

**Restricted**

**NEA/CSNI/R(95)10/PART1**



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

**OLIS : 10-Jan-1996**  
**Dist. : 11-Jan-1996**

**Or. Eng.**

**NUCLEAR ENERGY AGENCY  
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS**

**NEA/CSNI/R(95)10/PART1**  
**Restricted**

## **HUMAN FACTOR RELATED COMMON CAUSE FAILURE - PART 1**

### **Report from the Expanded Task Force on Human Factors**

#### **Principal Working Group No. 1 Meeting - November 1995**

**27763**

Document complet disponible sur OLIS dans son format d'origine  
Complete document available on OLIS in its original format

**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

**TABLE OF CONTENTS**

**EXECUTIVE SUMMARY.....4**

**1. INTRODUCTION.....5**

**2. SCOPE.....5**  
2.1 Definitions of HF related CCF provided by participating countries.....6

**3. SUMMARY OF CONTRIBUTIONS .....8**  
3.1 Sub-Task 1: Event analysis.....8  
3.2 Sub-Task 2: Predictive techniques ..... 16

**4. CONCLUSIONS .....20**  
4.1 Conclusions of sub-task 1.....20  
4.2 Conclusions of sub-task 2.....21

## EXECUTIVE SUMMARY

On its 13th meeting in September 1993 the Principal Working Group 1 (PWG1) proposed to the Expanded Task Force on Human Factors (ETF) to deal with Human Factor related Common Cause Failures (CCF). Preliminary investigations performed by Germany identified the interest of an in-depth evaluation. In March 1994 the detailed content of the task was defined.

The objective of the task was the identification of root causes of Human Factor related Common Cause Failures and lessons learned. In particular, it should be evaluated whether there are:

- typical areas of this type of failures,
- methodologies for pro-active identification,
- and possible measures to prevent them.

To meet the objectives the task was divided into two sub-tasks:

- event analysis and
- predictive techniques.

Each of the 14 participating countries contributed to one of the sub-tasks: 10 to sub-task "event analysis" and 4 to sub-task "predictive techniques".

The contributions were received by February 1995. The draft report was issued end of April for comments. The final draft was discussed at the ETF meeting September 1995. After approval by the PWG1 the report was finished end of 1995.

The sub-task "event analysis" includes two different kinds of contributions. Twenty-eight events from different countries are discussed in detail. In addition, some countries provided a general report on the treatment of HF related CCF in the respective country.

The results of the task can be summarized as follows: the two approaches covered many aspects of plant operation and maintenance. One main finding is that HF related CCF may occur in all safety related systems. A special accumulation of HF related CCF in one system could not be detected. Also, a large variety of tasks were reported that caused these failures. The root cause analysis showed no specific contributing factor. Consequently, simple measures to prevent HF related CCFs could not be derived.

Some events reported to the sub-task "event analysis" had significant impact on plant safety. This underlines the potential importance of HF related CCF. The in-depth analysis revealed two areas of concern: latent failures and "minor" tasks. Latent failures can occur if functional tests or requalification of equipment after maintenance are not representative regarding the loads on real demand. "Minor" tasks have no safety significance and thus require less preparation, supervision and quality assurance. The event analysis shows examples that safety related works have been erroneously treated as "minor" tasks. Thus failures in these "minor" tasks were not detected in time and caused serious safety system degradations.

The sub-task "predictive techniques" was covered by 4 countries. The different methodologies presented, analyse the safety significance of potential human failures. The relevant actions are identified and the sequence of actions described. Some methodologies take into consideration external contributing factors like environmental impact on the acting person. The methodologies developed are based on probabilistic analysis (PSA) or a detailed investigation of personnel tasks taking into account possible

failures and their effects on component behavior and plant safety, respectively. The "predictive techniques" described are in use in these countries and show practical results i.e. modifications in plant operation and procedures. Sub-task 2 demonstrates that there are tools available that can predict possible critical actions but that they require significant efforts.

## 1. INTRODUCTION

At the second meeting of the Expanded Task Force on human factors (ETF) on September 18, 1990, Germany volunteered to scan the Incident Reporting System (IRS) database to identify possible topics for further work. The evaluation covered about 200 events. A similar scan was performed by an IAEA consultant group about one year later. The main topics identified for further work were:

- single human failures resulting in significant degradation of safety systems and,
- human factor related common cause failures.

The first topic was covered by an IAEA consultant group in November 1993. During its 13th meeting in September 1993 the Principal Working Group 1 (PWG-1) agreed on the proposal of ETF to deal with human factor related common cause failures (defined as task 4). Germany volunteered to lead the task and to compile the report. At the March 1994 meeting, ETF members discussed the detailed content of task 4. The task was divided into two sub-tasks:

- Sub-task 1 "event analysis" and,
- Sub-task 2 "predictive techniques" used to prevent HF related CCF.

