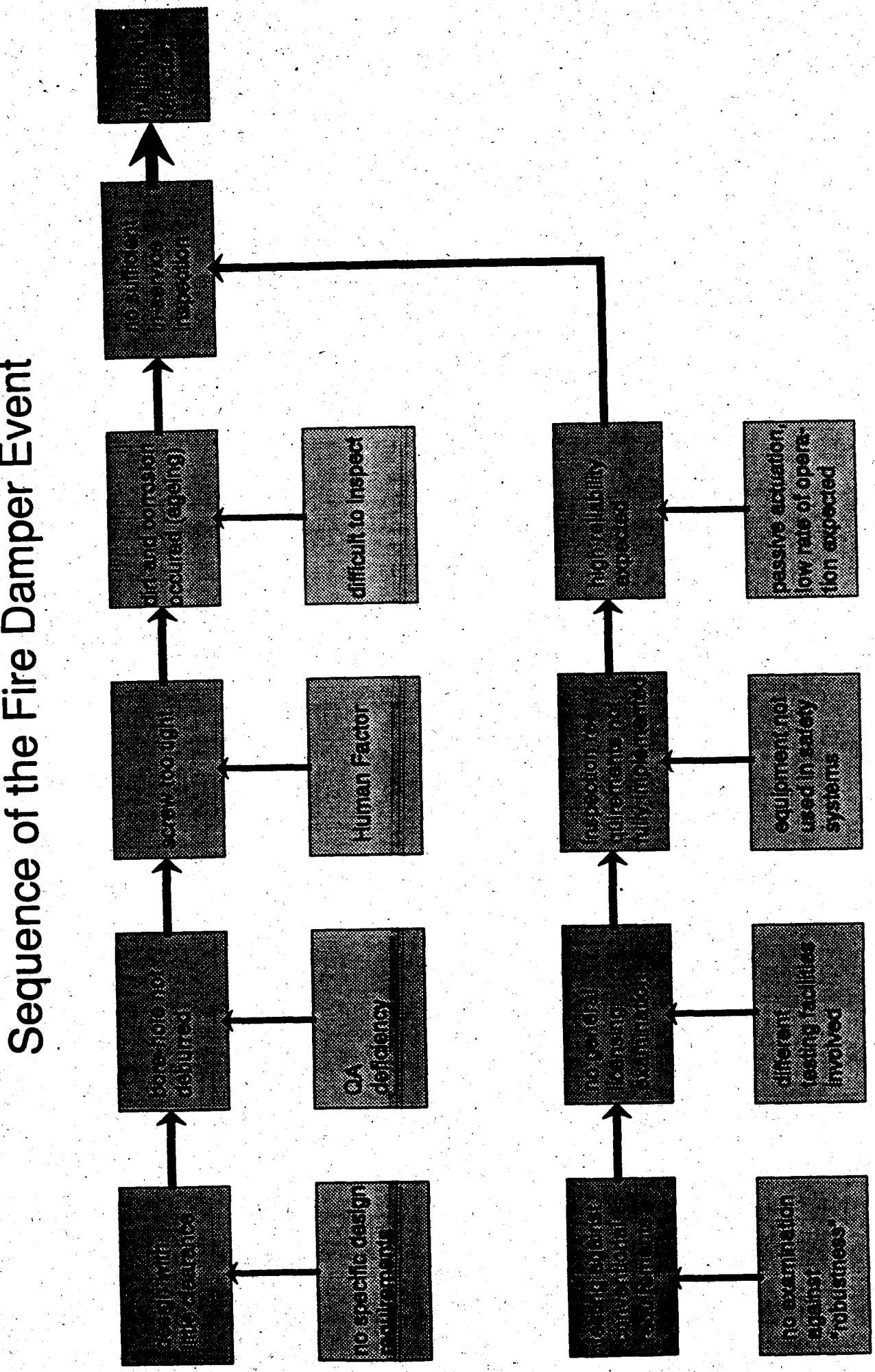


Fig. 1: Fire damper event analysis, sequence of the fire damper event

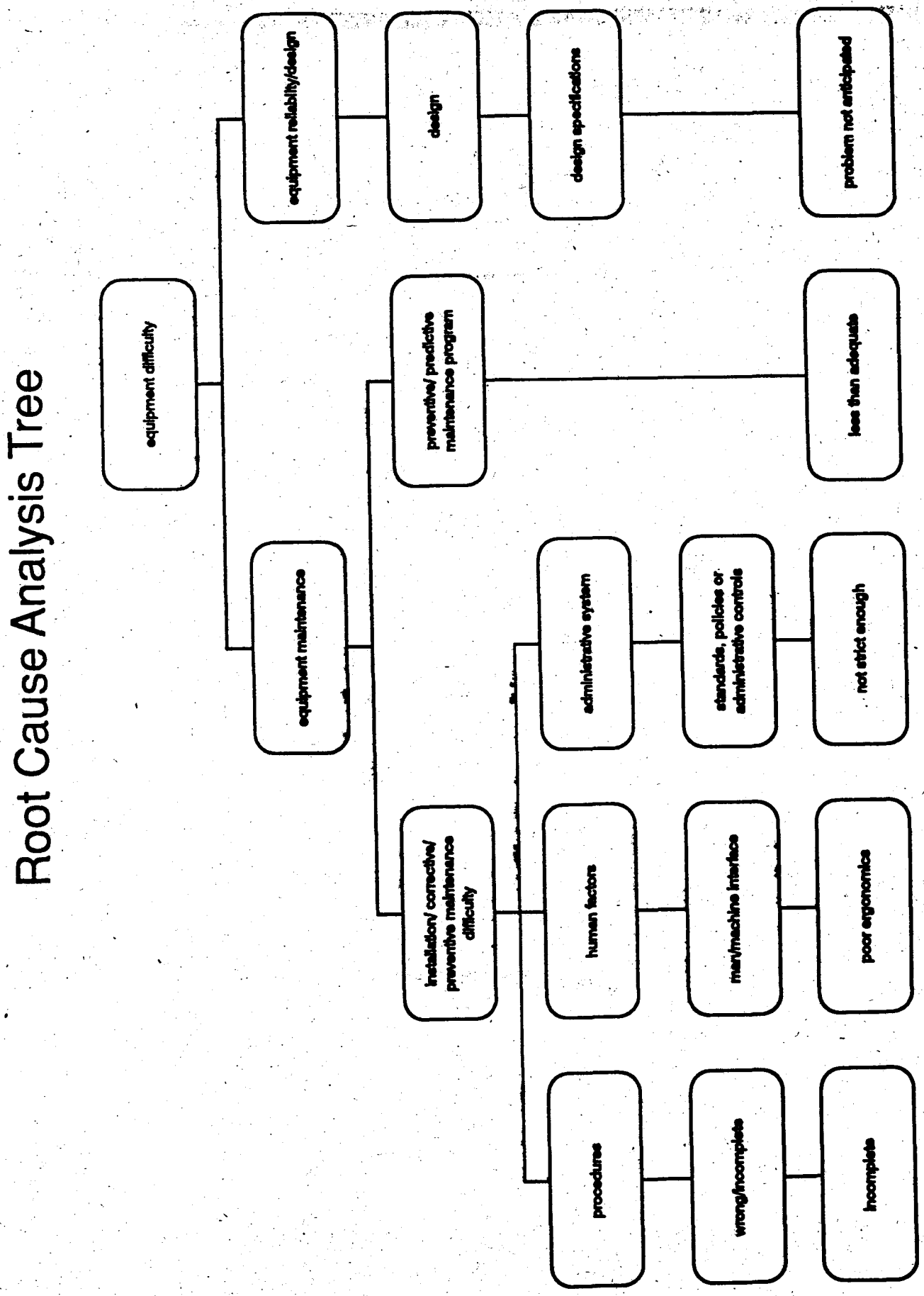


Fig. 2: Fire damper event analysis, root cause analysis tree

Italy

Italy

Even though all Italian Nuclear Power Plants are at present shut down for political reasons, the ENEL event data base was searched to identify events significant from the standpoint of human factors related common cause failures. The following events were selected.

Event n.1

While the plant was operating at full power, it was discovered that the coolant inside the radiators of one of the four emergency Diesel Generators (D.G.) was frozen. The region where the plant was located was experiencing, at that time, an unusual lengthy period of cold weather. The Diesel Generator was declared inoperable, as a result of the frozen coolant.

According to the plant Technical Specifications, the second D. G. connected to the same bus of the inoperable D.G., was tested and found to be operable. A test of the coolant of the two D.G.s, connected to the other bus, performed in the mean time, showed an insufficient concentration of the anti-freeze additive.

Anti-freeze additive was added to the D.G. coolant while keeping the generators running to improve coolant mixing.

The following day, coolant leaks were discovered from one of the D.G. radiators. The leaks were caused by cracks on the radiator.

After discovery of the damaged radiator, the plant was shut down for repairs and inspections.

As a result of a spell of unusually cold weather, the operability of all emergency D.G.s was either lost or challenged. This condition caused a plant shut down.

An investigation of the event revealed a number of problems and practices, which contributed to cause the event :

- Insufficient testing frequency of the freezing point of the D.G. coolant;
- D.G. coolant inventory made-up, in some cases, using only demineralized water, without supervision by Operations personnel;
- Lack of knowledge of some of the D.G. coolant system characteristics, such as detailed volume data, to allow calculation of the required amount of anti-freeze additive when draining and refilling the system .

Event n. 2

A few days before the event described above, the plant experienced a spurious activation of the fire prevention system installed on one of the unit transformers, which caused a turbine trip and subsequent reactor scram.

The spurious activation of the sprinkler system was caused by depressurization of the fire sensing line installed around the transformer.

The line is kept under pressure by compressed air and it is designed in such a way that in case of a transformer fire, the sensing elements on the line would break creating escape routes for the compressed air, thus causing a pressure drop in the line. The pressure drop triggers the deluge system.

The spurious line depressurization was caused by the formation of cracks in one of the drain pots installed on the line. In the severe weather condition mentioned in "Event n. 1", the water accumulated in the pot had frozen cracking the pot.

ENEL HKEH HII.NUCLEHKI Tel:0039-6-85098601 13 Set 95 6:59 No.001 P.02

Water had accumulated over time in the drain pot; drainage of the pot was not done at regular intervals and was not covered by a specific procedure.

To prevent recurrence of the event, a number of measures were taken:

- quality of the compressed air used in the sensing line was improved, using instrument air instead of service air. The plant instrument air has a very low dew point;
- The drain pots were modified with the addition of isolation valves to allow their drainage with the system in service;
- Plant procedures were modified to address draining of the drain pots in the fire prevention system.

Conclusion

These two events are interesting because show that the combination of unexpected weather conditions and inadequate plant controls and practices had the potential for disabling both internal and external sources of power.

ENEL AREA ATT.NUCLEARI Tel:0039-6-85098601 13 Set 95 6:59 No.001 P.03

Japan

OECD/NEA PWG-1, Expanded Task Force on Human Factors (ETF)

Task 4: Human Factors Related to Common Cause Failures

September 1994

Institute of Human Factors
NUPEC, Tokyo, Japan

Failure of Operation of Pressurizer Relief Valves during the Steam Generator Tube Break at Mihama Unit No. 2 of the Kansai Electric Power Company, Inc.

1. Chronology of the Events

February 9, 1991

Around 12.40 hrs. : An operator discovered that the record given by the steam generator blow-down water monitor (to be termed "R-19" hereafter), by which the leakage of the reactor coolant to the secondary side is monitored, was increasing slightly. Instruction was given to analyze the radioactivity concentration by collecting a sample.

Around 13.45 hrs. : The alarm of R-19 was sounded.

Around 13.47 hrs. : Operation was started to reduce the generator output with the intention of shutting down the reactor.

13.50 hrs. : The reactor trip signal was activated, and the reactor and the turbine were automatically shut down in accordance with normal sequence. And then, the safety injection signal was activated, and the injection of water into the reactor coolant system was started automatically.

Around 14.02 hrs. : Since the complete closure of the main steam isolation valve of A-steam generator could not be confirmed, the operator tightened the said valve manually.

14.02 hrs. to 14.17 hrs. : The main steam relief valve of B-steam generator was opened to cool the reactor coolant system.

Around 14. 10 hrs. to around 14. 25 hrs. : It turned out that the two pressurizer relief valves, which are used to reduce the reactor coolant system pressure, failed to open.

14. 34hrs. : Operation was started to reduce the reactor coolant system pressure using a pressurizer auxiliary spray.

14. 37hrs. : Two high pressure injection pumps were stopped after confirmation that the pressurizer water level had been recovered.

14. 48hrs. : The reactor coolant system pressure and the pressure of the secondary side of the damaged steam generator became almost equal, and the leakage of reactor coolant into the secondary side stopped.

2. Investigations

* An operator assumed that the air supply valve in the air junction box was not commonly used as an air supply valve for the air system to operate the pressurizer relief valves, and, assuming that it was a valve supplying an auxiliary air system, he closed the valve in question based on the assumption that it is not normally used.

The closure of this air supply valve was overlooked in the checking process of the inspection record. Therefore, the operating air was not supplied to the pressurizer relief valves, and the two pressurizer relief valves did not operate.

* It is evaluated that the operators responded appropriately to this incident, and safely led the incident to subsidence, despite the occurrence of such event as the in-operativeness of the pressurizer relief valves.

* The operations manual did not contain instructions for operating procedures in the event of malfunction of equipment such as the in-operativeness of the pressurizer relief valve. Also some instructions for the timing, sequence, conditions, etc. of equipment operation were not explicit.

3. Countermeasure to Prevent a Recurrence and Lessons

(1) Improvement and Intensification of Periodical Inspection

* The inspection of major equipment, including the pressurizer relief valve, shall be intensified.

(2) Improvement of Maintenance and Management System

* Concerning the instrumentation air supply system for equipment with important safety functions such as the pressurizer relief valve, considerations shall be provided to prevent misoperation.

* Measures for prevention of misoperation, such as locking management, shall be thoroughly provided to manually operated valves which are related to the operation of equipment with important safety functions.

* In addition, it is desirable to eliminate, as much as possible, the factors which could be the cause of simultaneous failure in designing equipment which have important safety functions.

(3) Improvement of Operations Manual

* The adaptable operations which are required in the case of an anomaly in equipment with important safety functions, such as failure of the pressurizer relief valve to operate shall be specifically detailed in the operations manual.

Republic of Korea

Korean Contribution to

Task 4 of the Extended Task Force on Human Factors

(OECD/NEA/CSNI/PWG1)

"Human Factor Related Common Cause Failures"

Topic: RHR Pump Failures during Mid-loop Operation

Young Choi, T. W. Kim, Chang K. Park

Integrated Nuclear Safety Assessment

Korea Atomic Energy Research Institute

Taejon, Korea

Abstract

An analysis has been performed for two incidents of the loss of residual heat removal (RHR) which Korean nuclear power plants have experienced. These incidents occurred on June 1, 1984, at Kori Unit 2 and on October 8, 1987 at Kori Unit 3. These two incidents are identified as the human factor related common cause failures in point of view of root cause. This analysis describes human related CCFs in RHR system during mid-loop operation. Also, even though loss of RHR occurred, the operator corrective actions during the incidents would be judged as reasonable and put successfully the situation under control. The results derived from the incident analysis and evaluation have been incorporated into the useful applications such as the development of operating procedures for nuclear power plants.

1. Introduction

The residual heat removal system is designed to remove residual and decay heat from the reactor core and to reduce and maintain the temperature of the reactor coolant system during plant cooldown and during refueling operation.

Pressurized water reactors (PWRs) have experienced numerous loss of RHR events worldwide. Events involving loss of residual heat removal capability are often initiated or exacerbated by adverse plant conditions and by concurrent maintenance activities. Fortunately, during the events that have occurred, RHR was restored without core damage, although, in some cases, the RCS water reached the saturation temperature. Thus, The loss RHR during the plant shutdown could lead to a serious consequence. Upon reviewing the loss of RHR incidents, it is generally agreed that there are human related CCFs under the Mid-loop operation (partially filled RCS operating condition).

Korean nuclear power plants have experienced two incidents of the loss of residual heat removal. One was initiated by residual heat removal pump trip due to a spurious low signal in the refueling water storage tank. The other was initiated by a suction pressure loss for residual heat removal pump resulted from a delayed water level indication. The operator was able to revive the system by utilizing the water from the refueling water storage tank. In case of the loss of RHR during the partially filled RCS operation, the necessary corrective actions must be taken at least prior to

the core uncovery due to coolant evaporation. For these two incidents, post-incident safety analyses confirmed that no core uncovery has occurred during the incidents. Possible preventive and corrective measures against the loss of residual heat removal system are now implemented in Korean nuclear power plants through the system reinforcement, operating procedure development, and operator training.