## 2. SCOPE

The objective of the task was the identification of HF related CCF and lessons learned. In particular, it should be evaluated whether there are:

- typical areas of this type of failures related to specific systems or human tasks (like - operation and maintenance),
- methodologies for pro-active identification,
- and possible measures to prevent these failures.

The two-fold strategy with event analysis and predictive techniques highlights the topic from two different points of view. Sub-task 1 covers the more re-active view, i.e. the analysis of a HF related CCF that has occurred, whereas in sub-task 2 pro-active techniques are presented, mainly to prevent safety significant CCFs. Within both sub-tasks, areas of concern should be identified. These areas cover specific systems or components which may be susceptible to HF related CCF, as well as types of human tasks in a NPP including operation, maintenance and contractor work. In sub-task 1 the actions taken after the events and the lessons learned should be presented. The methodologies discussed in sub-task 2 should have practical results like implementation of modifications.

To address adequately these aspects and to assure comparable contributions of different countries, the sub-tasks were structured as follows:

Sub-task 1:

- Event description
- Systematic HF-analysis
- Lessons learned and actions taken
- Possible general conclusions

Sub-task 2:

- Description of technique(s)
- Example of application
- Description of special areas of interest like detection, prevention, mitigation, and recovery actions
- Possible general conclusions

General conclusions may be drawn from a representative set of events. Therefore, the events analysed should be as much representative for identified HF related CCF in the participating countries as possible. Ideally, the general conclusions derived from the event analysis sub-task should be similar to those drawn from the analyses using predictive techniques.

## **2.1 Definitions of HF related CCF provided by participating countries**

Since at the beginning of the project the term HF related CCF was not clearly defined. Some countries provided their working definitions:

*Belgium:*

(A HF related common cause failure is an) 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.

*Finland:*

Common cause failures 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.

Observed longer time frames must be considered when failures are not detected in periodic tests or other planned checks.

*United Kingdom:*

Human error dependency: Dependency exists whenever probabilities of actions or errors (or a series), are linked more closely than in random events.

Nature of the failure deriving 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.

*Ukraine:*

Common cause failures: these are failures of some elements in one or several systems which result of internal or external effect, component failures or human errors during system design, manufacturing, installation and/or operation.

*United States:*

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 (in this case the cause is human error) and this cause must not be the failure or functional unavailability of another component. (from NUREG/CR 4780, Vol. 1). The definitions cover a wide range of aspects related to CCF. The main differences between these definitions are:

- treatment of dependent failures,
- consideration of non-simultaneous failures (time dependency) and
- consideration of potential failures of systems and components.

These differences depend mainly on various views on common cause failures. With respect to the human factor related part of this task, these differences have no significant influence. The main emphasis during this task is laid on the human factor related analysis. Therefore, any event presented by the participating countries was considered taking into account the country's definition. A summary of the definitions may be given as follows:

A human factor related common cause failure is:

- a set of identical human failures due to the same cause or,
- a common cause failure of systems or components due to the same human factor related cause.

### 3. SUMMARY OF CONTRIBUTIONS

#### 3.1 Sub-task 1: Event analysis

##### *Belgium:*

The entire Belgium event database was screened to identify events including human factor related CCF. The screening was performed using codes and additional check of the event reports. In total, 17 events were identified. All 17 events identified were analysed regarding the mode of operation, the type of activity which resulted in the deficiency, behavioral factors, the type of dependency, the way of discovery and the corrective actions. These analyses are contained in the report. In the following one example is presented.

In the course of the start up of the plant, it was discovered that the isolation valves in each of the three high pressure safety injection lines to the cold legs of the primary circuit were in closed position. Their power supplies were disconnected. The total unavailability of the high pressure injection system lasted 3 days. The deficiency was detected during a non-programmed independent check on the line up of safety systems.

One day before start up, a leaktight test of the check valves in the high pressure injection system was performed. The test requires that the isolation valve should be closed but not disconnected from the electrical power supply. It seems that the disconnection was performed in analogy of the isolation valves to the primary circuit hot leg. The test procedure did not provide specific instructions to restore or to verify the proper line-up of the system after the test. The day following the completion of the test, the operators verified twice the line-up of the safety injection system as instructed in the operating procedures which, however, did not specify the required position of the valves.

Several successive human errors can be identified in this event:

- omission to re-establish the required line-up of the system after the leaktightness test,
- disconnection of the valves' electric power supply without instruction,
- failure to verify the system line-up during verification as requested by the procedure applied to change technical specification modes during start up.

All these errors can be characterized as operating deficiencies.

The conclusions drawn from the analyses of all events show that the outage is the mode of operation which contributes most. Eleven out of 17 events occurred in the outage phase, 5 of these during start up. Thirteen events resulted from maintenance or testing tasks. The analysis of the behavioural factors showed the importance of omission errors (7 out of 17) which were often caused by deficiencies in the procedures. Other identified behavioural factors include lack of knowledge (4), confusion errors (2), and lack of attention (2). For the type of dependency four categories were identified: 7 events resulted from a single human error conditioned by a common instruction or procedure, 5 events were related to the failure of redundant components affected by a common human error induced condition, 3 events contained repeated human errors on redundant or similar components, and 2 events occurred due to the existence of a common component which was affected by human error resulting in the failure of redundant subsystems. Scheduled periodical tests detected most (9) of the events. In 5 events, the deficiencies occurred on demand and 3 deficiencies were detected by chance.

The corrective actions cover a broad spectrum of measures to prevent recurrence of the events. Some of them are listed below:

- reduce perception of time pressure during start up
- more explicit check-off lists for required system configuration
- improve configuration control procedures during outage
- introduce redundant and diverse verifications to cope with possible omission errors
- avoid common components in redundant safety systems; give special attention to such components in existing designs

*Canada:*

Operating Policies and Principles (OP&Ps) are referenced in the reactor operating license. They contain not only general safety principles, but also define safety parameters and their numerical values for the operation of the nuclear power plant. The event described highlights the difficulties to implement the OP&Ps into detailed purchase orders.

In CANDU reactors gadolinium nitrate and boric oxide are used as neutron absorbers in the moderator. The concentration of neutron absorbers in the moderator is safety significant because a small change in concentration in coincidence with other failures (e.g. LOCA) can result in a sudden increase of power. To ensure that new shipments of gadolinium nitrate or boric acid meet the required specifications, these must undergo quarantine so that samples could be taken and forwarded for analysis. The chemistry unit of the NPP issued this requirements in a "note to file". In the event, two separated purchase orders, one for gadolinium nitrate and one for boric oxide, were placed. The purchase orders did not stipulate the requirements to quarantine, inform the chemistry unit or to analyse samples. They only stated that correct isotopic and chemical purity were required. The gadolinium nitrate as well as the boron oxide were both not quarantined and even the purity was not verified.

The chemistry unit felt that a "note to file" memo was sufficient to ensure that the OP&Ps are met taking into account the low shipment rate and sufficient experiences before. The analysis of the event revealed several causal factors. Four main factors were pointed out:

- Work practices
- Resource Management
- Written communication
- Managerial methods

The actions taken after the event focused on the identified deficiencies.

*Germany:*

The German contribution deals with a generic issue regarding the malfunction of the thermal actuation mechanism of fire dampers. These fire dampers are part of the fire protection concept of German NPPs which consists of a combination of structural, equipment-related, and administrative measures. The fire dampers installed in ventilation ducts are part of the structural fire protection measures. They can be closed manually, remotely by electrical actuation, and by thermal actuation. In the events described only the thermal actuation was affected.

The first malfunction of a thermal actuation mechanism was detected during the annual inspection of fire dampers. The visual inspection of the inner parts of the damper revealed deficiencies of the thermal actuation mechanism. Subsequent investigations showed similar findings in the same NPP and other NPPs. It was also found that different types of fire dampers of the same manufacturer and dampers of other manufacturers were affected.

The root cause of the first event reported was analysed using an adopted HPES method. The analysis showed two main contributing sequences:

- deficiencies in design, fabrication, installation, and
- deficiencies in licensing and maintenance programme.

The analysis of the deficiencies in design, fabrication, and installation revealed that:

- the design of the thermal actuation mechanism was not robust enough,
- quality assurance deficiencies existed during fabrication and installation, e.g. the functional tests of the thermal actuation mechanism after installation might not have been performed, and
- the maintainability of the dampers was poor.

The analysis of the deficiencies in the licensing and maintenance program showed that:

- licensing was performed in sub-tasks by several certification agencies and that no test of the entire function of the damper was performed,
- ageing aspects were not considered in licensing, and
- in-service inspections of the thermal actuation mechanism were not performed according to the recommendations of the manufacturers.

All these deficiencies contributed to the significant amount of fire dampers not to close by actuation of the thermal actuation mechanism. An important contributor may be the assumption that the thermal actuation mechanism is of high reliability because it acts passively and that it is of minor safety significance. The main action taken after the events is to include the thermal actuation mechanism checks in the in-service inspections.

*Italy:*

Two events from Italian NPPs were reported with respect to HF related CCF. Common to both events is the combination of unexpected weather conditions and inadequate plant control and practices.

#### Event 1:

During an unusual lengthy period of bad weather it was discovered that the coolant inside the radiators of one of the four emergency diesel generators was frozen. A test of the coolant of the other diesel generators revealed that the concentration of the anti-freeze additive in the coolant was insufficient.