2. Event Description

Kori Unit 2 Incident

On June 1, 1984, at Kori Unit 2, having two loop systems with the thermal output of 587 MWe, RHR pump 2 was in operation prior to the fuel reloading. The reactor vessel water level was being maintained at 2 cm above the center line of the hot legs. While the refueling water storage tank (RWST) water level channel was under the maintenance, a 'Lo-Lo' level signal was caused. The following is the sequence of the incidents and the list of operator action taken:

11:44	A RWST spurious 'Lo-Lo' level signal occurred .
11:45	Valves 8810 and 8811(RHR pump to CV sump) opened automatically. The RHR pump 2 resulted in the apparent loss of suction pressure and flow.
11:46	RHR pump was manually stopped. Then valves 8810 and 8811 were manually closed. Valves 8701 and 8702 (hot leg to RHR pump) were manually closed.
11:52	Temperature of hot leg loop 1 reached 95°C. The 'Lo-Lo' signal at RWST was eliminated. The observed water level was 12 cm below the hot leg center line.
11:55	RHR pump 2 was tried to restart, but stopped immediately due to the insufficient suction pressure. Suction line vent was started.
11:58	RHR pump 2 was retried but failed.
12:00	RHR pump 1 was tried to startup, but failed due to an insufficient suction pressure.

12:05	Evacuation from containment vessel (CV) was ordered and health physicists were notified.
12:10	Operators tried to fill RCS by pumping water from RWST through charging pumps, but a sensible quantity of flow was not formed.
12:15	Volume control tank level was reduced by 10 %. The charging pumps were stopped due to hunting.
12:20	Operators lined up the recycled holdup tank to send water to RCS. Valve 8310 (from the boron recycle system evaporator (BRS) feed pump to charging pump suction) was opened. Charging pump 1 was started.
12:23	Since the emergency boration line was under maintenance, normal boration through the blender was performed. The RCS level was raised.
12:35	Valve 8812 was opened and RHR pump 2 was started. RCS temperature was reduced to 35°C. Charging pump was stopped.
12:37	RHR pump 2 was stopped and then the normal cooling mode was lined up with valve 8812 closed and valves 8701 and 8702 opened. RHR pump 2 was started.

Kori Unit 3 Incident

The RHR loss incident at Kori Unit 3, 3-loop, 950 MWe, occurred on October 8, 1987. The incident was caused by a delayed response of Tygon hose level indication during draindown operation , and is briefly summarized as follows.

09:00	Head Bolt detention began.
13:20	The RCS level was being maintained at 116'-5", when the water level reduced to an indicated level of 116'-3" by sending water to the RWST via valve 005A in preparation for installation of the steam generator nozzle dam.

14:00	The RHR heat exchanger bypass alarms set off due to a low flow rate, then the RHR pump recirculation valve 602A opened automatically. At this stage the operators closed valve 603A to maintain water flow to the RHR pump by establishing the recirculation flow sufficiently. The RHR pump A flow was recovered temporarily when valve 602A closed. Then the valve 603A reopening was tried.
14:02	The RHR pump was stopped due to severe fluctuation in flow and discharge pressure.
14:20	The RHR pump B was started at an indicated RCS level of 116'-10".
14:22	The RHR pump B was stopped due to hunting in the discharge pressure and flow indication. In the meanwhile, the actual RCS level was ascertained in the hot leg side of the steam generator to be lower than the indicated level by the Tygon hose stand pipe.
14:35	The RHR pump A was started to add water into the RCS with suction from the RHR.
14:40	RHR into the normal operating condition.

In these two incidents, the peak RCS temperature recorded was 95°C and did lead to no core uncovery.

3. Event Analysis

The CCF event analysis begins with dependency analysis. The dependencies of functional, physical, and human interactions are identified as explicitly as possible in view of the information available. Therefore maintenance/ calibration for RWST level transmitter must be reviewed in terms of dependency. Also RHR pumps should be considered as a viewpoint of RCS air vent and level control to continuous run.

In RHR event analysis, redundant components such as RHR pumps, RHR related valves, sensors, flow elements, electric power supplies are known to be susceptible to CCFs and important for the plant safety. The low level of RCS hot leg

might induce the loss of RHR. The human actions may cause some errors such as a failure to restore the equipment following testing and maintenance tasks and those errors in manipulating the equipment in response to an accident situation.

Kori Unit 2 Incident

For the case of Kori Unit 2, a spurious signal of low low level at RWST occurred to induce common cause failure which resulted in opening of sump valves. The recirculation mode of RHR operation is automatically initiated by the recirculation actuation signal (RWST low-low level). This signal secures the RHR pump, opens the containment sump isolation valves and closes RWST isolation valves. The RWST low-low level signal is generated when trip signals occur in two out of four channels. This event is induced by maintenance related human error during the calibration of RWST level sensor. Therefore, this event is considered to be one of the important human factors related CCFs. Basically this event came from the discrepancy between status of local control panel and that of schematic diagram. This discrepancy might be made under the last test / maintenance or construction. This event occurred during the first outage since commercial operation began. Before commercial operation, a lot of commissioning tests must be completed. The commissioning tests consist of many human related activities. Even though a few people are involved in a test at the same time, the mistakes could happen due to complicated job environment. Since the opening of sump valves resulted in the loss of RHR pump suction pressure and flow, RHR pump failed. However in this event operator didn't find out the cause of RHR pump failure and tried to start standby pump. As a result, both RHR pumps failed as type of CCF which came from loss of pump suction pressure or loss of suction flow. Therefore, if a RHR pump fails, the causes of pump failure must be identified before standby pump is started. The maintenance work are associated with maintenance group and operation group so that these two groups need good communication each other to succeed the maintenance activities. If operator could conceives the test status in this event, he easily could understand the mechanism of component failures. Then,

operator can take the corrective actions within limited time, for example, the make up of RCS using charging from RWST.

Also at least, maintenance team must examine the possibility of test-induced safety system failure. Whenever system or component comes to failure, maintenance team have to let operators know the status of event as soon as possible. Before maintenance activities are performed, the maintenance related document and drawing must be examined in detail especially for safety system. At this time, maintenance team must have a communication with operators to reduce the possibility of system failures which comes from system interface.

Kori Unit 3 Incident

For the case of Kori Unit 3, actual low water level in RCS occurred to induce common cause failure which resulted in failures of RHR pumps. It should be well recognized by the operators that the actual water level might be different from that of Tygon hose or the indication on the gauge under the current level indication system. the indicated water level by the Tygon hose may be higher than the actual due to the possible air entrainment in the lower part of the connection. The level difference may be substantial if the reactor vessel is pressurized without a vent path. Therefore, regardless of the indicated water level, if any signs of RHR loss appear, the operators should respond promptly in order to protect the RHR system and to maintain the plant in a safe condition.

Once a RHR loss is likely to have occurred, the operator should immediately stop the RHR pump to avoid any damage to the pump. Before restarting RHR pump for core cooling, the RCS water level must be maintained as required and the pump be vented when necessary. When needed, the RCS water level can be increased by several different ways. If the RCS is not under pressure, the water can be sent to the RCS from the RWST by gravity or by the safety injection charging pumps. Water can also be supplied from the primary makeup water storage tank. If the RHR system

cannot be restored in a permissible time period, some additional actions are required. For example, use of the secondary loop of steam generator as heat sink could be considered to mitigate the pressure increase in the reactor coolant system. In addition, containment closure and personnel evacuation procedure must be prepared as necessary. If the steam generators are not available for decay heat cooling, feed-and-spill type operation can be considered to avoid the RCS water boiling.

4. Conclusion and Recommendation

There are two major causes in loss of RHR incidents occurred in Korean nuclear power plants. One is the discrepancy between status of local control panel and that of schematic diagram for the case of Kori Unit 2, while the other is post-event human error from the misunderstanding of the system behavior in the consequential scenario for both cases of the Kori Unit 2 and 3. That is, after these events occur, the operator has to ensure that the NPSH is enough to restart RHR pump and that air bounding does not exist in these RHR loops. Therefore, these events give a kind of lesson for plant personnels to reduce CCF as the following.

- The communication between the maintenance and operation groups must be well established to prevent CCF to practice maintenance activities for safety related importance system such as a RHR system.

- Whenever there are maintenance activities or testing activities for RHR related components such as valves, these activities must be performed after enough reviewing system configuration.

- To restart RHR pump, it is necessary to acquire NPSH, air bounding and air venting in RHR related system. To get these objectives, developing a procedure is necessary to restart RHR pump .

- If RHR capability is not recovered within the required hours after event happens, boiling could occur in RCS loop. Thus, make-up of RCS is required essentially to preserve the integrity of RCS system and fuel.

- It is useful to establish monitoring system in order to suggest success path for make-up water in RCS during outage.

These events are barely mitigated by operator recovery actions with charging pump and boration system, but there are many defects in these recovery actions. Therefore, possible preventive and corrective measures against the loss of residual heat removal system could be implemented in nuclear power plants through the system reinforcement, operating procedure development, and operator training.

REFERENCES

[1] S.W. KIM, et al, "Study on the Loss of Residual Heat Removal While the Reactor Coolant System is Partially Filled", KINS/AR-207,KINS,1992

[2] H.C.KIM, S.W. Kim, et al, "Safety Analysis of Loss of Residual Heat Removal System Under Coditions of Partially filled Reactor Coolant System", IAEA-SR-169, IAEA, 1990

[3] Abnormal Operating Procedure for Loss of RHR System (in Korean), AOP 2-2-316, Rev. 1, Kori Unit 2, Korea Electric Power Corporation(1989).

[4] CHOI, Y.and T.W. Kim, "Operator Recovery Guidance for Loss of Offsite Power Events During Mid-loop Operation Using Success Path Sets", IAEA-J4-TC-606.4, IAEA,1994

Federation of Russia

OECD NUCLEAR ENERGY AGENCY

ROLE OF PERSONNEL IN THE OPERATION PROCESS

VNIIAES RUSSIA

V.KOROTKOV

1995

1. Role of Personnel in the Operation Process 3
1.1. Nature of Causes of Personnel Errors 3
1.2. Personnel Actions During Normal Operation and in Emergencies (abnormal regimes) 5
1.3. Staffing, Assigning and Training of Personnel. 8
1.4. Personnel Performance Indicators 10
1.5. The Role of NPP Technical Support Centres 11
1.6. Proposals for Improving the Methods of Working with Personnel 13

1. ROLE OF PERSONNEL IN THE OPERATION PROCESS

1.1. Nature of Causes of Personnel Errors

1.1.1. Characteristic of NPP personnel errors depends on specific features of the process. Peculiar properties of NPP personnel errors are defined by influence of process system as a whole and of its elements on the safety of NPP workers, population and environment and also on reliability and stability of major equipment functioning.

Various specialists participate directly or indirectly in generating electric power and heat at nuclear power plants. As a rule NPPs located in densely populated industrial areas are considered as potenttial sources of radioactive contamination both of nearby and significantly distant areas due to nuclear physical peculiarities of the nuclear reactor.

NPP staff is to meet high requirements because reactor or turbine operator errors can be the cause of unforeseen consequences as well as errors made by instrumentation technician attending the monitoring hardware operation; and driver of autocrane whose error may cause short circuit in electrical system and mechanic's error in assembling important component can lead to an accident.

The main problem is that major process facilities being potentially dangerous are not reliably protected against human error and this was proved by many years of NPP operation. So sometimes the operator is forced to interfere in the control process practically immediately after a signal of a deviation appears and operator's incorrect actions can't be inhibited by automatics or controls. As shown by the practice, the largest number of errors made by NPP personnel occurrs during the initial phase of unit operation especially if this is the first unit of the NPP.

The reasons of it are lack of experience in a joint staff operation, lack of "hands-on" experience for a majority of specialists, imperfection of Standards and Codes wich are often developed and issued by operating staff (documents

regulating performance of activities: operating instructions, operating diagrams, regimes maps and other organization and instructing materials). There are also impacts from errors in staff recruitment and allocation.

The number of personnel errors in the total amount of occurrences and failures is reduced as the unit goes into its 3-rd or 4-th year of operation and as a rule it is stabilized at a level of several percent per year.

Sometimes, one can see "peaks" on the error curve after rather a long period of smooth operation.They are explained by unjustified overestimation by personnel of his experience and capabilities, by degraded monitoring and inadequate practical measures taken by management and engineering support services.

1.1.2. Causes leading to erroneous actions of personnel can be broken down into the following main groups:

Causes not depending on the worker making an error:

- lack of sufficient experience if unexpected situation occurs and lack of possibility to get advice;
- inadequacy of specialist's training to meet the functional requirements of his job, and, as a consequence, weaknesses in the training system provided by the administrative & engineering management;
- lack of or poor quality of organizational-technical measures to eliminate deviations and faults;
- limits of psycho-physiological capabilities of the human organism.

The causes which depend on the worker are the following:

- intentional violations of Codes & Standards aiming to speed up or facilitate the solution of the existing problem, to avoid the predicted consequences (e.g., reactor "overpoisoning");
- unintentional deviations from the requirements of instructions and specifications due to distraction of attention by parallel events, poor coordination of related services' interface, and also due to the worker's psycho-physiological condition which may be the result of the problems of psychological atmosphere in the team, social and living conditions.

There is a number of causes based on the human factor effects. These are connected with problems in providing the operator with the technical support from the corresponding engineering services: inaccuracies in the operating documents (diagrams, cards, schematics, tables etc.), irrational and inconvenient presentation of information.

1.2. Actions During Normal Operation and in Emergencies

1.2.1. The structure of organizing the operations activity at NPPs is based on the "single management" principle. The management of unit operations is performed by the Unit Shift Supervisor. His direct subordinates are those specialists who directly ensure equipment/system functioning and the conduct of technological regimes. Engineering support for operating personnel is provided by NPP Services.

In normal operation, when the unit is operating at steady state or while performing the routine operations of power raising/reduction the main tasks of shift personnel are to monitor the parameters of the working media, of equipment, to perform equipment and system changeovers/realignments in accordance with the procedures and instructions.

In case of deviations from normal operation the Shift Supervisor has a possibility to involve any specialists he needs who also become his direct subordinates and perform their functions on his instructions according to guidelines and procedures existing at the plant.

In case of an emergency the Shift Supervisor notifies NPP management and takes measures to eliminate the emergency. Appropriate emergency operating procedures are activated.

Personnel, especially operating personnel, during abnormal/unusual events, accidents, natural phenomena (earthquakes, floods, tornadoes, fires etc.) has to strictly perform his functions and comply with manager's instructions. It is in such periods of stress situations that conditions may originate provoking unreasonable decisions; errors are made which become obvious while being addressed in calm condition. To provide analytical and advisory assistance at the NPP in case of emergency, the engineering support group is expected

to arrive at the plant. Its task is to perform comprehensive analysis of the event, to carry out necessary calculations, to recommend installation of additional means for collection and processing of information, to develop proposals to eliminate abnormal situation accident and to develop technical assignments (terms of reference) to develop specific means and methods for implementing these proposals.

To reduce the negative effect of human factor it's necessary to perform thorough training, select the staff with account for business and personal qualities of specialists, to assure optimal distribution of the staff in their work places avoiding overloading by functional duties, to create convenient conditions for work and interactions with each other. The next compulsory condition is to organize permanent training of operating personnel, of engineering support groups, of managers responsible for work conduct.

1.2.2. Analysis of operations personnel errors allows to conclude that most of errors are made due to lack of reliable system of specialists selection and training taking into account their psycho-physiological capabilities, psychic and spiritual qualities of a person.

Poor discipline leads to violation of regulations, Standards and other documents requirements and as a consequence results in failures in equipment operation, in incorrect system functioning, aggravation of transients. This may have a negative effect on specialist's performance at any work place. A mechanic became the cause of unit shutdown because he didn't tighten an RCP bolt according to the requirements of the instructions, failed to lock the bolt and the bolt later got into the core causing degraded functioning of control rod system.

Lack of discipline and responsibility are the most frequent causes of failures due to errors of operating staff attending auxiliary systems and working in maintenance service.

Selection and training of specialists for responsible posts to control reactor and turbine or major plant equipment are more stringent. Therefore errors for this category of

staff are rather due to psycho-physiological capabilities of a person, to level of knowleadge, technical training and working process organization. For example, because the turbine operator in the control room did not hear the command from the reactor operator and instead of partial reduction of turbine load performed turbine shutdown an abnormal situation followed involving unit shutdown. If an operator observes a sound or light alarm going off on the control panel he naturally experiences a nervous stress. The severity of an abnormal regime or probability of avoiding it will depend on operator's ability to cope with this nervous stress, to remain calm with a clear mind, on his ability to promptly obtain the needed information, to analyse the situation and correctly fulfil the required commands with the needed sequence.

To facilitate personnel actions during an accident, to make them precise and consistent sets of symptom-based emergency operator actions are being introduced at present. Such a set includes the background Codes & Standards documentation which regulates operating personnel actions while assessing an abnormal situation, the employed monitoring hardware/instrumentation, actions to restore the normal regime and preclude event progression.

These background regulatory documents include the following basic materials:

- rules for document structure, content and presentation;
- requirements to personnel who is to perform the symptom-based actions;
- requirements to software means for calculating transients and to the content of computational analysis used to justify operator actions;
- guidelines for the monitoring of critical functions' status;
- symptom-based actions set's User Manual.

Incorporation of the symptom-based actions set into the plant operations management system will make it possible to significantly reduce the probability of personnel errors. A significant point here is that the operator performs the actions prescribed by the path which was assessed and

calculated in a quiet atmosphere without time shortage by a group of competent experts. The operator only has to precisely comply with all the procedure instructions and maintain good interaction with his colleagues.