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

- insufficient testing frequency of the freezing point of the diesel generator coolant,

- diesel generator coolant inventory was maintained, in some cases, without supervision of the plant personnel and using only demineralized water, and
- lack of knowledge of some diesel generator 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 2:

During similar weather conditions like in the first event described, a spurious actuation of the fire suppression system occurred at one of the unit transformers which resulted in turbine trip and subsequent reactor scram. The spurious actuation of the sprinkler system was caused by depressurization of the fire sensing line installed around the transformer. The depressurization occurred due to cracks in a drain pot installed at the line. Because of the cold weather the water accumulated in the drain pot had frozen and cracked the pot. The drainage of the pot was not performed at regular intervals and was not covered by a specific procedure. To prevent the recurrence of the event, a number of measures was taken:

- The quality of the compressed air used in the sensing lines was improved, using instrument air instead of service air. The plant instrument air has a very low dew point.
- The drain pots were modified by adding 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.

*Japan:*

During a steam generator tube rupture event, the operators tried to open the pressurizer relief valves in order to reduce the reactor pressure in accordance with the operating instructions. Both pressurizer relief valves failed to open because one valve of the pilot valves' common air supply system was closed. There was no redundancy provided so that this closed valve led to the common cause failure of the pressurizer relief valves. The control room staff managed the event appropriately although the operating procedures did not contain instructions for such malfunctions.

The investigations identified a failure during maintenance causing the closure of the air supply valve. An operator assumed that this valve was not used commonly to operate the pressurizer relief valves but belongs to an auxiliary air system. Therefore he closed the air supply valve based on the assumption that it is normally not used.

Several countermeasures were taken to prevent the recurrence of the event:

- Improvement and intensification of periodical inspections
- Improvement of management and maintenance system
- Improvement of operating manual

*Korea:*

Two events are addressed in the Korean contribution which both led to a loss of residual heat removal (RHR) during mid-loop operation.

Event 1:

One RHR pump was in operation while the reactor water level was maintained at 2 cm above the center line of the hot leg. At that time, the refueling water storage tank was under maintenance. Due to a maintenance error the "low-low" level alarm was unintentionally annunciated. This caused the switch over of the operating RHR pump to the sump suction mode, which resulted in the loss of RHR. The temperature in the hot leg increased within 8 minutes to 95°C and the water level dropped 12 cm below the hot leg center line. Attempts to start the second RHR pump failed due to the insufficient suction pressure. The reactor pressure vessel water level was maintained with aid of the charging pumps. The RHR system was lined up again and vented. It was operable about 50 minutes after starting of the event.

Event 2:

The event was caused by a delayed response of a Tygon hose level indication during a draindown operation. Both RHR pumps were lost due to oscillations in flow and discharge pressure. The cause was a water level decrease in the reactor pressure vessel resulting in insufficient suction pressure of the RHR pumps. The level indication of the Tygon hose indicated an appropriate level in the pressure vessel. The actual level was some centimeters below the indicated level. This led consequently to the loss of RHR.

Detailed investigations followed both events. The main lessons learned with respect to human interactions to reduce CCF were:

- Communication between maintenance and operation staffs must be strengthened.
- Before starting of maintenance activities, the system configuration must be reviewed.
- Recovery procedures after loss of RHR should be implemented in the operating procedures as well as in operator training.

*Russia:*

The prevention of human induced failures in Russian NPPs is performed by measures in different areas. The evaluation of operating experience shows that the number of personnel errors reduces when the NPP operates longer than 3 - 4 years. If suddenly more failures due to personnel error occur after years of smooth operation, these may be explained by overestimation of personnel experience or capabilities, by degraded monitoring, or by inadequate practical measures taken by the management or engineering support services. The failures occurring can be divided into two parts: failures depending on the person making an error and failures not depending on the person.

It is pointed out that an appropriate organisation is important to prevent failures. This includes provisions taken for emergency situations. Analysis of operation personnel errors allows to conclude that most errors are due to the lack of a reliable system for specialist selection and training, taking into account psycho-physiological capabilities, psychic and spiritual qualities of the persons. Lack of discipline and responsibility are the most frequent causes of failures due to errors of staff operating auxiliary systems and working in maintenance service.

In Russia, a NPP technical support center was established to encourage efforts on following areas:

- development of structures to provide experts in crisis situations;
- development and upgrading of a nuclear information system;

- enforcement of communication between NPPs and supporting companies;
- development of standards, codes, instructions, methodologies, and regulations;
- adoption, at a governmental level, of a programme for the development of a safe and effective NPP operation system.

Further improvements are necessary in work organisation.

*Slovenia:*

In total, 23 Slovenian events were analysed with respect to human failures. The most frequent mechanisms of human malfunctions were knowledge-based and skill-based errors. At the time of the lowest level of operator's cognitive availability, errors like "not taking into 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 effective behavioural patterns and cognitive as well as sensorimotor availability of operators show that the highest number of knowledge-based errors was at the time of the lowest level of cognitive availability. The highest number of skillbased errors was at the time of the lowest level of sensorimotor availability. In addition to these internal causes, several external factors affected the human behaviour like inadequate organisational model and inadequate training. The results of these analyses were also compared with results from other field measurements of human availability and fitness for duty.