1.3. Staffing, Assigning and Training of Personnel

Managers of corresponding structural divisions recruit specialists for job positions. Training and further education are conducted mainly at the plant and in the plant Training Point which exists or is being established at each NPP. Specialists for jobs with higher responsibility are selected from those who have practical experience with auxiliary systems. Plant Service management sends the selected candidates to be trained in a specialized Training Centre where specialists are retrained for the specific post during several months according to validated methodologies and established programs using sophisticated computer complexes and simulators. After successful completion of training the specialist has to take on-the-job training under the guidance of the division manager.

Training Points and Centres are equipped with full-scope simulators intended to teach operators how to control the unit and obtain the necessary skills.

A set of technical means including unit control board, measuring hardware, alarms and computers ensures immitation of simulator operation regimes in real time.

The aim of personnel training at Training Points and Training Centres is the following:

- maintaining high professional level of NPP staff;
- systematic improvement of NPP managers, specialists and workers proficiency;
- training, retraining, organization of training course to train workers for related skills.

Specialists to work in operating services are selected by testing method and taking into account the analysis of previous activity of the candidate in three main areas:

- psych-physiological capabilities;
- psychic and spiritual qualities;

- extent of engineering-technical proficiency to master the new level of knowledge and functional peculiarities.

Psycho-phisiological factors are evaluated considering range of natural capabilities and state of physical health, deviations are detected and degree of their non-conformance to professional requirements is defined. Especially important conditions are:

- memory status and possibilities;
- quality of vision, hearing, speech;
- lack of medical contraindications relating to cardio-vascular, gastric intestinal, nervous-psychological and other deseases.

The quickness of situation assessment and of decision taking to a great extent depends on the amount of information kept in operator's memory. Reduced colour visual sensation (loss of spectacles in critical moment) deafness, inaudible speech may be the cause of delays or incorrect information perception.

Psychic and spiritual qualities of a person are connected with his upbringing. One can name the following main features here:

- coolness, i.e. ability to keep oneself calm and have clear thinking in case of unforeseen circumstances;
- discipline and ability to control one's actions;
- ability to concentrate to solve tasks that arise;
- quick response to the changing situation;
- a sense of duty and high responsibility.

Undoubtendly, these human qualities are closely connected with the natural capabilities of a person.

Scope of knowledge, of engineering education, i.e. the level of technical preparedness to absorb complex and versatile processes and later to control them significantly influence the time and quality of operating personnel training.

Given an approach to the control of complex technical features where the main load in solving problems especially at the initial stage of their origin is to be carried by operating personnel, all those aspects are of importance especially in nuclear power industry where technological processes are very fast.

1.4. Personnel Performance Indicators

As noted above, while assessing the current status of operational safety we analyse the activity of operations personnel both with the unit on power and in maintenance.

An indicator of personnel erroneous actions is calculated to obtain quantitative assessment of personnel technical proficiency at unit normal operation mode and in emergency. Indicator of maintenance quality is calculated while carrying out maintenance. Both indicators are calculated in a quarterly and integral form according to the formula where the numerator is the total number of unit operational events due to human error and the denominator is the number of hours of unit operation for the reviewed period. To provide convenience in calculation the obtained relationship is adjusted to 1000 hours.

This indicator is defined as an average arithmetic value in the industry. It is also calculated for NPPs equipped with a certain reactor type.

Analysis of actual causes of personnel unavailability indicator changes demonstrates that the typical deficiencies common for all NPP types are the following:

- violation of procedure requirements;
- lack of necessary monitoring of actions;
- negligence in performance of operations;
- insufficient level of specialists training;
- poor organization of work places;
- lack of complete sets of working and operations documents;
- poor quality of the documents.

Annual reports contain separate chapter where maintenance status of safety-related systems is analysed, violations caused by failures in operation of services providing and performing these functions are considered.

The above mentioned chapter systematizes information obtained from NPPs in the form of accident investigation reports, protocols, technical decisions and other materials;

summarizes the data; shows the trends; characteristic causes are identified and suggestions to eliminate failures are formulated.

Main reasons of violations for NPPs of all types being made in maintenance are similar and explained by the same factor: attitude of a person to performing his functional duties:

- violation of technological discipline while preparing and performing work;
- inadequate checking of equipment status after preventive maintenance, recovery and mounting;
- errors made by managers of production and functional NPP servies;
- insufficient knowledge of the attended equipment status and of its peculiarities;
- lack of optimization in the organization of materials and components supplies (tooling, equipment, devices, mechanization means, spare parts, materials).

1.5. Role of NPP Technical Support Centres

In spite of the satisfactory situation regarding operating personnel training system at all stages from initial training to maintaining high preparedness to perform functional duties in working places the system is constantly being improved in order to create conditions allowing to reduce probability of human factor negative effect on NPP safety, to enhance stability and reliability of plant's most important systems and equipment operation. One way to solve this problem is described in the concept of the "Scientific technical support for NPP safe operations and NPP Technical support centre" developed by joint efforts of VNIIAES and Russian-American firm "JET-T" based on experience of countries with advanced nuclear power such as USA, France, England, Sweden. Two main activity areas are addressed in the concept:

- system for the management of NPP emergencies;
- operation system.

Both systems belong to a range of general problems, main of which are the following:

- development of specilized structures able to provide prompt mobilization of experts, of interested organizations capable, if necessary, to take control and management function to solve the problems facing NPPs in crisis situations:

- development and upgrading of information systems on NPP and nuclear industry level used to collect, accumulate, process and submit data on technical status of a nuclear unit;

- creation of efficient systems for providing operating communication between NPP and specialized structures to ensure identification and mobilization of necessary means and resources, coordination of activities of those who take part in implementing corrective measures;

- development of a set of Standards & Codes, instructions, methodologies, regulations etc. and also the models of technological and emergency processes;

- installation of modern computers to the extent sufficient to solve tasks of corresponding level;

- adoption at a governmental level of a soundly funded Program for the development of NPP safe and effective operation system.

Structurally the scientific-technical support is organized at three levels:

- industry level;
- level of organizations involved in the support effort;
- NPP and NPP Service level.

At each level they prepare the materials to assure the solving of tasks of this level within the competence of its elements and aimed at resolving the general problem.

The technological element of the scientific-technical support is determined by specific features of nuclear electricity generation and by the most important processes from the viewpoint of safety and is maintained in such areas as:

- neutron physics;
- dynamics and technological regimes;
- performance of structural metals and of materials;
- water chemistry control and technology;
- radiation safety;

- summary of operational experience and analysis of NPP operational events;

- reliability of equipment and of safety-related systems;

- maintenance and repair;

- regulatory documentation, assessment and review of the design;

- automatic control system (ASU-Rus. abbr.) and software;

- optimization of organizational-technical and management structures.

Main types of technical support for NPP safety are implemented by the industry centre through the Local Crisis Centres of NPPs. These LCCs are to perform their functions at NPP level as a structural division of an emergency management system. All NPP operation modes are covered:

- commissioning of the unit;

- normal operation according to established Standards;

- operation in cases of breach of normal functioning;

- operation in design-basis and beyond-design-based accidents;

- decommissioning of the unit.

Main task of the Centre is to prevent NPP operational events and to ensure efficient assistance to cope with the accident.

1.6. Proposals for Improving the Methods of Working with Personnel

To improve the organization of work with personnel the following is necessary:

- while developing process control systems for new NPPs one should foresee such mode of their operation where participation of operator is to be excluded at least during the first 30-40 minutes of unauthorized event. Operator's duty is only to ensure supervision of automatic systems proper functioning. Engineering support group is to analyse events and prepare decisions relating to further actions of operator in case of unpredictable progression of situation and absence of unambiguous instructions in the symptom-based actions procedures;

- implement the concept of NPP safety scientific-technical support and introduce a system of crisis situation management in the "Technical Support Centre";

- improve the system of operations personnel training on the basis of modern computer means, software and methodologies;

- introduce a complex of symptom-based actions for technological safety-related systems at all NPP types;

- develop a program for establishing a base of Standards and guidelines for recruiting and assigning specialists to the jobs taking into account their individual features on the basis of modern scientifically substantiated methods.

Slovenia

OECD / NUCLEAR ENERGY AGENCY

Principal Working Group 1, Expanded Task Force
on Human Factors

Participating Country: SLOVENIA

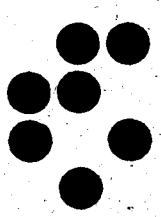
Task Title: Human Factors Related to Common Cause Failures

Marija Molan Škof*, Ljubo Fabjan

Ljubljana, September 1994

University of Ljubljana
"Jožef Stefan" Institute, Ljubljana, Slovenija

in collaboration with:
**University Medical Centre, Ljubljana, Slovenija*



1. INTRODUCTION

Thank you very much for invitation to new "Expanded Task Force" (ETF) task which will deal with the "Human Factors Related to Common Cause Failures".

The stated task is actually for our plant, too. We recognised that large majority of unusual events may be a results of human inefficiency. According to our results, about 80% of analyzed events were the consequences of human mistakes. Further investigations and analyses of human role in the events situation is so desirable also for us. Our results could be use as the base for appropriate investigation of human reliability and availability.

On the results of these analyses improvement in organisation and new investment in human part of the system will be possible. With relative low cost investment a significant improvement could be achieve, if we invest in the improvement of human behavioral.

The purpose of this paper is to present our preliminary view on work of subgroup which will be oriented to the event analysis and to present our experiences with analysis of human factors.

2. BACKGROUND

Data collection of unusual events has been done at Krško NPP during operational period since 1981. Events has been mostly related to post outage tests and surveillance activities. The events has been uniformly distributed during NPP Krško twelfth years operation.

Some of the events has been reported in accordance to IAEA Incident Reporting System recommendations, the remaining events has been reported only briefly since they causes some evaluation problems. This problem were typical for the events which occurred at the very beginning of the operation.

3. METHODOLOGY FOR EVENT EVALUATION PROCESS

Regarding to nature of the events, the evaluation process should focus on people involved in:

* main control room activities,
* maintenance activities,
* test activities, and
* surveillance activities.

Figure 1 presents the general inputs and outputs of the evaluation process in the block diagram form. The diagram shows two major functions in the evaluation process. The first is the problem definition, and the second is the diagnostic function.

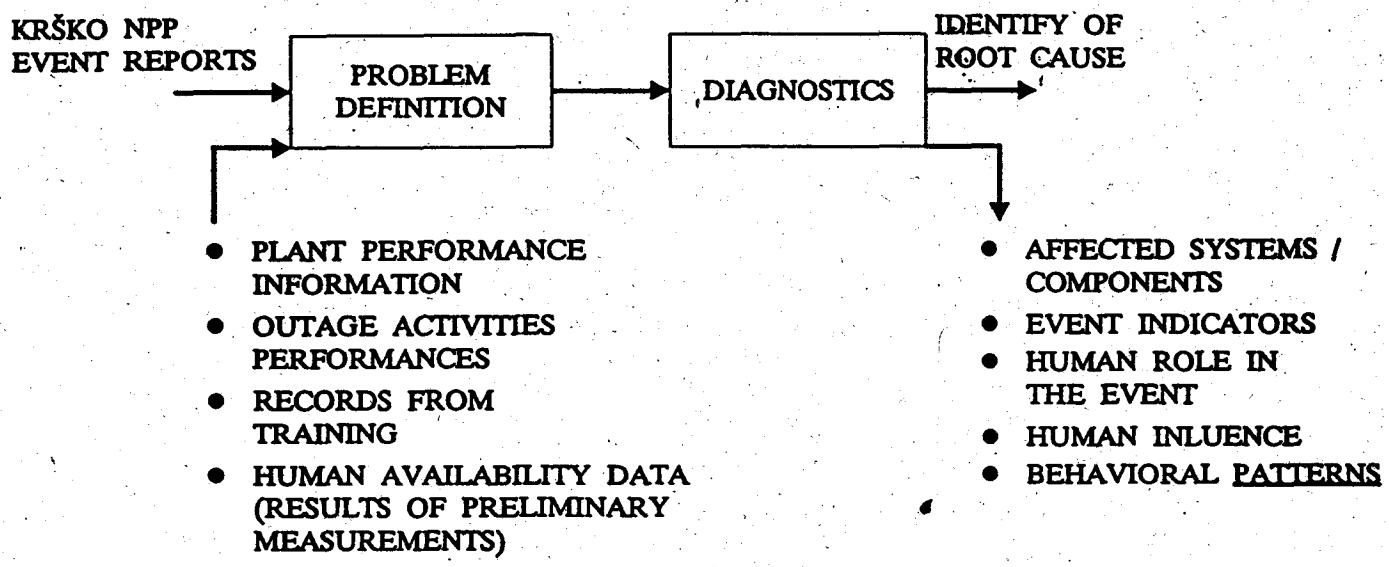


Fig.1 Inputs/outputs of evaluation process

For event evaluation process supporting plant documentation will be use:

- event's report,
- plant operating history records,
- maintenance records,
- surveillance and maintenance procedures,
- other records of system and components operation.

Important review data are personnel availability data which are based on document's review as follows:

- level of personnel availabilities,
- nature of personnel proficiency testing,
- trending of personnel performance,
- acceptance criteria for personnel proficiency,
- description of workers behaviour in the event situation.

3.1 Identification of the nature of event

Identification of the nature or direct cause of the event is used as the first step of evaluating process. Direct cause of an event could be based on:

- equipment failure (mechanical, electrical, chemical, core physics, hydraulic or instrument failure),
- environmental (internal or external conditions), and ...;
- human error.

A flowchart of identification of direct cause of event is presented on Fig. 2.

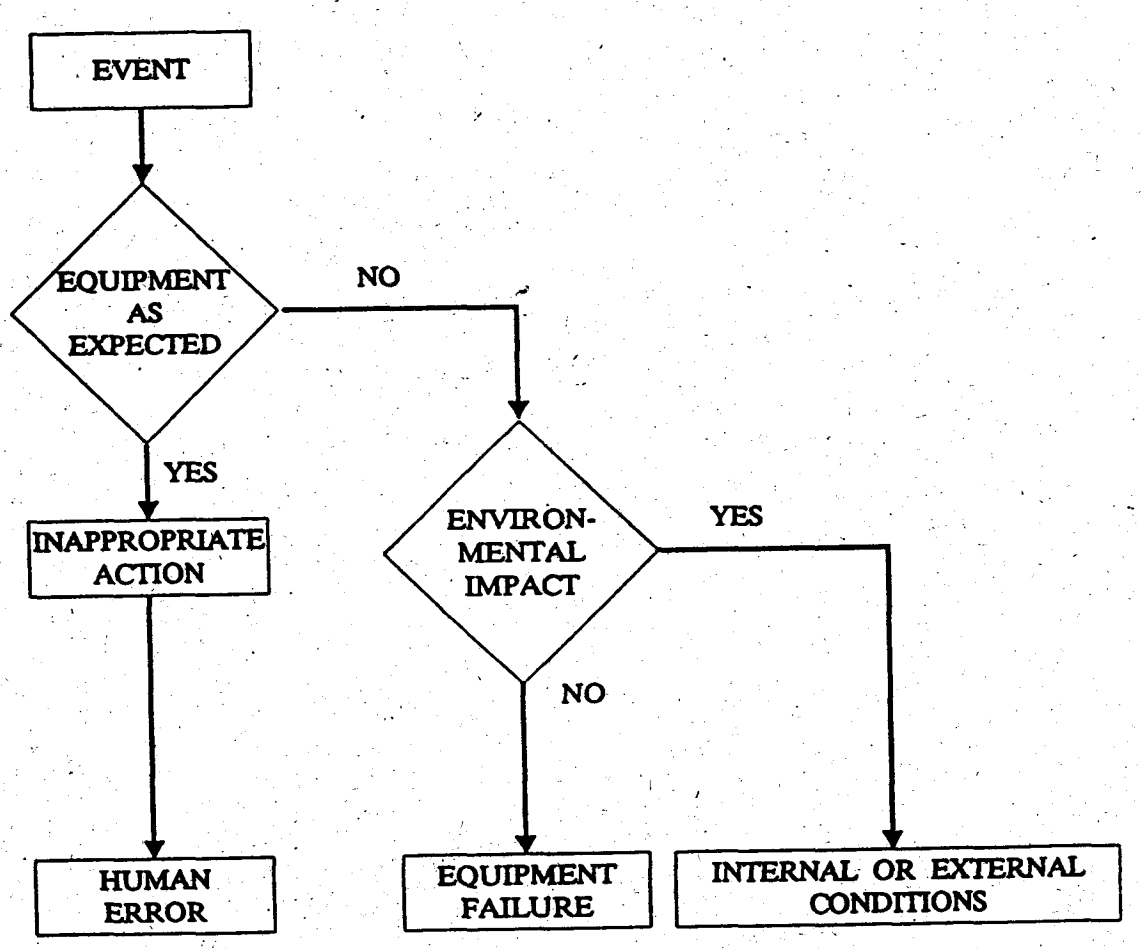


Fig. 2: Flowchart for identification of the nature of the event.

Our attention will be oriented to the human error related events. Irrespective of human error related events, all events will be analyzed and selected into two steps regarding to:

- plant operation conditions (operating and refuelling conditions), and
- nature of the event.

3.2 Identification of the root causes of an event

The starting point of the investigation of the root causes of the event is the latent weakness and its contributors, which were identified as direct causes of the event in section 3.1. The root cause analyze include the potential contributions to stated human errors and equipment deficiency.

Different method can be used to identify the root causes. The method depends on nature of the event. Sometimes, more than one method is required to identify the true root cause(s).

First step of event's analysis is related to the chronological sequence of event and it's check for logical consistency.

Events are usual a combination of several interconnected occurrences. To analyze potential significance the logic tree should be used. The logic tree establishment make more easily identification of any relevant missing information.

For all events, where we have enough reliable data we will use the method which is presented in part 3.3. This method is focused to the human malfunction.

3.3 Description of the method used for analysis of events involving human malfunction

For detailed analyses of human aspect of the reported event we had decided for Classification System for Reporting Events Involving human Malfunctions (RISO-M-22490) /5.3/.

Used method has the following chapters:

3.3.1 Description of the facility

In this chapter facility as itself, operational status and equipment where the error occurs are described.

3.3.2 Description of work

In this chapter work, working situation and the error location are described.

3.3.3 Description of mistakes

In this chapter mistakes' characteristics as the way of mistakes detection, work phase in which mistake occurs, description of mistaker's cause, mistakes circumstances and recovery possibilities are described.

3.3.4 Mistakes mechanisms

In this chapter task phase and mistake's influence are described.

3.4.5 Description of human factors

In this chapter personality's factors, situation's factors influencing human behaviour task performing by the worker who did a mistake, causes of human ineffective behaviour, internal causes of ineffective behaviour and external aspects of ineffective behaviour are described.

For detailed analysis of mistakes impacts, description of ineffective behavioural patterns and internal causes of ineffective behaviour special, more detailed procedures are used.

On the basis of analysis' results conclusions about mistakes and its influence on system's performance are possible.

Detailed analysis of human ineffective behavioural patterns describe the most frequent human mistakes and ineffective behavioural patterns.

The most frequent mechanisms of human malfunctions are:

* malfunction in discrimination:
  - stereotype fixation,
  - familiar short-cut,
  - stereotype take-over,
  - familiar pattern not recognised.

* malfunction in information processing:
  - information not received,
  - misinterpretation,
  - assumption.

* malfunction in recall:
  - forget isolated act,
  - mistake in choosing alternatives,
  - other slip of memory.

* malfunction in interference:
  - condition or side effect not considered.

* malfunction in physical coordination:
  - motor variability,
  - spatial disorientation.

According to our results the most frequent were knowledge based and skill based errors. At the time of the lowest level of operators cognitive availability errors, "like not taking into the account all circumstances and side effects", were very frequent. On the skill based level errors like motoric variability and reaction slips were frequent.

Detailed analyses of ineffective behavioural patterns and cognitive and sensorimotor availability of operators shows that the highest number of knowledge based errors was at the time of the lowest level of cognitive availability. The highest number of skill based error was at the time of the lowest level of sensorimotor availability. These were internal causes of human mistakes. Connections between time distribution of erroneous behavioral patterns and worker's availability confirm the right path of the analysis. External factors affecting human behaviour were: inadequate organisational model, inadequate training and technological problems and were analyzed separately.

Results of these analyses were compared also with results of other field measurements of human availability and fitness for duty. Connections between human availability and human performance is obvious. Model for this connection was developed. Combination of different kinds of data and use of developed model together with analysis of behavioural patterns in event's situation should be a useful tool for further improvement of workers' behaviour in operations's and outage's situations.

4. CONCLUSION

On the results of sample's analysis, we analyzed 23 events, same changes in organisation and work complexity were done. It is obvious that a lot of event's causes may be avoid with investments in organisation and human availability.

More detailed analyses of human behaviour and human error in connection with the data of human availability may offer answers on questions like: how to organize work, how to define responsibilities and communications, how to organise training, recruitment of personnel and fitness for duty activities.

5. REFERENCES

/5.1/ Asset Guidelines, IAEA-TECDOC-573, International Atomic Energy Agency, Vienna, 1990.

/5.2/ System for Reporting Unusual Events in Nuclear Power Plants, Safety series No. 93, IAEA Safety Guides, International Atomic Energy Agency, Vienna, 1989.

/5.3/ Rosmussen I., Mancini G., Carrino A., Griffan M. and Cognolet P: Classification System for Reporting Events Involving Human Malfunctions. Roskilde: RISO-M-2240, 1981.

/5.4/ Škof M.: Organizacija dela v različnih izmenah in delovna učinkovitost upravljalcev rezervnih avtomatiziranih procesov, Univerza v Mariboru, 1990.

Spain

OECD/NEA PRINCIPAL WORKING GROUP Nº 1

EXPANDED TASK FORCE ON HUMAN FACTORS

TASK 4:

"HUMAN FACTORS RELATED TO COMMON CAUSE FAILURES"

SPANISH CONTRIBUTION:

" THE USE OF HUMAN RELIABILITY ANALYSES INCLUDED IN PROBABILISTIC SAFETY ANALYSES AS PREDICTIVE TECHNIQUE TO IDENTIFY POTENTIAL HUMAN COMMON CAUSE FAILURES "

September 1994

" THE USE OF HUMAN RELIABILITY ANALYSIS INCLUDED IN PROBABILISTIC SAFETY ANALYSIS AS PREDICTIVE TECHNIQUE TO IDENTIFY POTENTIAL HUMAN COMMON CAUSE FAILURES" .

1. INTRODUCTION

1.1 HRA methodology: identification of dependencies.

1.2 Detailed analysis of dependencies.

2. APPLICATION OF THE METHODOLOGY FOR IDENTIFICATION AND ANALYSIS OF POTENTIAL HUMAN COMMON CAUSE ERRORS.

2.1 Human Errors related to Uncorrected Positions after Testing, Maintenance, Calibration and Operative Realignements.

2.2 Human Errors related to Miscalibrations

2.3 Human Errors during Accident Sequences

2.4 Common Cause Failures and Dependency Analysis

3. PROPOSED IMPROVEMENTS AND LESSONS LEARNED

4. GENERAL CONCLUSIONS

References

1. INTRODUCTION

The Probabilistic Safety Analysis (PSA) is an analytical technique for integrating diverse aspects of design and operation in order to assess the risk of a particular nuclear power plant and to develop an information base for analyzing plant-specific and generic issues. In achieving these objectives, PSAs serve many purposes.

An analysis of the plant-specific risk provides both a measure of potential accident risks to the public and insights into the adequacy of plant design and operation.

A PSA involves the definition and analysis of initiating events and accident sequences, an analysis of plant systems and their operation, the development of a data base for initiating event frequencies and component unavailabilities, the analysis and quantification of human errors, and an analysis of results after accident sequence frequencies estimation.

Past PSAs have shown the importance of operator error. These human errors are included in the system and sequence models (fault and event trees). The analysis performed in the human reliability task mainly involved a review of testing, maintenance, calibration and operating procedures to identify the potential human errors to be included in the PSA. A review of plant administrative controls and procedures and of the control room design is also performed to establish a foundation for the assignment of failures rates to the human errors.

The Human Reliability Analysis (HRA) basic objective, within a PSA, is that all credible human actions, which could affect safety, be incorporated into the overall analysis in an adequate, systematic and traceable way, documenting properly the assumptions, expert judgements, analysis methods and information sources considered.

EMPRESARIOS AGRUPADOS has developed most of the PSAs done in Spain, along with the associated HRAs. From internationally accepted methodologies, this company has developed, based on its own practical experience, the analysis method described in the following.

1.1 HRA methodology: Dependencies identification

The basic steps of an HRA, during a Probabilistic Safety Analysis, are:

- Process of Definition and Identification of Human Actions. Basic criteria and the method for determining human actions to be considered in the different PSA models and in the preliminary analysis of dependencies are indicated at this step.

- Assignments of Preliminary Estimates to the human error basic events.

- Selections of the Human Actions to be analyzed in more detail.

- Analysis and assignments of Final Estimates to the human error basic events.

- Final process for Dependency Analysis.

- Identification and analysis of Recovery Actions for accident sequence cut sets, if necessary.

- Documentation of the HRA.

At the first step (Definition and Identification of Human Actions), a search for possible dependencies is already done. These human error dependencies may be roots of common cause failures.

When there are human actions that affect unavailabilities of components included in PSA models and combined by means of "AND" gates a potential human error basic event is considered. That is, a potential human common cause error is analysed when occurrences of at least two events are needed for a considered failure and there are identified human actions affecting both events.

Furthermore, if during a sequence analysis, there are functional headers including diverse components that must be actuated simultaneously in accordance with some plant procedure steps, even if they are trains of the same system, a possible dependency is considered between them. This dependency is considered as total in most cases, being modelled as an only overall human action.

It is interesting to outline that there are essentially two types of dependencies: First type is the functional dependencies among the operation shift actions, that must mitigate the accident conditions. Second type is the dependencies due to the fact that modelled components are manipulated during normal operation by maintenance or operation personnel, affecting the unavailability of those components when they are not restored to their correct position. These later type of dependencies are called specifically common cause human errors. Nevertheless, although they only appear in accident scenarios, functional dependencies are also important and they will also be considered in the following.

Normal, abnormal and emergency operating procedures as well as test and calibration procedures; along with the administrative process for components and systems outage and return to operation in all the plant operational modes, are used as basic sources for the identification and modelling process. Additionally, the analysis of specific situations needs support from plant operation personnel. This means that models will represent plant specific characteristics more adequately.

1.2 Detailed Analysis of Dependencies

After construction of the models and before quantification, estimates for human error basic events are given. Generally, for human errors related to common cause failures in a system, a "BETA" factor of 0.1 is allotted. This means that the estimate is the product of that "BETA" factor times the corresponding estimate for the individual human error basic event.

Once the quantification results are available, the selection process of important human errors is finalized and detailed analysis are developed for the most significant ones.

At the same time, dependencies are looked into the whole minimal cut set list of the different accident sequences. When several human actions appear in the same minimal cut set, they are analysed trying to identify dependencies among them. For that, some criteria like the following ones, are used:

1. Dependencies already considered, in an explicit way, while fault and event trees construction are excluded.

2. Possible dependencies between the manual part of human actions during accidents and actions before the initiating events are also excluded, due to timing differences.

3. Dependencies between functions with widely different characteristics are not considered either.

4. Dependencies between human errors in the same cut set, caused by actions on different systems during an accident, are not considered when there exist clear timing differences and there is not any functional dependency.

Minimal cut sets of this type where none of the preceding criteria are applicable are identified as cut sets with potential human dependencies within them.

At last, the final process of dependency analysis is completed by means of detailed analysis of the most significant ones. For that, the method indicated in Ref.1, related to task analysis, is used and, more specifically, the levels of dependency included in Chapter 10 of that document are applied. Methods based on Non Response Probabilities versus Time Curves are sometimes used for quantifying dependencies among human actions during accidents.

2. APPLICATIONS OF THE METHODOLOGY FOR IDENTIFICATION AND ANALYSIS OF POTENTIAL HUMAN COMMON CAUSE ERRORS

The above indicated methodology allows for identification of potential common cause errors and functional dependencies of human origin. Afterwards, for those selected as important, detailed analyses are done, with the objective of obtaining not only the best and most realistic estimate, but also for finding out which are the mechanisms or factors that contribute more to the error appearance.

2.1 Human Errors related to Uncorrected Positions after Testing, Maintenance, Calibration and Operative Realignements.

For this type of human errors, that are basically linked to the component unavailability, due to uncorrected positions after Testing, Maintenance, Calibration and Operative Realignements, all the manipu-

lations requiring a change in component position or an actuator electrical disconnection are identified. They are also identified all those test or operating procedures that allow somehow for verification of the proper component position.

Later, and by means of a weighting formulation based on the relative frequency of manipulations and verifications as described in Ref. 2, the remaining unavailability of the specific component is calculated, taking into account all the activities taking place on it.

In this way a list of manipulations and verifications is available for all the PSA modelled components. This is the basis to determine the need for including this type of human common cause errors into the models. Thus, if it is observed a manipulation that affects to two functionally redundant components, that is, they come into the models combined with an "AND" gate, it will be necessary to include a common cause error on them, due to that shared manipulation. On the other side, those different manipulations on functionally redundant components, but with some similarity, in timing, location or in operational state, that may make feasible a human common cause error on those components, will have to be also considered.

2.2 Human Errors related to Miscalibrations

The very calibration processes have the characteristic of verifying instruments calibration and, at the same time, they are also themselves possible causes for generating another miscalibration.

It is only after a channel actuation test that the operative functionality of the channel set points can be demonstrated. However, when there are several channels measuring the same variable, cross comparison is feasible and it allows for detecting some channel that might be miscalibrated or actuating in a non adequate way.

The human common cause errors in calibrations come up to be the most significant in the case of cross comparisons among channels that cannot detect the error, e.g. miscalibration due to the use of an inadequate calibration master. Therefore, common cause errors for instrumentation channels that are combined under redundant actuations logics must be considered.

Additionally, the perfomance of calibration processes, in individual channels or in several channels simultaneously when allowed by the logic, is also a relevant factor to be considered when searching for possible common cause failures due to miscalibration.

2.3 Human Errors during Accident Sequences

During the mitigation of initiating events the operation personnel are one of the main causes of potential dependencies between different trains, systems or functions implemented to cope with those events. Therefore, it is necessary to analyse in the PSAs that possibility of dependencies.

To identify those dependencies, not only the needed tasks for action development, but also the necessary instrumentation to make decisions about what to do, are taken into account.

This identification is done initially by allotting total dependency to simultaneous actuations on components of redundant trains. Additional dependencies are considered and analysed when operators must do timed manipulations along the accident sequence, taking into account the variables that must be awared, instructions of the emergency operating procedures, organization of operation shift, ...

2.4 Common Cause Failures and Dependency Analysis

Once the human errors with potential to cause common cause failures or to generate functional dependencies along accident sequences are identified, a detailed analysis is performed for the significant ones. To determine which are the most important two selection criteria are basically used. The first is qualitative and based on the selection of those human errors that cause simultaneous failures of several functions, systems or trains. The second is quantitative and applied after the preliminary quantification of accident sequences. It means the selection of human errors that appear in minimal cut sets contributing at least 1% to the overall core melt frequency per initiating event group.

All selected errors are analysed in-depth by means of detailed analysis. The others are kept with the initial conservative values due to their less importance.

For human errors representing uncorrected positions after Test, Maintenance, Calibrations or Operative Realignements, a detailed analysis is done according to Ref. 1 methodology for the most contributing manipulations to the analysed error. In this analysis, the specific paths that are more likely to cause the failure are identified and studied. In this way, for instance, for two functionally redundant components that are actuated simultaneously during a test, the omission of returning to their initial positions could be considered the most significant common cause error when this instruction is on the same step of the testing procedure and there is not any additional caution or alarm against this error.

Regarding erroneus calibrations, the most frequent common cause error is a miscalibration of the very calibration master, or its inadequacy. This means that every instrumentation channel calibrated with that master will be left with uncorrect setpoints, which is very important when calibration of redundant channels are performed with the same master.

Finally, related to functional dependencies among human actions on an accident sequence, it is a significant error the dependency due to an erroneus determination of the symptoms that, according to emergency procedures, initiate several human actions that tend to achieve the functionality of redundant equipment.

The in-depth analysis of all the tasks required for a correct development of the considered human actions, improves the knowledge of the influences, or perfomance shaping factors, that contribute more to each of the potential failure paths. It also allows for a valoration of how abnormal, emergency and administrative procedures affect the development of human actions and, not only implies a correct estimate for the considered error, but also the way to minimize or eliminate its possibility by means of changes or modifications.

3. PROPOSED IMPROVEMENTS AND LESSONS LEARNED

In all the Spanish PSAs there have been identified human common cause failures that were significant contributors to core melt frequency. Corrective measures have been taken, about most of them, that can be classified into the frames of prevention, detection,

mitigation and even recovery of accidents. At this point, some of them are going to be presented.

- Category of human common cause failures:

a) One of the dominant contributors to the recirculation phase failure in a PWR reactor, after depletion of Refueling Water Storage Tanks, was that the flanges in the containment sump suction lines be not removed. These flanges should be installed during shutdowns for getting the pressure needed to test the contaiment sump valves. This common cause human error would affect to all the system trains suctioning from the containment sump (Containment Spray and Safety Injection), if all the flanges were not removed from there.

Once the basic event was identified and its importance detected, several solutions were proposed. The finally implemented improvement consisted of a verification of the flanges removal by two redundant and diverse means. The first was the verification, using a check list and before containment closure, by the operating walkaround teams, and the second was the independent verification, by the engineering staff, of the correct flanges relocation in their storage, when required work was over. Consequently, a solution to detect the most likely human common cause error, the flanges non removal error, was taken.

b) During the execution of the AFW turbo-pump functionality test, the realignement of three manual valves could be required in such a way that if the three valves were left, simultaneously, in the wrong position when the test be over, this pump train would result unavailable. Although during normal operation these valves are locked open, due to the importance of such train, it was recommended to place limit switch indicators in the control room panels for these manual valves and to include these valves position in the control room daily verification check list. In these way the unavailability allotted to the human common cause failure could be decreased down to a practically negligible value. This is another example of solution based on error detection.

c) In situations of erroneus calibration of transmitters, the dominant error, regarding individual failures, was represented in a plant by the need to transfer the affected instrument setpoint values to

an auxiliary sheet, in order to avoid contamination of transmitter cards if carried into the containment building. Fortunately, this type of error was not applicable to common cause errors since that plant uses individual transmitter cards, but in the case that cards were used per type of primary element, this failure mechanism would have had the same relevance as the calibration master failure. The finally implemented solution consisted of making a photocopy of the transmitter card instead of transfering the setpoints by hand from the transmitter card to the auxiliary sheet. Consequently, a solution based on the prevention of error mechanism was adopted.

d) Regarding Safety Injection Accumulators discharge in PWRs, the dominant failure was the common cause miscalibration of the pressure instrumentation which is used for measuring the accumulators N_2 atmosphere pressure. Since calibration is performed during plant shutdowns and there are two channels per accumulator, to prevent the common cause failure, the channel calibrations was decided to be performed by two different teams with different calibration masters. Consequently, the solution adopted was of the type to prevent occurrence of the most significant error.