*Ukraine:*

In the Ukraine, events are analysed using the IAEA-ASSET methodology. A review of the recent years was performed to identify common cause related events. In 1992 two events, in 1993 eight, and in the first half of 1994 four events occurred involving CCF. As examples for the analysis, two events are presented in the first part of the contribution. A third event from the second half year of 1994 was reported additionally.

Event 1:

During power operation, high pressure feedwater heater group A was in operation, group B was in maintenance and the related parts of the safety protection system were switched off. Due to an unintentional actuation by the maintenance personnel, a high level alarm of heater B was annunciated. Consequently, the turbine driven feedwater pumps and one turbine generator were switched off. The main steam pressure rose to the set point of the relief valves. According to the operation manual the operator manually scrammed the reactor. During the further event sequence, a loss of automatic control of all four bypass valves occurred. These valves remained fully open. Thereafter, the main steam isolation valves were automatically closed and the emergency core cooling system and the emergency feedwater system were actuated. About 3 minutes later, the operators closed the bypass valves from the control room. This action terminated the transient and the operators began to restore the systems.

The occurrence of the failure to close off the bypass valves was analysed in depth with the ASSET methodology. The direct cause of the blocking failure was a lack in the control algorithm while all the bypass valve regulators being in a remote mode. The root cause was the absence of a routine procedure for a control algorithm blocking test. It was classified as poor development of technical documentation by

I&C personnel. The corrective measures included the modification of the control algorithm to ensure the valve closure in all modes of operation. Additionally, with special respect of the root cause, supervisory methods to check modifications were developed and a revision of the routine valve test programme was performed.

Event 2:

At nominal power, the shift carried out a routine test programme on one train of the high pressure boron injection system. During the test, it was detected that one valve on the discharge side of the injection pump did not open. Subsequent investigations showed that the respective valves of the other two redundant trains did not open either. The valves were disconnected from the electrical supply, i.e. the reactor operated with the high pressure boron injection system totally unavailable. The reactor had been started up after outage about 2 weeks before.

During the outage maintenance, work was performed on the three redundant trains of the high pressure boron injection system. To perform this work, the instructions required to disconnect the electrical supplies from the valves. The re-connection was not covered by the procedure. After completion of the work, the trains were tested and the unavailability of the valves was not detected. A detailed procedure how to perform the tests did not exist. Some days later the actuators of the valves were re-assembled, but the electrical supply cables remained disconnected. The indication in the control room showed that the valves were closed. A further test of all safety systems was performed which, however, did not reveal that the valves were still electrically disconnected. After this test the start up of the reactor was initiated.

The analysis of the root causes in the report is restricted on the occurrence that the operators failed to interpret the observed valve position indication. The two root causes of this occurrence have been identified firstly as a deficiency of the supervisors because they are not encouraged to carry out surveillance of staff competence and performance, and secondly there is an inadequate demonstration of the requirements for operational behaviour and competence by management. The actions taken after the event include further training especially regarding the interpretation of control room indications, the importance of work attitude and diligence, as well as that the role of management providing guidance to supervisors and support for surveillance. Regular meetings should be established as a forum of communication between supervisor groups, operators and other staff members.

Event 3:

The third event concerns an erroneous switching in the oil supply system of the main coolant pumps during power operation. In violation of the scheduled program the operator began to carry out switchings without appropriate approval and preparation. Subsequently, the oil pressure decreased and the main coolant pumps were shut off.

The direct cause of the event was the erroneous opening of two valves. Communication deficiencies and a lack of clear marked equipment contributed to that event. A further root cause was determined to be deficiencies in the work orders and reports.

Conclusion:

It can be concluded from the events described that they have been caused by non-adequate documentation, lack of necessary control of manuals and routine programme development. The corrective measures are mainly aimed to improve the technical documentation and the process of its development.

Corrective measures on personnel qualification upgrading to prevent CCF have, up to now, not been defined.

*United States of America:*

During start-up preparations, after refueling outage, the operators failed to establish the expected pressure in the containment. After entering the containment, the investigations determined that 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 eight instruments, the control room had no accurate indication of the containment pressure and several actuations of the engineered safety features were unavailable.

The lines were capped by a maintenance crew using a "work list" that they believed described work of "minor maintenance". However, the crew had performed unauthorized work that was safety-related, required a "formal work request", and resulted in a permanent plant configuration change. The evaluation revealed less than adequate management/quality assurance as a human factor related CCF. The main deficiency identified was the failure to differentiate between minor maintenance and major safety-related maintenance that resulted in a permanent change to the plant.

More detailed analysis were performed using different systematic HF analysis methods. Both analyses identified the sequence of events that led to the incident, the HF-related failures and further contributing causes. The licensee applied a method called "level 2 root cause investigation". The NRC used the Human Performance Investigation Process (HPIP) method. The main contributing factors identified by the NRC were:

- Drawings difficult to read (man-machine interface problem)
- Typographical error regarding the number of pipe penetrations
- Written and verbal communication less than adequate
- Labeling less than adequate

The short term and long term corrective actions taken by the plant are based on the lessons learned from the root causes and contributing factors.