- Finally, regarding <u>category of functional dependencies</u> among actions during accidents, after in-depth analysis of failure mechanism in the manual and cognitive parts, most of the solutions adopted for significant actions have been based on specific design modifications and changes in plant procedures, oriented towards human error prevention. Some of the solution types are summarized in the following:

e) In some situations, the analysis has demontrated that available time for developing an only action, needed commonly for the success of several functions or systems, was not enough to assign a proper value. This is the case of complex manual tasks associated to an overall human action. For this reason, design and procedure modifications were done, in order to reduce the available time, like changing the type of some actuators from local to remote and transfering the tasks to the control room. Time margins were improved in this way and more time is available to develop the action.

f) Finally, some situations appear where the number of symptoms described in the procedures for specific accident sequences is not sufficient or symptoms are confusing. In that cases the scenarios can

be improved by adding new redundant symptoms for reducing existing dependencies.

4. GENERAL CONCLUSIONS

This Probabilistic Safety Analysis methodology has proven its adequacy to identify some types of human common cause errors, mainly those related to deficiencies in test, maintenance, calibration and verification procedures and those representing functional dependencies among human actions during accident sequences.

This methodology has the advantages of helping to search for, in a sistematic way, the potential most relevant human common cause errors and of permitting to obtain a relative ranking of the importance of these erros. Thus, it is easy to know which are, if improved, the solutions that would contribute more to an overall risk reduction.

Additionally, the detailed analysis of tasks that could generate the considered errors implies a better knowledge of mechanisms contributing more to error progression. In this way, failure paths that must be mitigated are put into evidence and it is also possible to evaluate and compare different options for correction, if they exist.

It is important to remark that this methodology requires of a strong interaction with plant personnel to have with them the specific view for identification, analysis and solutions of detected errors. This contributes also to a better acceptance and knowledge of the relevant aspects and to more adequate recommendations about specific needs in each situation.

Therefore, the availability of results and models of a Probabilistic Safety Analysis and the associated Human Reliability Analysis is a very adequate means for identification, evaluation and correction of some types of common cause failures and functional dependencies. And this allows for a continous updating according to changes and modifications during the plant life.

References

1. NUREG/CR-1278: "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications". (1983).

2. PSA'89 International Topical Meeting on Probability, Reliability and Safety Assessment (Pittsburgh, USA): "Evaluation of the Contribution of Unrevealed Human Errors to Core Damage Following a Transient" (1989).

3. Spanish NPPs PSAs.

United Kingdom

HUMAN ERROR DEPENDENCY

J Berman (Four Elements Limited, Greencoat House, Francis Street, London SW1P 1DH)

on behalf of HFRG Human Error Dependency Sub-Group

1. INTRODUCTION

This paper is based on the work of the Human Factors in Reliability Group (HFRG) Human Error Dependency Sub-Group, which comprises representatives from across a range of industries. Contributors to this work are listed in Annex 1. Although the work of the group is by no means complete, this paper describes the current status of a programme intended to provide a better understanding of Human Error Dependency (HED), and methods for addressing the issues, both in design and assessment. The paper presents a framework for addressing HED, and highlights by example the nature of the critical issues.

The structure of this paper is to discuss the background to HED, and to define the relevant terms and concepts. A framework for identifying potential dependencies, the conditions which induce them, and the processes which underpin them is described and discussed, and the manner in which potential defences against dependency can be identified and assessed is considered.

2. BACKGROUND

Error dependency is of concern for high hazard systems, in that it can lead to system reliability being different from that which might be claimed under particular circumstances. Typically, where high reliability is required, such as in the context of standby power supply to essential safety systems, one of two solutions is usually adopted to ensure availability; the provision of multiple redundant systems, or multiple diverse systems. However, the benefit of such an approach is only realised if there is no dependency which might affect the true diverse nature of the systems, or the real value of their multiplicity. Whereas this issue has been recognised in the context of hardware dependency, there is a less adequate treatment available with respect to human error dependency.

To determine the anticipated reliability of the system, it is important to be able to identify and predict the possibility of dependency between systems, including HED. Understanding the mechanisms, causes and effects will help identify defences to enhance the system itself. It will also assist in the treatment of dependency within risk assessment, and will generally assist in recognising situations which are sensitive to dependency effects.

Initially, the objective of the Sub-Group was to identify how properly to represent HED effects within fault trees and other analyses. However, as the

understanding of the group developed, it became apparent that greater benefit may derive initially from considering the development of a tool to support the design process. This tool would support the understanding and identification of dependency-prone tasks, particularly during the hazard identification process.

Before discussing HED further, it may be valuable to review examples of HED, as a means of illustrating the nature and scope of the issue. There have been a number of major disasters over recent years, such as Clapham Junction, Zeebrugge, and King's Cross, all of which included the consequences of HED. However, these major disasters represented the unfortunate concatenation of a large number of deficiencies, particularly with respect to management systems, and have been the subject of extensive analyses. Consequently, a selection of examples is taken from less well-known or 'spectacular' incidents.

Example 1:

Standby emergency diesel generators were supplied by two fuel tanks, one duty and one standby. When the duty tank required refilling, the two tanks were changed over, such that the low tank became the standby tank. A person was sent to change over the tanks, by re-aligning appropriate valves. In error he went to the wrong valve on the standby tank. However, expecting that the valve would be locked, and finding that he had a key which fitted the lock, he decided that this was the correct valve. Having therefore re-aligned the wrong valve on the standby tank, there was a much increased probability that he would go to the same wrong valve on the duty tank, which occurred. The consequence was that the inlet rather than the outlet valve was opened on the 'new' duty tank, and hence for some days there was no fuel supply to the standby generators. The probability of a correct second valve identification and alignment was influenced by the initial identification error.

Example 2:

A charge machine for charging and discharging fuel elements in a reactor was designed such that a single set of indicators could refer to either of two channels, depending on how the settings were aligned. On one occasion the settings were incorrectly aligned such that the channel being discharged was not displayed. On attempting to discharge the element from the reactor, no fuel element was seen to move, and hence the operators concluded that the machine had failed to remove the fuel element. None of the operators in the team questioned this diagnosis, nor detected the misaligned indicators. It was only when the charge machine was moved to a maintenance bay that it was found to contain an irradiated fuel element. The probability that any one of the team members would detect the misaligned indicators, or suspect that this was the cause of the apparent failure, was influenced by the behaviour and decisions of the other team members.

Example 3:

A freight train passing an axle hot box detector initiated an alarm. It was reported to the train guard that the hot axle box in question was on a pulpwood wagon. The train was stopped and the guard investigated but went to the wrong wagon and hence found no abnormality. Shortly afterwards the train passed another hot box detector which alarmed. The guard went to investigate, checking all axles, but did not detect the faulty axle box. Whereas the driver should then have independently checked the axles, he decided that the guard was competent, and hence it must be another false alarm. Shortly afterwards the axle box failed and the train derailed. The probability that the second, independent, check would recover the error by the guard was reduced due to the driver's perception of the guard's competence and the previous apparent false alarm.

Example 4:

A final delay tank contained a liquid which could only be discharged when a particular concentration was below a certain value. The liquid was tested and found to be x µg/l, which was below the permissible discharge limit. In fact, the concentration was x mg/l (which was above the limit), but the reading had been misread. The supervisor assumed that the tester was competent, and did not notice the incorrect reading, also misreading the value. The tank was therefore discharged in error. The assumed probability of error recovery by independent check was incorrect.

The importance of each of these examples of HED is that assumed independence led to an incorrect estimation of the probability of certain failures or errors. Thus, a proper understanding of HED would support assessment of the benefits and weaknesses of identified defences against failure. The penalties associated with an identified defence can be assessed. It may also be that there are some benefits associated with an awareness of dependency, concerned with positive self-checking, and awareness of potential difficulties.

3. DEFINITIONS

The Sub-Group recognised a need for agreed definitions of key terms, to avoid potential confusion and ambiguity.

Human Error Dependency

Dependency exists whenever probabilities of actions or errors (or a series), are linked more closely than if random events. (ie the probabilities are conditional).

To be of concern, there must be a functional linkage between the actions which determines the consequences of the dependency.

Functional Links

The functional link is the overall objective that may be affected by the action or group of actions in error. It probably relates to the top event in the fault tree.

Thus, where there are redundant or diverse systems to ensure availability, then there is a functional link between the diverse systems. An HED which affects those systems is of concern. A functional link might exist between diverse systems, and a human action could lead to common failures across multiple plant items. A functional link exists between human actions on a single system, and the reliability of a second action might be conditional on the success of a previous action on that system.

Consequences

The nature of the failure which derives from the dependency:

- *Common Cause Failure (CCF) - a series of system failures for the same reason;*
- *Common Mode Failure (CMF) - a series of system failures in the same manner;*
- *Human Induced Dependency (HID) - the cause of the dependency is human error or action;*
- *Human Dependent Failure (HDF) - the human error or failure is caused or contributed to, by a previous human action.*

Of these consequences, the first two (CCF and CMF) are similar to those which have been considered in the context of hardware dependency, and may be addressed in a similar manner. The third one (HID) also is similar to hardware dependency, except that the cause of the dependent failure happens to be human error or action. The fourth category of dependent failure (HDF) is the most difficult to address, and is a particular focus of the Sub-Group's attention, as it represents the key issue of the probability of a given human error being influenced by the probability of success of a previous action or event.

Human Contribution

The areas of human performance affected by dependency:

- *Intra-individual dependency*
- *Inter-individual dependency*
- *Global/external dependency* (training, procedures e.g.)

The first is dependency between actions by the same person. The second is dependency between actions by different people (eg a Fitter and Supervisor). The third is dependency due to external factors such as procedures or training.

Conditions

The task types which can give rise to dependency. These are combinations of:

- *Person (same/different);*
- *Task (same/different);*
- *Action : Device (same or similar/different);*
- *Time (same or same shift : different).*

There are 16 basic conditions. These range from one person undertaking

Thus, where there are redundant or diverse systems to ensure availability, then there is a functional link between the diverse systems. An HED which affects those systems is of concern. A functional link might exist between diverse systems, and a human action could lead to common failures across multiple plant items. A functional link exists between human actions on a single system, and the reliability of a second action might be conditional on the success of a previous action on that system.

Consequences

The nature of the failure which derives from the dependency:

- *Common Cause Failure (CCF) - a series of system failures for the same reason;*
- *Common Mode Failure (CMF) - a series of system failures in the same manner;*
- *Human Induced Dependency (HID) - the cause of the dependency is human error or action;*
- *Human Dependent Failure (HDF) - the human error or failure is caused or contributed to, by a previous human action.*

Of these consequences, the first two (CCF and CMF) are similar to those which have been considered in the context of hardware dependency, and may be addressed in a similar manner. The third one (HID) also is similar to hardware dependency, except that the cause of the dependent failure happens to be human error or action. The fourth category of dependent failure (HDF) is the most difficult to address, and is a particular focus of the Sub-Group's attention, as it represents the key issue of the probability of a given human error being influenced by the probability of success of a previous action or event.

Human Contribution

The areas of human performance affected by dependency:

- *Intra-individual dependency*
- *Inter-individual dependency*
- *Global/external dependency*

The first is dependency between actions by the same person. The second is dependency between actions by different people (eg a Fitter and Supervisor). The third is dependency due to external factors such as procedures or training.

Conditions

The task types which can give rise to dependency. These are combinations of:

- *Person (same/different);*
- *Task (same/different);*
- *Action/Device (same or similar/different);*
- *Time (same or same shift/different).*

There are 16 basic conditions. These range from one person undertaking

the same task on identical devices during the course of a single shift, to different fitters undertaking different tasks on different systems at different times. The susceptibility to dependency effects will be different for each condition, as will the causal factors.

Coupling Mechanism/Causal Factors
The processes which give rise to the dependent failures:

- *Common training;*
- *Deficient procedures;*
- *Environmental stressors;*
- *Limitations of human information processing*
- *etc.*

In conjunction with the functional link, this is an important part of the understanding and prediction of HED, as it represents the mechanism whereby the dependency arises, and hence indicates the manner in which it might be defended against.

Performance Shaping Factors
Factors which affect the performance of a single task, independent of other tasks.

Whereas a single PSF can affect many tasks, eg the effect of excessive noise on human performance, PSFs differ from HED in that their effect on any one task is independent of their effect on any other task, and hence they do not affect the manner in which probabilities might be represented in a fault tree. They must be distinguished from Global or external Human Contribution, which might be a PSF in another context, but which contribute to HED where there is a functional link between tasks.

4. DEPENDENT BEHAVIOUR, FUNCTIONAL LINKS AND CAUSAL FACTORS

Functional links are significant in the context of HED in providing a means of identifying tasks which might appear unrelated, but which must be assessed for potential dependency, or which, although clearly related, might not immediately appear to be dependent.

Functional links provide a means of pre-specifying task combinations of potential concern. They provide a means of predicting what are the critical paths in the fault tree, or what are the critical design issues on which to focus. Functional links provide a means of 'containing' the HED issue.

Coupling mechanisms can be considered in terms of a set of generic mechanisms into which all *causal factors* can be allocated. The identified categories are:

- Training (Trg)
- Procedures (Proc)
- Hardware (Hdwr)

- Organisation/Culture (Org)
- Physical Environment (Env)
- Cognitive/Psychological Factors (Psych)

Dependent behaviour is affected by the causal factors which influence performance on tasks related by way of identified functional links. To identify how the causal factors might affect dependent behaviour, it is necessary to consider the task combinations in terms of the *conditions* described previously.

Each of 16 conditions can be identified which uniquely describe a given task combination. Examples of these conditions are presented in Annex 2. The purpose of this approach is to identify important conditions in terms of type of dependency. For example, functional links between the task of a fitter, and the task of his supervisor are associated with conditions involving different people. The causal factors associated with conditions involving different people are concerned with training, procedures, etc. This approach provides a basis for developing a framework to assess dependency effects.

5. ASSESSMENT FRAMEWORK

When considering dependency effects it is important to be able to relate coupling mechanisms and conditions. From this, sensitive combinations can be highlighted, and relevant defences can be identified based on control of the coupling mechanisms, the conditions, or both.

The identification of coupling mechanisms and conditions would also act as a screening mechanism for limiting the range of tasks which should be considered in detail for dependency effects. The development of such a screening mechanism has been a focus of attention for the Sub-Group.

Two matrices are being developed, based on the experience of members of the group in hazard identification, risk analysis, and human factors. The first of these matrices can be used to address how well or poorly HED is accounted for in conventional hazard identification and risk assessment, and hence where to focus attention. For each of the possible HED-prone conditions, the type of dependency which could arise is shown, ranked from 1 - 5 (little likelihood of dependency to significant likelihood).

The second matrix can be used to highlight how to defend against potential dependencies by indicating which are the sensitive coupling mechanisms. For each dependency-prone condition, possible coupling mechanisms are ranked from 1 - 5 (least prone to most prone). By highlighting significant coupling mechanisms, and hence potential defences, the analytical process can then consider whether the relevant defences are present within the system in a robust form.

Two sample matrices are presented below. The data presented within them are given for illustrative purposes. The matrices have not yet been fully completed, and will be subject to further review and refinement. In order not to imply that they are in a fully usable form, some columns have been left blank. Furthermore, for clarity, the matrices do not currently show all of the potential conditions. The numbers under each condition refer to the examples given in Annex 3.

Matrix 1: Condition v. Consequence

	sssd 1a	ssdd 1b	sdsd 2a	sddd 2b	dsss 3a	dssd 3b	dsds 3c	ddss 4
CCF	5			3		5		2
CMF	5			1		5		1
HID	5			3		5		1
HDF	4			1		5		3

Matrix 2: Condition v. Coupling Mechanism

	sssd 1a	ssdd 1b	sdsd 2a	sddd 2b	dsss 3a	dssd 3b	dsds 3c	ddss 4
Trng	5	5		2	4			
Proc	5	5		3	5			
Hdwr	5	2		1	5			
Org	5	5		5	4			
Env	5	2		1	4			
Psych	3	3		1	2			

6. DEFENCES

Having determined the existence of a functional link between certain tasks, the assessment process will assist the analyst to determine that a given task condition is sensitive to certain forms of HED. The particular coupling mechanisms which may contribute to dependency can then be considered.

In order properly to review the coupling mechanisms according to the factors which have been suggested from the matrices, it is necessary to examine those relevant factors in more detail. Sets of typical error inducing factors can be identified from human factors knowledge concerning human error and human performance relating to each of those causal factor categories. Annex 4 presents sets of such typical error inducing factors. These are not considered complete, and are being further developed to encompass those conditions with particular relevance to HED.

Typical defences which could be considered as a means of reducing the impact of HED might include the following:

- Staggered testing and maintenance (time separation)
- Redundant operations/maintenance (different personnel)
- Training (eg handovers)
- Safety management systems (culture)
- Communications systems/protocols
- Environmental factors
- Standards specification
- QA
- Supervision/checking
- Good working practices
- Good change management
- Post-maintenance functional testing or inspection
- Avoidance of stereotype violations
- Hardware defences
- Consistency of labelling
- Job support systems
- Experience
- Equipment diversity

If the task condition indicates potential dependency between actions by the same person, then it may be appropriate to consider the psychological error inducing factors. Alternatively, if the dependency of concern arises between different people, then it may be appropriate to consider training factors and procedures. An extended look-up table is being considered as a means of highlighting the relevant error inducing factors for different conditions, and how they might be defended against.

By considering conditions and causal factors, the advantages and disadvantages of each potential defence can be assessed. There will be weaknesses associated with any particular defence. For example, whereas hardware interlocks such as key systems can prevent certain errors, over-reliance on them can introduce dependencies of their own. Similarly, over-reliance on procedural defences such as certain QA systems may reduce the ability to detect and respond to other types of failure.

Defences against dependency can address the coupling mechanism, or they can change the condition itself. For example, potential dependency between actions by the same individual might be defended against by provision of diverse information sources, or by changing self-checking arrangements. Alternatively, it may be more effective to change the task conditions such that different people undertake the various sub-tasks. The assessment process assists in determining the benefits of each approach.

Inevitably there will be a range of different defences against an identified dependency. The assessment process which has been outlined is considered to provide a basis for making explicit the strengths and weaknesses of each potential defence. The precise task demands and organisational requirements

will affect the relative value of each potential defence, and hence careful assessment is required.

7. CONCLUSIONS

HED is a significant issue when considering how to ensure that a system is robust with respect to certain human errors. HED must be explicitly recognised if defences are not to be inadvertently weakened. However, the treatment described above is basically qualitative. Quantification of HED effects is more problematic.

It is important, through consideration of functional links, to identify the significance of potential HED. This will then assist the analyst to determine how far to go in terms of qualitative analysis. The approach to consideration of HED which has been described here can be usefully applied to support conventional analyses. For example, a conventional analysis might claim benefit from the availability of supervision as a means of reducing the probability of unrecovered human error. However, a proper assessment of the opportunity for HED might indicate that the existing supervisory system will not be capable of detecting certain failures. Alternatively, the analysis process might indicate methods for enhancing the effectiveness of the supervisory process.

It is important to consider how dependency will affect the validity of assumptions concerning independence within fault trees. It is important to be able to control the pessimisms which otherwise might need to be built into assumptions. It is important to be able to identify how the design might be further enhanced.

In support of these goals, an approach to consideration of HED is being developed. Whereas an original objective of the HFRG HED Sub-Group was to consider the mathematical treatment of HED in fault trees, the approach which is now considered to be of most value is predominantly qualitative. This approach is considered to support a better understanding of HED issues, and provides a basis from which to identify enhancements to the system which can provide defences against dependency effects.

It is suggested that this more detailed understanding of the system, and of methods for making it better defended against human error, is both a prime benefit of the analysis process which has been described, and also is a typical benefit of the process of risk analysis. The value of that process in terms of assisting the risk analyst properly to understand the system should not be underestimated. The improvements to the system which ultimately derive from that understanding can fully justify the effort expended.

Annex 1

Membership of HED Sub Group

The following organisations (in alphabetical order) have contributed to the work of the Sub-Group:

AEA Technology
British Gas
BNFL
DnV Technica
EWI
Four Elements
HSE
Lloyds Register
Nuclear Electric
NNC
Rolls Royce and Associates

The following persons (in alphabetical order) have been involved with the work of the Sub-Group for some or all of the time:

Peter Ackroyd
Jon Berman
Andy Dolby
Bill Gall
Steve Harris
Paul Hollywell
Gareth Hughes
Angela Jenkins
Keith Mitchell
Gary Munley
Martin Ridal
Sam Samuel
Trevor Waters
Barry Whittingham
Jerry Williams

Annex 2: Conditions

Examples of Conditions:

For each condition, the combination of Person, Task, Device, and Time is represented by 's' or 'd', depending on whether it is same or different. Thus, 'ssss' represents the same person undertaking the same task on the same (or similar) device, at the same time (or in quick succession). Time is considered to be 'same' if the tasks occur on the same shift.

ssss - Fitter carries out same maintenance task, identical plant items, same shift

sssd - Fitter carries out same task on same plant item at regular intervals

ssds - Fitter calibrates pressure and flow transducers on same pump

ssdd - Fitter calibrates pressure transducer on one shift, temperature transducer on different plant item on next shift

sdss - Operator starts diesel generator and loads onto bars

sdsd - Fitter checks pressure of pump on one shift; checks flow on next shift

sdds - Fitter isolates pump and calibrates sensor on same system, same shift

sddd - Fitter isolates pump on one shift; checks operation of valve on next

dsss - Two fitters each carry out half the calibrations on same system

dssd - One fitter calibrates system one time, another the next

dsds - One fitter tests pressure transmitter while another tests guardline

dsdd - One fitter isolates pump, another overhauls valve on next shift

ddss - One fitter inspects components while another assembles them

ddsd - Fitter assembles item, supervisor checks work later

ddds - Operator starts pump while fitter closes valve elsewhere on system

dddd - Fitter opens flange assuming system has been isolated and drained on previous shift

Annex 3: Conditions

Examples of Conditions used in Matrices

The following examples provide an indication of the conditions which might give rise to the dependencies to be considered in the matrices. The numbering corresponds with that used for the development of the matrices.

A performs task T1, then -

1a A performs same task on same device, eg tightens successive studs on pipe flange.

1b A performs same task on different device, eg greases valve then greases pump.

2a A performs different task (T2) on same device, eg opens valve then inspects stem to ensure not leaking.

2b A performs different task (T2) on different device, eg notes vessel level reading, then adjusts temperature in drying chamber.

3a B performs task T1 on same device type at same time, eg A overhauls 3 valves in train, B overhauls other 3.

3b B performs task T1 on same device, as a check, eg A tightens valve, B attempts also to tighten valve.

3c B performs task T1 on a different device, eg A replaces gasket in pipe, B replaces gasket in valve.

4 B performs T2 on same device as a check, eg A handtightens valve to closed position. B checks flow through upstream sight glass.

Annex 4: Typical Error Inducing Conditions

The following lists represent a selection of typical error inducing factors for consideration when assessing potential dependency-prone conditions.

Training Factors

- transfer of training
- inert knowledge
- fidelity
- feedback
- part-task training
- domain-specific training
- overtraining
- interface validity
- team training
- meta-knowledge training
- etc

Procedures

- availability
- accuracy/content
- methods of development
- systems for review and control
- presentation style, clarity and format
- suitability for purpose
- peer group attitudes to use
- management attitudes to use
- training in use of procedures
- etc

Hardware

- layout and access
- controls, interfaces and interface devices
- maintenance and testing
- labelling
- etc

Organisational/Culture

Workload and job management

- excessive workloads
- excessive duration
- inadequate scheduling
- inadequate handover mechanisms
- inappropriate allocation of staff

- failure to manage systematically
- inadequate communications channels
- etc

Provision of job support

- quality/availability/adequacy of procedures
- availability of tools/spares
- training
- pre-task briefing
- etc

Policies and practices

Change management

Expectations, rewards and sanctions

Etc

Physical Environment

- lighting
- noise
- temperature
- protective clothing/equipment
- access
- exposure
- etc

Psychological factors

Individual information processing

- arousal - overload/underload
- workload
- information presentation
- stress
- task consistency
- working memory demands
- long-term memory demands
- etc

Individual decision making

- availability of information
- fixation
- focusing
- hindsight bias
- overconfidence
- immediacy
- oversimplification
- etc

Individual actions

- habit intrusion
- skill

- place-losing errors
- timing
- control
- etc

Group decision making

- failure to share information
  - false consensus
  - pluralistic ignorance
- social pressures
  - group think
  - collective rationalisation
  - stereotyped perceptions
  - exertion of group pressures (conformity)
  - self-censorship of doubt
  - illusion of unanimity
  - etc

Ukraine

SCIENTIFIC TECHNICAL CENTRE OF UKRAINIAN
STATE COMMITTEE
ON NUCLEAR AND RADIATION SAFETY

HUMAN FACTOR IN OPERATION EVENTS DUE TO COMMON CAUSE FAILURES

Analysis of operational event on South-Ukraine NPP from 1.09.94

Presented by A. Rodionov

Analysis of malfunction occurred at the South-Ukrainian NPP

Malfunction name: Shutdown of reactor facility by AZ-1 action due to MCP switching-off because of uncorrect actions of operating personnel.

Date of event: September 1, 1994.

INES rating: 1

PNAE G-12-005-91 rating: P05

1. Brief description and assessment from safety point of view

1.1. Initial state of power unit

Power unit 1 was operating at the level of 500 MWt (1800 MWt). The power rising was carried out in an accordance with start-up program after PPR-94 being finished. Turbine-generator TG-1 was connected to the grid at 17:58 31.08.94.

There MCP 1-4, CP 1-4, feeding turbine pump TPN-A,B, automated power regulator ARM - in «N»-mode (power maintaining), electric hydraulic system regulator EGSR - in «RD-1»-mode (pressure maintaining before turbine stop valves) were in operation. Oil supply to MCP was provided by TA11,12D01 pumps and TA11,12W01 oil-coolers operation. TA13,14W01 oil-coolers were switched-off on cooling water and oil state. Main water level regulator in steam-generator PG-1 was in a remore control mode.

All the protecting and interlocking systems were introduced completely.

1-3 safety systems were reserved.

Scheme of electrical connections was as designed one.

1.2. Brief description

09:30. Due to increasing oil temperature after MCP oil-coolers an application № 286 was filed for to actuate reserve MCP oil-coolers and to take out of action oil-coolers being acted for repair and cleaning in an accordance with the 1.2-103PM program.

10:00. In an accordance with the 1.2-103PM program the preparation was began to make switchings at MCP oil supply systems.

10:09. In violation of 1.2-103PM program, reactor shop operator ORO-7 without appropriate approval and preparation has begun to carry out switchings at MCP-2,4 oil supply system for to actuate a reserved oil-cooler and to switch off acting one.

10:11:11 Due to engineering protection system TZ acting on lubricant pressure decreasing MCP-2,4 were switched off.

10:12:33. Due to interlocking action on level decreasing in steam-generator auxiliary feeding electric pumps VPEN-1,2 were switched on.

10:13. ORO-7 without appropriate approval and preparation began to carry out switchings at MCP-1,3 oil supply system for to actuate reserved oil-cooler and to switch off acting one.

10:14:11. When valve at oil input to TA13W01 oil-cooler was opened, pressure at TA11D01 head had decreased, resulted in that it switched off due to appropriate interlock acting and TA13D01 switch on.

10:14:27. Because of TZ on lubricant pressure decreasing action MCP-1,3 were switched off.

10:14:28. On MCP switched off, emergency protection system AZ-1 was actuated.

10:14:40. AZ-1 was doubled by key from the UCP.

10:14:46. TG-1 stop valves were closed by key from the UCP.

10:14:49. TD70D11 pump was actuated, boric acid solution introduction into the primary circuit began.

10:14:55. TPN-B stop valve was closed by key from the UCP.

10:15:14. TPN-A stop valve was closed by key from the UCP.

10:15:45. TD70D31 pump was actuated.

10:16:22. Generator was disconnected from the grid.

10:16:23. Electric power supply for own needs 6 kV sections feeding was transferred for redundant supply.

10:17. Reactor facility parameters were stabilized in a natural circulation mode.

1.3. Final state of unit

Reactor is in subcritical state - hot shutdown.

1.4. Malfunction consequences for safety

a) off-site impact

- external radioactivity release - none
- public irradiation - none

b) on-site impact

- on-site radiational contamination - none

- NPP staff irradiation - none

c) protection-in-depth degradation

- safe operation limits violation - none

- safe operation conditions violation - none

1.5. Malfunction characterization from the safety point of view

From the safety point of view given malfunction can be characterized as an initial event for a design based accident - heat removal over the primary circuit violation due to 4 MCPs switching off. It is necessary to note that this malfunction was initiated by the common cause failure.

2. Selection of events for deep analysis

2.1.Composition of malfunction involved events chronological sequence.

Event 1. Oil temperature increasing.

Event 2. An application for TA11W01, TA12W01 oil-coolers taking into repair and TA13,14W01 reserved oil-coolers actuation was filed.

Event 3. Absence of communication between UCP and A102/1 and A102/2 premises.

Event 4. ORO-6 left to another room to communicate with UCP.

Event 5. ORO-7 began to carry put switchings without an order and in absence of ORO-6 which was requested by program.

Event 6. Erroneous opening of TA12S07, TA14S07 valves.

Event 7. Unsuccessful transition to redundant heat-exchanger TA14W01 by TA14S08 being open and TA12S08 being closed.

Event 8. MCP-2,4 switching off due to TZ action on oil pressure decreasing.

Event 9. ORO-6 report on unsuccessful transition to redundant oil-coolers.

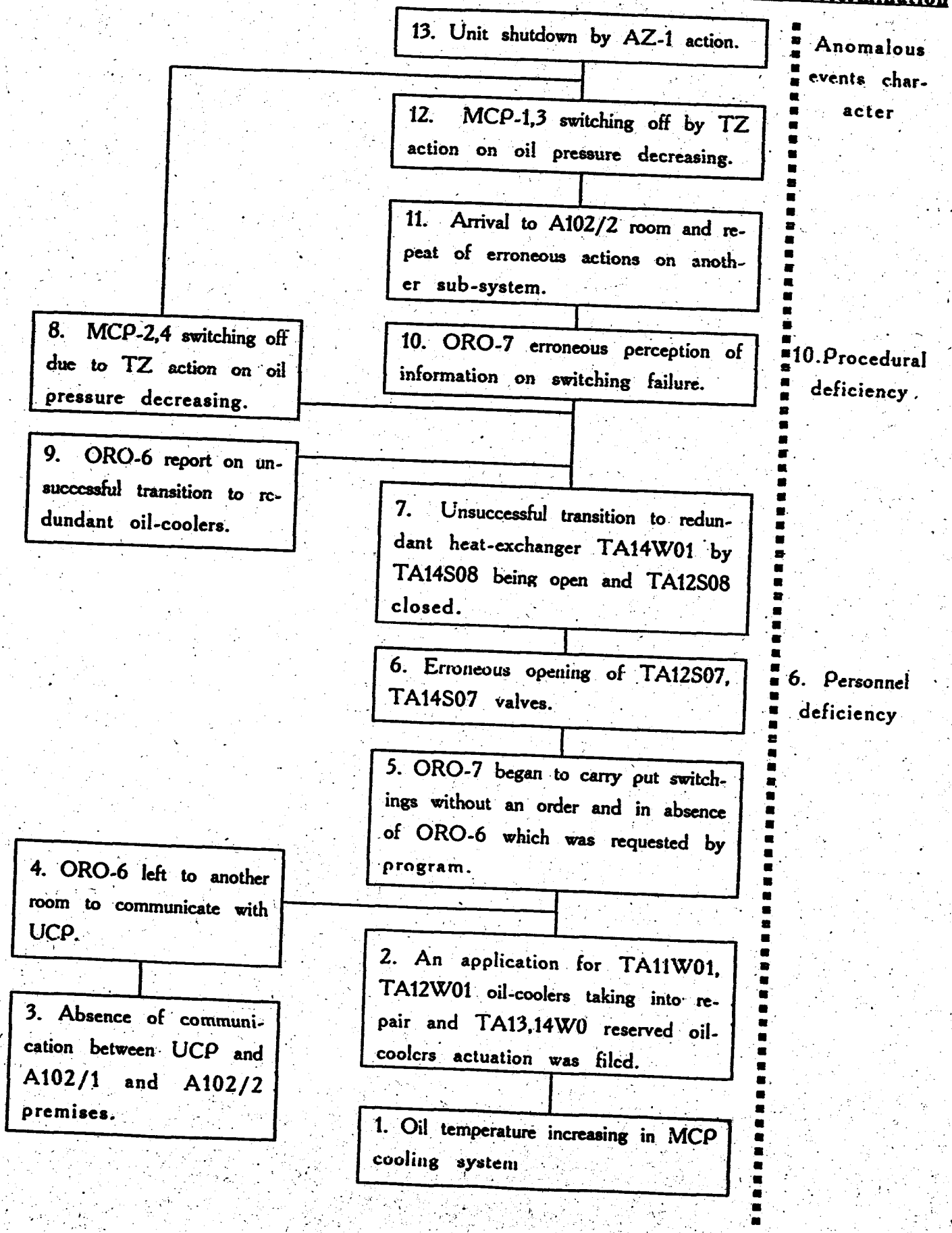
Event 10. ORO-7 erroneous perception of information on switching failure.

Event 11. Arrival to A102/2 room and repeat of erroneous actions on another sub-system.