### **3.2 Sub-task 2: Predictive techniques**

*Finland:*

In connection with the Nordic project "Optimization of the technical specifications by use of probabilistic methods" a method was developed to use probabilistic safety criteria to investigate the effect of testing and maintenance on nuclear safety. Especially, the effect of inadvertent human activities has been under investigation. The main emphasis of the method developed is the identification of possible test and maintenance originated CCFs.

The basic assumption of this method to identify human action related CCFs is simple: Human errors cannot cause a system to fail in a new way. This means that system failures can only exist due to technical reasons and it is always possible to create check-lists for the most of them. Organisational

liability or human errors may appear as direct causes of the failures, but even human errors cannot create technically impossible failures. The identification of human errors was performed by a modified application of HAZOP (Hazard and Operability Study) and FMEA (Failure Modes and Effects Analysis) principles.

The systematic evaluation of a system and a component group, respectively, is done by the investigation team (including plant maintenance personnel). The study starts with the review of all relevant test and maintenance tasks. Thereafter, the frequencies of the tasks are identified and the possible human actions related CCFs are discussed. The consequences of each CCF are determined and possible ways of detection (e.g. tests, indications, inspections) are assessed. The frequencies of the measures to detect the failures are considered.

An analysis form was developed to fill in the results of the analysis steps mentioned above. It is completed with the potential risk of the CCF and measures to be taken to avoid the respective CCF or to mitigate its consequences. The CCF risk has been divided into three classes with respect to the task frequency, the inspection frequency and the consequence. The ranking process is influenced by the expert judgment of the investigation team.

The method has been tested in a Finnish NPP at safety related systems. About 20 human originated CCFs were identified in the two highest risk classes. The results of the study were discussed with the plant personnel leading to several remarks useful for future operation and maintenance. e.g. suggestions of maintenance programme extension to new items and ideas to modify some tests and changes in maintenance practices and tools were introduced.

A further Finnish study being under performance is based on the systematic evaluation of maintenance experiences by reviewing thousands of failure and repair reports in the maintenance history systems of Finnish NPPs. The fault and maintenance history records of 3 - 6 years are evaluated in co-operation with the plant maintenance personnel to identify human related CCFs using another specific analysis sheet. By this analysis model the causes of human errors leading to CCFs, their detection and inspection procedures and the severity of the CCFs can be analysed, classified and documented for statistical treatment, interpretation and conclusions. The analysis model facilitates also identification of recurrent errors in relation to maintenance and of potential CCFs. The results aim at justifying corrective measures in order to prevent CCFs in the future. The study will also analyse such CCF mechanisms that have a significant potential to penetrate different detection and inspection processes. Tests and checks which are not effective, shall be identified. The study on one plant will be available in 1995 and on the second plant in 1996. A more detailed description will be available after publication of the results.

*France:*

Based on a maintenance related incident in a French NPP, an analysis method was developed to determine organisational influences on plant safety. The detailed analysis of the incident revealed that several levels of the defense-in-depth concept failed. Therefore, these levels were identified at first:

- human action
- check
- internal quality assurance
- demonstration of functionality of the equipment
- regular testing
- operation

The deterioration of the defense-in-depth concept may result from organisational influences. The first three levels are directly influenced by the maintenance personnel in the incident mentioned above due to high work load and resulting tiredness. Therefore, these three levels are not independent.

The analysis method is based on the technical analysis of a system and simultaneously on the analysis of human factors involved during maintenance operation. The different steps of the analysis take into account:

- functional analysis including interfacing systems, transients, balance of man-machine interaction, description of regular human actions and their environment;
- analysis of the availability of components and personnel including e.g. time dependency of modes of operation and time dependent personnel work load, respectively;
- identification and classification of deviations including safety significance and frequency as well as consequences of personnel actions and failure classification with respect to compensatory measures;
- root cause analysis of "critical" failures including a detailed analysis of consequences and related scenarios as well as analysis of coincidence of contributing factors, strategies for actions to be taken and identification of necessary tools and information; and at last
- proposals for actions to be taken.

For any analysis step, the detailed objective, the method and the tool is given. The application of the method is focused on the analysis of events. The systematic analysis allows to identify the type of failure, the relevant scenario, the significance of single elements of the overall system contributing to the failure, and the degree of robustness and reliability of the system. In the analysis, human factors are considered equally to technical aspects. The safety significance of human actions is taken into account and proposals for improvement are given.

*Spain:*

The Probabilistic Safety Analysis (PSA) is an analytical technique to assess the risk of a particular NPP and to develop an information base for analyzing plant specific and generic issues. A PSA involves, besides other aspects, the analysis and quantification of human errors. Recent PSAs have shown the importance of operator errors. 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 operation procedures to identify potential human errors to be included in the PSA.

The basic objective of the Human Reliability Analysis (HRA) within a PSA is the incorporation of all credible human actions, which could affect safety, into the overall analysis in an adequate, systematic and traceable way. The assumptions, expert judgments, analysis methods, and information sources are documented during the analysis.

To identify human factor related common cause failures the analysis method developed in Spain, based on the HRA methodology, has been applied. The analysis starts with the definition and identification of human actions. At this step, basic criteria and the method for determining human actions are indicated to be considered in the different PSA models and in the preliminary analysis of the dependencies. These dependencies may be roots of CCFs. Further steps include the selection of human

actions to be analysed in detail and the identification and analysis of recovery actions for accident sequence cut sets, if necessary.

When there are human actions affecting the availability of components included in the PSA model (and combined by "AND" gates), a potential human error basic event is considered, i.e., a potential HF related CCF is analysed when occurrences of at least two events are needed for a considered failure and there are human actions identified that affect these events.

Two basic types of dependencies are considered: the first type is the functional dependency among shift actions especially during accident conditions, the second type is the dependency due to the fact that modeled components are manipulated during normal operation by maintenance or operation personnel, affecting the availability of these components when they are not restored to their correct position.

Operating procedures as well as test and calibration procedures including the administrative processes in all plant operational modes are used as basic sources for the identification and modeling process. The analysis of specific situations needs support from plant personnel.

The methodology was applied to identify and analyse potential HF related CCF. Three examples are presented:

- Human errors related to uncorrected positions after testing, maintenance, calibration, and operative realignments
- Human errors related to miscalibration
- Human errors during accident sequences

After identification of human actions causing CCF or generating functional dependencies in accident sequences, a detailed analysis is performed for significant error probabilities. To determine the most important human errors generally two selection criteria are used. The first one is qualitative and based on the selection of those human errors causing simultaneous failures of functions, trains, or systems. The second criterion is quantitative and applied after the preliminary assessment of the accident sequence. The relevant sequence should contribute at least 1% to the overall core melt frequency of the initiating event group.

In all Spanish PSAs, HF related CCF have been identified with significant contribution to the core melt frequency. Corrective measures are taken to prevent, to detect, to mitigate, or even to recover from an accident. Some examples are given in the report:

- Independent verification of the removal of temporary flanges in the containment sump after refueling outages.
- Installation of limit switches at three manually operated valves to ensure correct realignment after AFW turbo-pump functionality test.
- Photocopy of transmitter cards placed at the transmitter in the containment to avoid errors during manual transferring the setpoints from the transmitter cards.
- The calibrations of the two pressure transmitter channels at each accumulator are performed by two different teams with different calibration masters.

- For control of accident sequences, some design and procedure modifications were done to increase the available time by e.g. changing the type of some actuators from local to remote and transferring the tasks to the control room.
- For some specific accident sequences of accidents, the former procedures did not describe the symptoms sufficiently or respectively, the symptoms were confusing. In these cases new redundant symptoms were added to reduce the existing dependencies.

It is concluded that PSA and the associated HRA methodology is adequate to identify some types of HF related CCF. In addition, it allows a continuous update according to changes and modifications during the plant life.

*United Kingdom:*

The UK paper is based on the work of the Human Factors Reliability Group (HFRG) Human Error Dependency Sub-Group, which comprises representatives from across a range of industries. Although the work of the group is not complete, the programme is intended to provide a better understanding of Human Error Dependency (HED), and methods for addressing the issues, both in design and assessment.

To determine the anticipated reliability of systems, it is important to be able to identify and predict the possibility of the dependency between systems, including HED. Understanding the mechanisms, causes and effects will help identify defenses to enhance the system itself. It will also assist in the treatment of dependency within risk assessment, and will generally assist in recognizing situations which are sensitive to dependency effects. The HFRG subgroup developed a tool to support the understanding and identification of dependency-prone tasks, particularly during the hazard identification process.

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. Functional links provide also pre-specifying task combinations, prediction of possible critical paths in a fault tree, and critical design issues to focus on.

Coupling mechanisms can be considered in terms of a set of generic mechanisms into which all causal factors can be allocated, like training, procedures, organisation, culture, etc. Dependent behavior is affected by the causal factors which influence performance on tasks related by the 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 below:

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

Each of the 16 possible conditions can be identified which uniquely describe a given task combination. The purpose of this approach is to identify important conditions in terms of types of dependency. This approach provides a basis for developing a framework to assess dependency effects.

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 defenses can be identified based on control of the coupling mechanisms, the conditions, or both. The identification of coupling mechanisms for limiting the range of tasks should be considered in detail for dependency effects. The development of such a screening mechanism has been a focus of attention for the HFRG sub-group.