Event 12. MCP-1,3 switching off by TZ action on oil pressure decreasing.

Event 13. Unit shutdown by AZ-1 action.

2.2. Composing of logical event tree and their character determination



2.3. Selection of events for deep analysis

2.3.1. Events 6 and 10 are anomalous ones.

2.3.2. Event 6. Erroneous opening of TA12S07, TA14S07 valves.

2.3.3. Event 10. ORO-7 erroneous perception of information on switching failure.

3. Determination of anomalous events direct causes

Event 6. Erroneous opening of TA12S07, TA14S07 valves.

Direct causes: communication means failure, lack of clear marked equipment.

Event 10. ORO-7 erroneous perception of information on switching failure.

Direct cause of event was an operator error.

4. Determination of anomalous events root causes

Event 6. Erroneous opening of TA12S07, TA14S07 valves.

Root cause of event was in unqualified control over the communication means and equipment marking.

Event 10. ORO-7 erroneous perception of information on switching failure.

Root cause of event was in lack of orders and reports passing path in working program description.

5. Determination of correcting measures

Event 6. Erroneous opening of TA12S07, TA14S07 valves.

Correcting measures on direct causes	To implement modern and reliable communication means. To check presence of marking on NPP equipment in an accordance with GOST. To make a clear marking with bright paint.
Correcting measures on root causes	To complement maintenance work program with point on obligatory checking of marking availability and state. To enhance shop management control over the operators implementing their duties.

Event 10. ORO-7 erroneous perception of information on switching failure.

Correcting measures on direct causes	To instruct operators on their interaction while switching of equipment.
Correcting measures on root causes	To develop regulated command format to use while switching of equipment.

6. Common lessons learning

6.1. It is necessary to note that the root and direct causes of considered event such as lack of communication or poor communication between operators and the UCP, poor operators interaction while implementing the works, unavailable or unclear equipment marking are common for all the NPPs.

6.2. Above deficiencies were noted in ASSET- recommendations after missions were conducted at the Ukrainian NPPs. The similar problem was discussed at OECD working group meeting on human factor role while failures on common cause studying.

6.3. Because of failures on common cause are of great importance it is necessary to pay a particular attention to implementing of analytical methodologies for this problem into practice of UkrSCNRS and UkrSCNPU.

SCIENTIFIC TECHNICAL CENTRE OF UKRAINIAN STATE COMMITTEE

ON NUCLEAR AND RADIATION SAFETY

HUMAN FACTOR IN OPERATION EVENTS DUE TO COMMON CAUSE FAILURES

Presented by A. Rodionov

1. Introduction

The present report gives an in-depth analysis of some safety significant common cause failures and role of human performance in these failures, using two examples of operational events occurred at Ukrainian NPPs. The analysis is being performed according to the methodic developed in UkrSCNRS Scientific and Technical Centre , following to IAEA Guide (TECDOC - 632, ASSET).

Some definitions and concepts related to generic approaches to common cause failures analysis are given below:

Common cause failures - these are failures of some elements in one or several systems appear as a result of internal or external effect, component failures or human errors during system design, manufacturing, installation and/or operation. Common cause failures are classified according to failure main source:

- failures caused by internal or external effects;

- structural- functional failures;

- common mode failures: common design or operational conditions;

- failures caused by human errors.

In their turn, common cause failures happened because of human errors could be explained by a likeness of adjustment, calibration, maintenance, testing or operation procedures. It also could be an error in installation, procedure or organization drawbacks, incorrect actions or missing of the action in the process of work performance etc.

In general, common cause failures analysis is aimed on identification and registration of these failures for safety ensurance and development of preventive measures.

In the database, which is processed in UkrSCNRS Scientific and Technical Centre there are registrated some events, qualified as common cause failures:

as for 1992	2 events
as for 1993	8 events
as for first half of 1994	4 events

Despite comparatively small statistic flow, this type of failures seems to be extremely important to safety and worth special attention , what will be illustrated in the examples given below.

2.Example of analysis of operational event at Zaporozhje NPP.

Event title: Zaporozhje NPP unit 2 safe operation limits violation due to a steam leakage in the secondary circuit in the isolated part because of bypass valves (BRU-K) failure to close due to common cause.
Event date: 3.01. 1994
Level according to INES : 1

2.1. Brief description and assessment regarding to safety

2.1.1 Unit primary status

January 3, 1994 unit 2 was operated with power level Ne=950 MW. High pressure feedwater heater (PVD) of group A was in operation, high pressure feedwater heater of group B was in maintenance. Safety protection systems of high pressure feedwater heater of group A were in operation, safety protection systems of group B were switched off.

2.1.2 Brief description

15:11:01 Due to improper actions of I&C Department maintenance personnel there was a false actuation of safety protection system on water level increase in PVD 6B. Turbine driven feedwater pumps 1,2 (TPN) were automatically switched off on fact of safety protection systems actuation on level increase in any PVD. Turbine generator 2 (TG) was automatically switched off on the signal of the last TPN trip. On the fact of load discharge bypass valves began to open and on the signal P_{st}>73 kg/cm^2 dump valves worked for the short time. Unit unloading system and power governor were actuated to unload reactor facility.

15:11:23 According to the «Accident Mitigation Instruction» paragraph 16.4.1. operator had performed the reactor scram manually from CR control panel. On level decrease in SG 1-4 main

circulation pumps (MCP) 1-4 were switched off.

15:11:40 There was lost the automatic control of all the four bypass valves, which were fully open. Despite the pressure in the main steam header (MSH) was lessened, bypass valves had not closed on the signal $P_{MSH} < 57 kg/cm^2$.

15:11:59 On the fact Tsi-ii>75C, Psg<50 kg/cm², Tik>200C main steam isolation valves were automatically closed and 1-3 trains of ECCS and emergency feedwater system were actuated.

15:14:20 Bypass valves were closed remotely from CR control panel.

15:30-17:50 After core status assessment safety protection systems were switched off, level in SG1-4 restored, MCP4,1 switched on.

Because of bypass valves beyond design basis failure there was level decrease in the pressurizer down to 3720 mm and pressure drop in SG 1-4 to 44kg/cm². This was safety limits violation on level in the pressurizer by 280 mm and pressure in the steam generator by 1kg/cm².

2.1.3 Unit final status

18:00 Reactor is subcritical, T1k=160kg/cm², T1=260C, MCP 1,4 are in operation.

2.1.4 Violation consequences for safety

a) Off-site effects:

- off-site radioactive release NO

- public exposure NO

b) On-site effects:

- site radioactive contamination NO

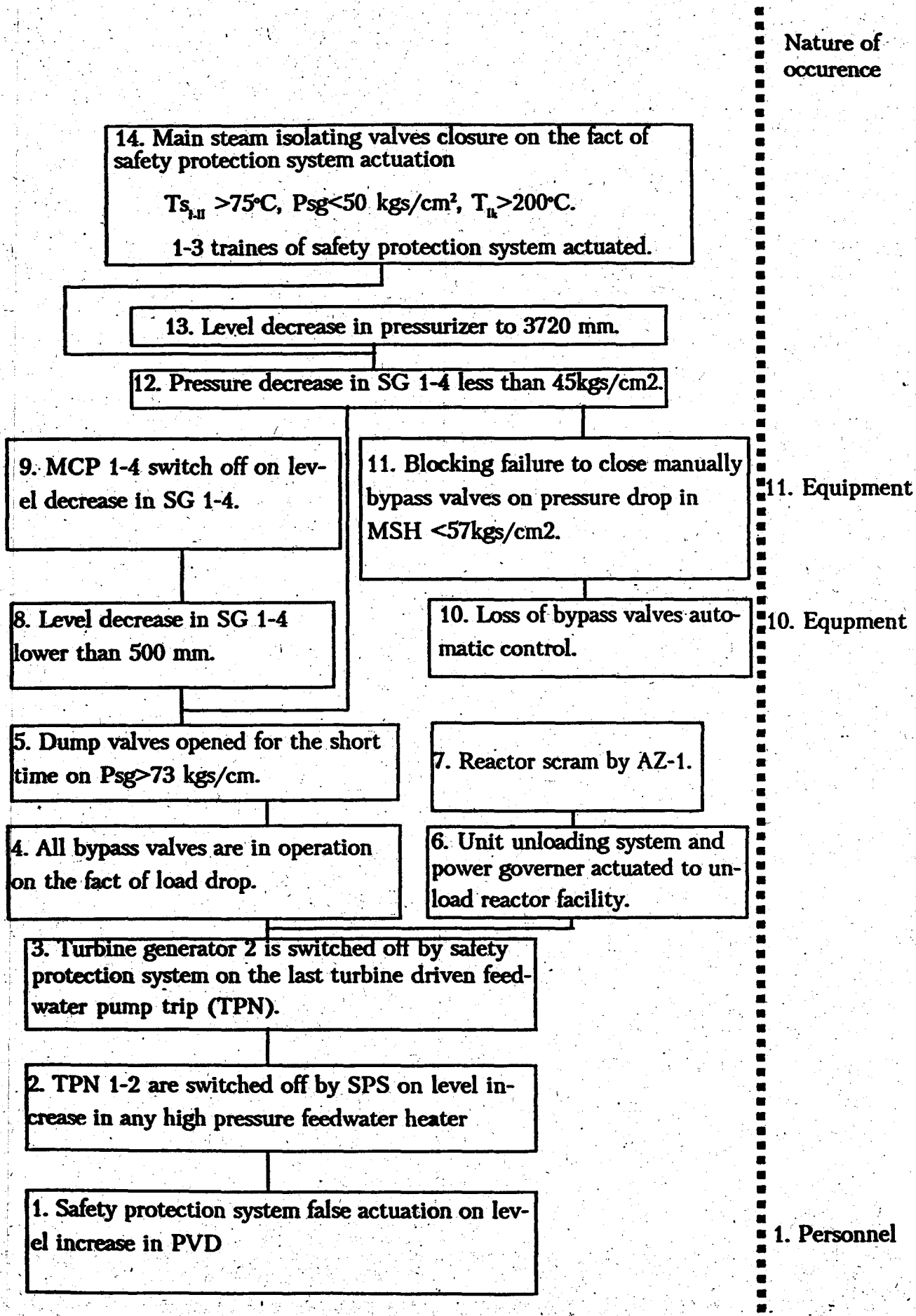
- plant personnel exposure NO

c) Defence-in-depth degradation:

- safe operation limits violation YES

2.2. Event screening for in-depth analysis

2.2.1. Development of a logic tree of the event



2.2.2. Screening of events for in-depth analysis
The occurrences 1, 10 and 11 are abnormal.

Occurrence 11. Blocking failure to close bypass valves due to pressure decreased in MSH less than 57 kgf/cm2 in a remote mode. This occurrence is safety related because of it is an initiating event for «secondary circuit leakage in a isolated part» accident.

2.3. Determination of occurrence direct cause

The direct cause of blocking failure was lack of control algorithm YBS-12 while all the bypass valves regulators being in a remote mode.

2.4. Determination of occurrence root cause

The root cause of YBS-12 blocking failure was absence of a routine procedure for YBS-12 blocking test. It is classified as poor development of technical documentation by I and C perssonnel.

2.5. Determination of corrective measures

Corrective measures on direct causes	To change bypass valves governors'control algorithm with the purpose to ensure bypass valves complete closure on pressure decrease less than 57 kgf/cm2 in any working mode.
Corrective measures on root causes	1. To agree upon new control algorithms of technological equipment blocking with the Main Technologist Service to check their compliance with design technical requirements. 2. To develop the «Programme on Implemented Technical Solutions Review» at Zaporozhye NPP. 3. To carry out a revision of routine programme for bypass valves test.

2.6. Common cause failure characteristics

In this case, all the bypass valves common cause failure (CCF) can be classified as bypass valves structural/functional failure, i.e. that the present control sub-system revealed to be inoperable in this mode. At the level of the direct cause analysis the human factor influence is not observed.
However, event root causes are connected with the improper technical documentation development and checking by the plan management.

3. Example of analysis of operational event at Khmelnitskaja NPP.

Event title: Inoperability of the safety function of the high pressure boron injection systems.

Event date: 26 February 1991

INES rating: Level 2

3.1. Description of the event:

3.1.1 Initial status of the plant.

On 26 February 1991, Unit 1 was operating at nominal ~full power. The first (night) Shift were detailed to carry out a routine test programme on equipment in the 1st safety train. During the test it was found that the valve, on the delivery side of the high pressure boron injection pump, did not operate as expected.

3.1.2 Brief description of the event:

1. As a result of a short reactor outage, for maintenance and for reactor cooling, there was a requirement to electrically disconnect valves TQ13,23 and 33S07 under procedure Reactor Department 061,N388 also TQ14,24 and 34D01.

2. There is a maintenance procedure for disconnection of supplies to prevent operation of high pressure boron injection pumps, procedure number Reactor Department 061 Operating Instruction 88. This was carried out at 22.35 on 4 February 1991. The requirements of the procedure covered the disconnection of the supplies to the valves only.

3. On 7 February 1991 at 22.00, testing of the 1st and 2nd Protection trains were technically/ logic tested and by 22.35 all three trains had been tested. The unavailability of the high pressure boron injection systems was not found. This work had been carried out to a schedule but no procedures for tests existed.

4. On 10 February 1991, the actuators of valves TQ13,23 and 33S07 were re-assembled but electrical supply cables not reconnected. The indication in the control room indicated that the valves were closed. During 09.30 to 13.10, safety system tests were carried out which did not reveal that there were valves electrically disconnected.

5.On 11 February 1991 at 21.00, the reactor was at minimum controllable level.

6. During 26 and 27 February 1991, with the reactor at full power, the plant personnel discovered that the high pressure boron injection system was not available.

7. On 26 February 1991, during routine testing, by operations personnel, it was discovered that valve TQ13S07 was not controlling. Local inspection showed that power supplies were not connected. At 06:00, the cables were reconnected and the valve tested, operationally.

8. At 11.40 on 27 February 1991, it was discovered that valves TQ23 & 33S07 were also

disconnected. At 14.50 both systems were reconnected and satisfactorily tested. The availability of the 3 high pressure boron injection systems was re-established.

3.1.3. Final status of the plant:

Unit 1 remained at full power throughout this event. By 14.50 on 27 February 1991, all high pressure boron injection systems were fully operational.

3.2. Actual consequences of the event under each of the safety attributes

a) Off-site impact:

Impact on the public:	No
Impact on the environment:	No

b) On-site impact:

Impact on plant personnel:	No
Impact on plant safety:	No

c) Degradation of defence in depth: Yes

The event consequences lie solely in the area of defence in depth. Deficiencies in procedures and personnel led to the Unit operating without any high pressure boron injection systems for 16 days and would not have fulfilled its emergency function during that period.

3.3. Selection of occurrences for in depth analysis

The analysis of the event revealed four occurrences, these were considered, and one selected for in depth analysis.

Occurrence 4 - Personnel
Operator fails to interpret observed valve position indications.

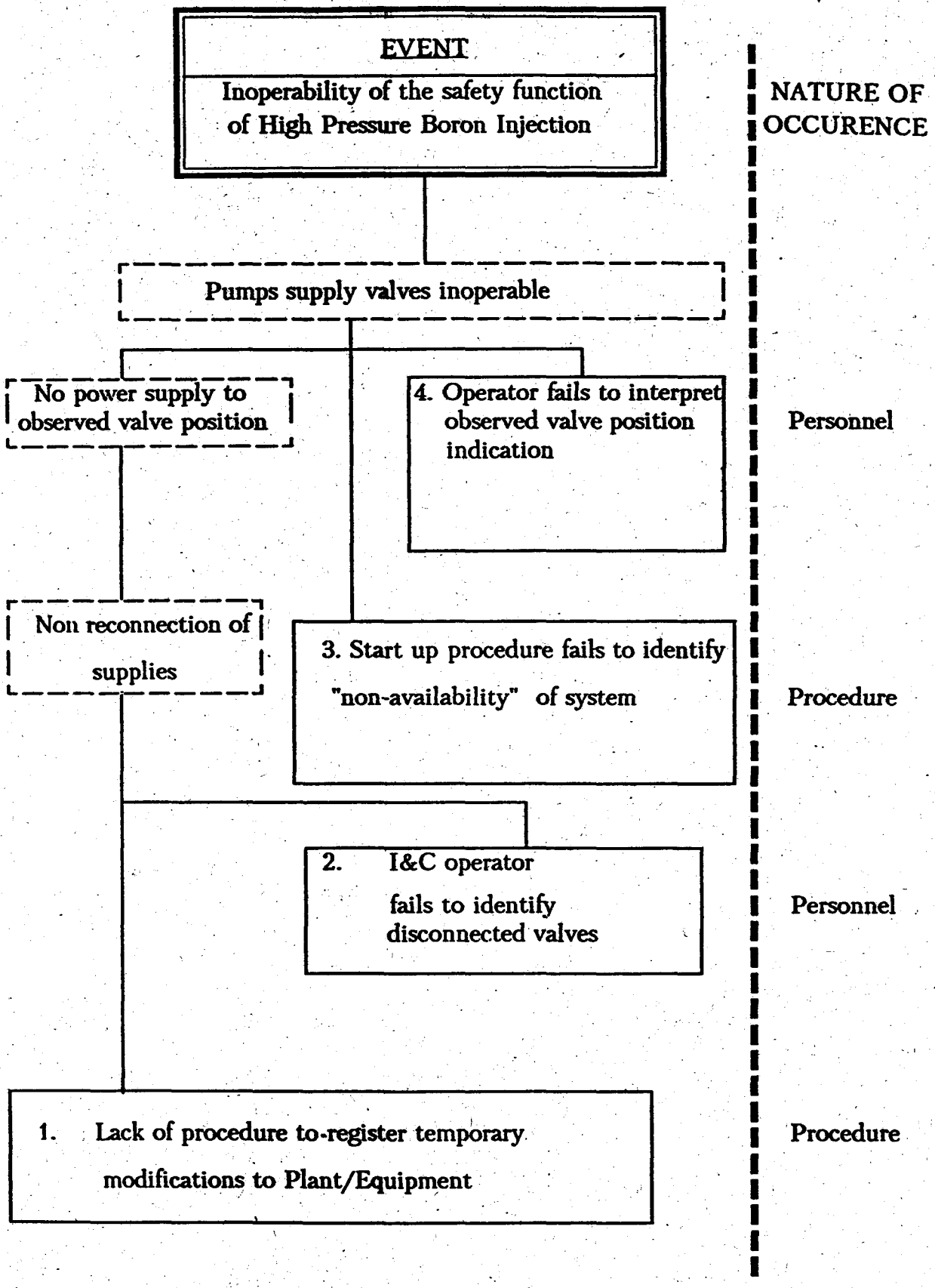
3.4. Identification of direct causes of the occurrences:

1) Operators approach to verifying completion of test is inadequate. The valve operation of the event is similar to other operations in the control room and it would be expected that the operator would be familiar with the interpretation of observed indications.
2) Refresher training does not give sufficient emphasis to attitudes for operating plant equipment. The important aspect of attitudes of staff had not been considered in training programmes in any significant way.