Two matrices have been developed by the group. The first matrix is used to address how HED is accounted for in conventional hazard identification and risk assessment, and hence where to focus attention. The second matrix highlights the defense against potential dependencies by indicating which are the sensitive coupling mechanisms. In both matrices the HED-prone conditions respectively the dependency-prone conditions are ranked from 1 to 5. With aid of the matrices, the analytical process can consider whether the relevant defenses are present within the system in a robust form.

Typical defenses which could be considered as a means of reducing the impact of HED are given in the report. By considering conditions and causal factors, the advantages and disadvantages of each potential defense can be assessed. Defenses against dependency can address the coupling mechanism, or they change the condition itself. Inevitably there will be a range of different defenses 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 defense.

The method presented to assess human error dependencies is basically qualitative. The HFRG sub-group developed an analyzing tool that provides a systematic way to assess dependencies considering conditions and causal factors. In addition, the group included a way to choose the appropriate defense.

## **4. CONCLUSIONS**

### **4.1 Conclusions of sub-task 1**

Event analysis was performed by ten countries. The spectrum of the analyses covered the investigation of 28 events as well as the description of the general treatment of human factor related event analysis in a country. Due to this broad spectrum no single general conclusion can be drawn.

In the reports presented some events are discussed that had safety significant consequences. These consequences include:

- loss of RHR during mid-loop operation,
- difficulties to control a steam generator tube rupture,
- unavailability of stand-by safety systems, and
- violation of technical specifications.

One event report addressed a CCF for components of different manufacturers installed in several plants. The unavailability of a special actuation mechanism of these components was deteriorated by the same type of root causes.

The reported HF related CCF occurred in several systems and components. The types of human tasks resulting in the CCF are wide spread. Maintenance tasks, operator errors, work preparation deficiencies, quality control deficiencies and further tasks were mentioned in the contributions. This means

that any system or human task could cause a HF related CCF or could be affected by a HF related CCF. No specific weak point in the plants could be detected.

One country provided the results of a search covering all national reported events. The results of this investigation are similar to the findings of this sub-task. The investigation could not identify a system or personnel task which is specifically sensitive to HF related CCF.

The synopsis of the contributions shows some common aspects of the described HF related CCF. At least two different kinds of failures can be identified: common cause failures and dependent failures. Root causes reported with respect to CCF include for example procedural deficiencies, repeated errors on redundant components, and lack of awareness of personnel. Dependent failures were caused by e.g. communication deficiencies, deficiencies in maintenance task scheduling, overreliance on skills and knowledge, assumption of minor safety significance of a task, less than adequate labeling, and licensing deficiencies.

Dependent failures may include organisational deficiencies in several working groups of a plant (e.g. operators, maintenance staff, work preparation).

The in-depth analysis revealed two areas of concern: latent failures and "minor" tasks. Most failures can be detected immediately after their occurrence or during the first function test. Failures which have not been timely detected, are called latent failures. Several latent failures described in the events resulted from deficiencies in the functional test performed after initial installation or maintenance activities. In some cases function tests cannot be performed with representative loads or under the same environmental conditions existing during real demand. In these cases additional actions should be taken to detect possible latent failures.

Another area of concern are maintenance tasks which are believed to have minor safety significance. There are a lot of "minor" tasks in the plants. A "minor" task needs much less effort in preparation, supervision and quality assurance than safety related works. The event analysis shows examples that safety related works have been erroneously treated as "minor" tasks. Thus failures in these "minor" tasks were not detected in time and caused serious safety system degradations.

The actions taken after the event reflect the variety of systems affected, tasks performed and causes. In order to avoid the recurrence of an event, the main focus of corrective actions corresponded to the identified root causes. Some of the generally applicable corrective actions are:

- operator training,
- modification of procedures,
- modification of the maintenance frequency or the maintenance programme, and
- design changes.

## **4.2 Conclusions of sub-task 2**

Four countries presented predictive techniques to identify HF related CCF. The goals of the described techniques are:

- the identification of possible weak points in equipment or human actions,
- the quantification or assessment of human actions with respect to probabilistic analyses and

- the analysis of "critical operator actions" during accident management measures.

All approaches have been well developed and are increasingly used or in one case ready to use in these countries. All of these techniques depend on a detailed analysis of tasks and assess them regarding their safety significance. Some techniques include maintenance related activities explicitly. The work environment is also considered.

The techniques developed are based either on probabilistic methodologies or on failure mode and effects analysis. Both types of analysis are time consuming and need high efforts. Applications of these techniques show valuable results. After identification of weak points actions have been taken to prevent possible failures before they occur on real demands. These actions include measures like:

- modification of the operating manual,
- modification of maintenance procedures, testing procedures and scheduling,
- installation of additional alarms and annunciations in the control room, and
- design changes.

A second goal of the application is the identification of so called "critical operator actions" especially during accident management activities. Because of the extreme low probability of occurrence of these events, feedback of operational experiences is not available. The predictive techniques can aid in designing the operator actions in a suitable way. The knowledge of the safety significance of the identified critical actions should be introduced into the operator training programme.