3.5. Root causes:

1) Supervisors are not encouraged to carry out surveillance of staff competence and performance. There appears to be no guidance in terms of ensuring staff are performing to the normal requirements of their tasks.

3.3.1. Establishment of the logic tree of occurrences.



2) There is inadequate demonstration of the requirements for operational behaviour and competence by management. For the conduct of staff, consideration is not given to the behaviour expected by operational staff and others.

3.7. Corrective action:

1) Consider further training programme. Operating staff need to be aware of the interpretation of observed indications of common systems within the control room.
2) Include attitude aspects and importance of diligence in future training programmes.
3) Managers should provide guidance to supervisors and provide support for surveillance. Supervisors should be monitoring the performance of their staff and this guidance should be provided by management.
4) Regular meetings with supervisor groups would provide a forum to develop the necessary competencies for operators and other staff. It is important the staff understand what is expected of the in terms of standards of behaviour to ensure safe operations.

3.6. Characteristics of CCF.

In this case, operator fail to identify right positions on the valves, what had lead to CCF classified as failuere due to human error during regular system test perfoming. Here the human factor is the source of CCF on the level of direct cause of the occurrence.

4. CONCLUSIONS

The present study demonstrates topical importance of CCF analysis, their timely identification and development of necessary measures for preventing such failures occurrence.

Safety significance

In both examples common cause failures had directly affected plant safety followed by safe operation limits and conditions violations .At Khmelnitsk NPP there was completely lost for 16 days safety function of emergency coolant supply into reactor, being carry out by ECCS. This safety function is necessary to be carried out in the most accidents with high-frequency initiating events including «blackout», »a small leak in primary circuit», »transients with primary circuit heat removal violation» etc..

At Zaporozhje NPP an initiating event-loss of feedwater had evolved into an accident initiating event-large leak in secondary circuit in an isolated part. This event is a design-basis accident and considered in reactor facility feasibility study. Taking into account possible accident succession we conclude that this event is very dangerous because of possible failure any of four bypass valves to close during leak localization, that could lead to an accident with more severe consequences.

Role of the human factor

In both examples common cause failures were connected with personnel errors, being the root cause of the event at ZNPP while at KhNPP - the direct one. It should be noted that in both cases CCFs were results of non-adequate documentation, lack of necessary control of manuals and routine programmes development.

That is why the corrective measures are mainly aimed to improve technical documentation and process of its development. At the same time corrective measures on personnel qualification upgrading aimed to prevent CCFs reoccurences still have not been provided.

It is necessary to emphasize that at the present time in Ukraine there are no any spesific provisions or methodics for identifications, analysis and development of corrective measures to present common cause failures.

At present time the real contribution to the study and solving of this problem could be the following:

- in-depth study of all events with the CCF,

- to criate methodic for CCF analysis and corrective measures development using national and foreign practices,

- to arrange some seminars on CCF analysis.

United States

PWG1/ETF
September 1994

TASK 4:
Human Factors Related Common Cause Failures

United States Response To:

The Organization For Economic Cooperation and Development (OECD)
Nuclear Energy Agency (NEA)
Steering Committee For Nuclear Energy

Committee On The Safety Of Nuclear Installations
Expanded Task Force Of Principal Working Group No. 1 (PWG-1)

Task No.4:

Human Factors Related Common Cause Failures

Introduction

This report was prepared in response to the Working Plan on Human Factors Related Common Cause Failures agreed upon by the PWG-1 members at the 9th meeting of the Expanded Task Force NEA/SEN/SIN/WG1 (94)3 held March 16-17, 1994. This report represents the contribution from the United States to Subtask 1, "Event Analysis" and describes a testing and maintenance-related event.

Definition of Common Cause Failure

For purposes of this report, a common cause failure is defined as an event in which two or more components must be affected by a single, shared cause and this cause must not be the failure or functional unavailability of another component. (Adapted from NUREG/CR 4780, Vol. 1, Procedure for Treating Common Cause Failures In Safety and Reliability Studies, January, 1988, p. 2-8).

Event Description

1. **Title of Event:** Inadvertent Capping of Containment Pressure Sensing Lines

2. **Event Summary:** On March 23, 1994, operators at a PWR in the United States were preparing to bring the reactor for unit 1 back on line following a scheduled refueling outage (actually progressed from Mode 5, Cold Shutdown, to Mode 3, Hot Standby). While attempting to vent containment, pressure indications in the control room did not lower as expected. After entering the containment, investigation determined that the four sensing lines of eight safety-related containment pressure instruments were capped-off inside containment. As a result of capping these lines and inoperability of these eight instruments, the control room did not have an accurate indication of containment pressure and several automatic actuation functions of the Engineered Safety Features (ESFs) were inoperable. The blocked lines caused the inoperability of the following ESFs: Safety Injection on a Containment Hi Pressure Signal; Containment Spray Actuation; Phase B Containment Isolation; and Main Steam Isolation Valve isolation on Containment Hi Hi Pressure Signal.

   Since the core was refueled and the unit had been shut down for six months, the decay heat was low and the safety significance of the event was reduced. The incorrectly capped lines were uncapped and normal system functions were restored.

   The sensing lines were capped on March 19, 1994, by a maintenance crew using a "work list" that they believed described work that was "minor maintenance" (the crew thought they were to complete "housekeeping" tasks which included making certain that foreign materials would not obstruct containment penetrations). However, the crew actually performed unauthorized work that was safety-related, required a "formal work request," and resulted in a permanent plant configuration change (the crew capped containment sensing lines that should not have been capped). The human factors-related, common cause failure in this event is a management/quality assurance deficiency (failure to differentiate between minor maintenance and major, safety-related work that results in a permanent change to the plant).

   The NRC determined that the utility was in violation of 10 CFR Part 50, Appendix B, Criterion V, "Instructions, Procedures, and Drawings," which requires, in part, that activities affecting quality be prescribed by and accomplished in accordance with documented instructions, procedures, or drawings of a type appropriate to the circumstances. The violation was assessed a civil penalty.

   A more detailed analysis of the event follows as item 2 under Systematic HF Analysis, Using Different Methods. The analysis identifies the sequence of events that led to the incident, the human factors-related common cause, contributing causes, and specific multiple failures.

Systematic HF Analysis Using Different Methods

1. **Level 2 Root Cause Investigation:** The plant applied an analysis method to follow up the event. Called a "level 2 root cause investigation," the plant assembled an investigation team to conduct a detailed analysis of the event. The analysis included creating a list of all lines that were required to be open inside the containment and inspecting both unit's containments; interviewing the maintenance crew members who installed the pipe caps to determine the quantity and location of the caps that were installed; reviewing and verifying labelling of all penetrations inside containment; adding a verification step in the containment close out procedure; and strengthening minor maintenance restrictions on plant changes.

2. **Human Performance Investigation Process:** To help analyze this event, the NRC Human Factors staff applied, in part, a standard NRC investigation process used when investigating human performance related events at nuclear power plants. The process is called the Human Performance Investigation Process (HPIP). A complete description of HPIP is contained in a three volume NUREG/CR-5455, Development of the NRC's Human Performance Investigation Process (HPIP), October, 1993.

   To explain the event, the staff used three techniques contained in HPIP, "Barrier Analysis"; "SORTM" (Stimulus, Operation, Response, Team Performance, and Management); and "Events and Causal Factors Charting". Barrier Analysis is a method of identifying the events that, if avoided, will prevent the incident from happening or might lessen the consequences of the incident. A "barrier" can be any physical boundary, natural occurrence, human action, or administrative control that could keep the event from occurring. SORTM is paper and pencil activity that provides basic questions similar to those that an expert investigator in human performance might ask during an event investigation. The questions are presented in a "Yes/No" logic tree format with the answers to the questions leading the investigator to those human performance areas most likely to have contributed to the human error during the incident. The Events and Causal Factors Chart is a graphic presentation of the sequence of events that led to incident/accident and the causal factors for those events. The chart helps the investigator understand the event's progression, identify gaps and inconsistencies in the information, and explain the event to others.

   Following are the Sequence of Events Chart (Figure 1) and Causal Factors Chart (Figure 2) for the capping event, which contain the results from SORTM and Barrier Analysis performed by the NRC staff.

Initial Conditions:
Reactor at 0% power

Conducting materials condition corrections for containment closeout prior to restart

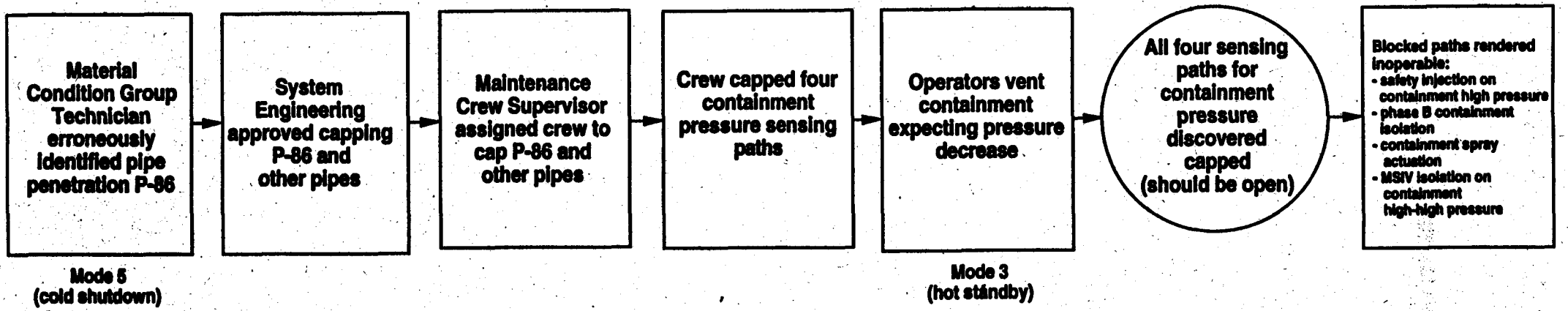


FIGURE 1: Sequence of Events Chart

Initial Conditions:
Reactor at 0% power
Mode 5 (cold shutdown)

Conducting materials condition corrections for containment closeout prior restart

Broken Barrier

Broken Barrier

Broken Barrier

Broken Barrier

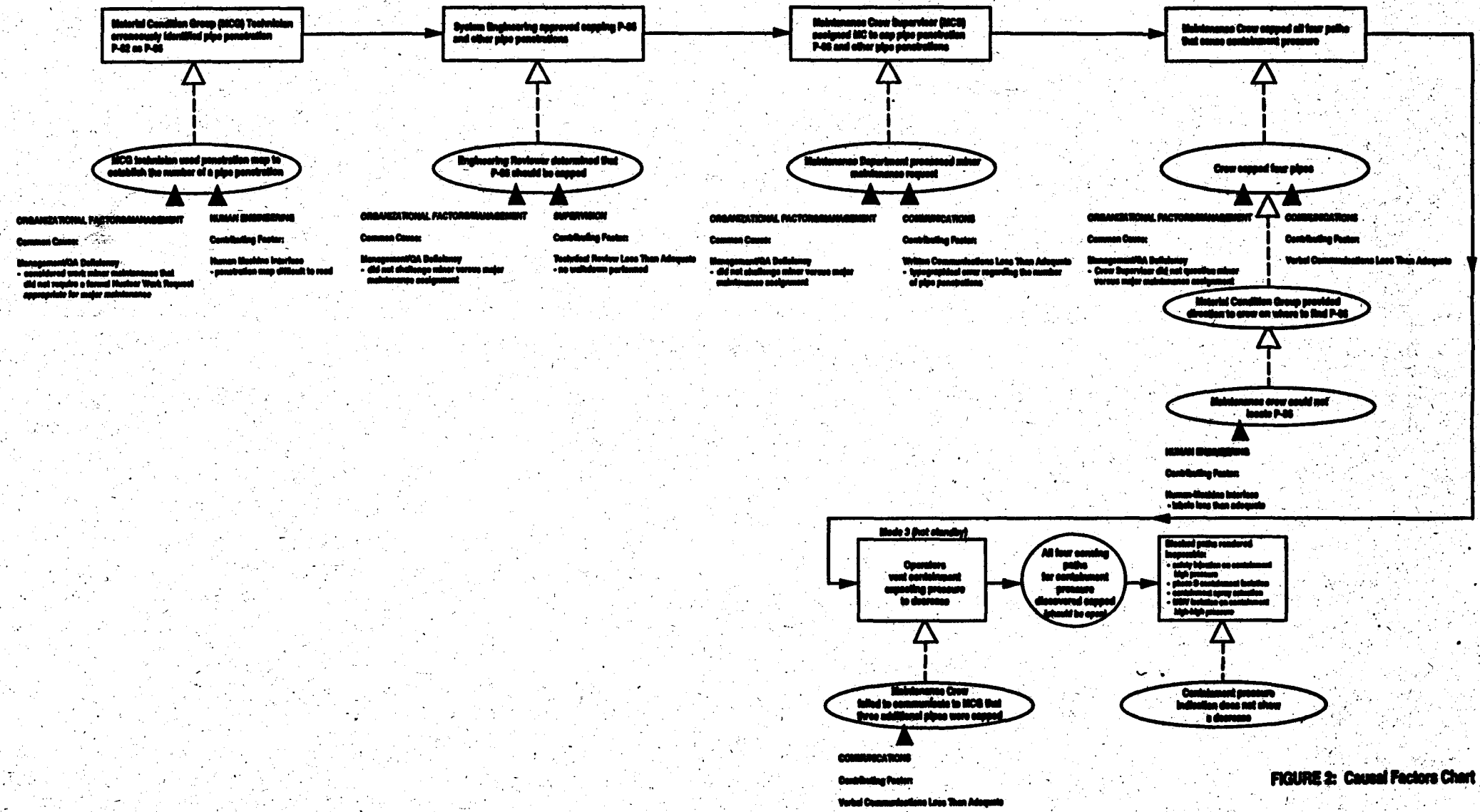


FIGURE 2: Causal Factors Chart

Actions Taken, Lessons Learned, Improvements

1. Actions Taken: The following immediate actions were taken by the plant to correct the inadvertent pipe capping:

   a. the pipe caps were removed from the unit 1 containment pressure sensing lines.

   b. both units were inspected and the lines in systems that were required to be open to containment pressure were verified to be open.

   c. interviews were conducted to determine the number and location(s) of the caps installed. Walkdowns were performed to determine that no additional caps were incorrectly installed.

   d. maintenance work activities were restricted to a formal work request process in the auxiliary building and in units 1 and 2 containments.

2. Lessons Learned: The following are lessons learned by the plant from the event:

   a. containment penetrations inside containment must be properly labelled.

   b. communications between work crews and supervision must be improved.

   c. supervisory follow-up of work activities must be improved.

   d. QA of work lists required for capping activities must be improved.

3. Improvements: The following are long term corrective actions taken by the plant in response to this event:

   a. labelling of penetrations inside units 1 and 2 containments reviewed; all penetrations will have appropriate labelling.

   b. the plant's operating department changed plant procedure to ensure that containment penetrations or associated lines are verified open/uncapped before plant heat up.

   c. the plant procedure for using a work request was revised to clarify and strengthen minor maintenance restrictions on plant changes.

Possible General Conclusions

1. common cause failure events that have occurred in U. S. nuclear power plants can be identified that have as their common cause, a human factors-related reason (e.g. poor written/verbal communication, less than adequate procedures, less than adequate supervision).

2. the Human Performance Investigation Process is an effective process for events and causal factors charting and identification of human factors-related common cause failures.