STUK

STUK-YTO-TR 139 January 1998

HUMAN ERRORS RELATED TO MAINTENANCE AND MODIFICATIONS

K. Laakso, P. Pyy
VTT Automation
L. Reiman
STUK

STUK • SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

The conclusions presented in the STUK report series are those of the authors and do not necessarily represent the official position of STUK.

ISBN 951-712-242-X
ISSN 0785-9325

Oy Edita Ab, Helsinki 1998

LAAKSO, Kari, PYY, Pekka (VTT Automation), REIMAN, Lasse (STUK). Human errors related to maintenance and modifications. STUK-YTO-TR 139. Helsinki 1998. 36 pp. + Appendices 6 pp.

ISBN 951-712-242-X
ISSN 0785-9325

Keywords: fault history, maintenance, human factors, experience feedback, reliability, common cause failures, safety, statistics, modifications, instrumentation, defensive barriers, nuclear power plants

ABSTRACT

The focus in human reliability analysis (HRA) relating to nuclear power plants has traditionally been on human performance in disturbance conditions. On the other hand, some studies and incidents have shown that also maintenance errors, which have taken place earlier in plant history, may have an impact on the severity of a disturbance, e.g. if they disable safety related equipment. Especially common cause and other dependent failures of safety systems may significantly contribute to the core damage risk.

The first aim of the study was to identify and give examples of multiple human errors which have penetrated the various error detection and inspection processes of plant safety barriers. Another objective was to generate numerical safety indicators to describe and forecast the effectiveness of maintenance. A more general objective was to identify needs for further development of maintenance quality and planning

In the first phase of this operational experience feedback analysis, human errors recognisable in connection with maintenance were looked for by reviewing about 4400 failure and repair reports and some special reports which cover two nuclear power plant units on the same site during 1992–94. A special effort was made to study dependent human errors since they are generally the most serious ones.

An in-depth root cause analysis was made for 14 dependent errors by interviewing plant maintenance foremen and by thoroughly analysing the errors. A more simple treatment was given to maintenance-related single errors. The results were shown as a distribution of errors among operating states i.a. as regards the following matters: in what operational state the errors were committed and detected; in what operational and working condition the errors were detected, and what component and error type they were related to. These results were presented separately for single and dependent maintenance-related errors. As regards dependent errors, observations were also made about weaknesses in audits made by the operating organisation and in tests relating to plant operation.

The number of plant-specific maintenance records used as input material was high and the findings were discussed thoroughly with the plant maintenance personnel. The results indicated that instrumentation is more prone to human error than the rest of maintenance. Most errors stem from refuelling outage periods and about a half of them were identified during the same outage they were committed. Plant modifications are a significant source of common cause failures. The number of dependent errors could be reduced by improved co-ordination and auditing, post-installation checking, training and start-up testing programmes.

LAAKSO, Kari, PYY, Pekka (VTT Automaatio), REIMAN, Lasse (STUK). Ihmisen virheet kunnossapidon ja muutostöiden yhteydessä. STUK-YTO-TR 139. Helsinki 1998. 36 s. + liitteet 6 s.

ISBN 951-712-242-X
ISSN 0785-9325

Avainsanat: vikatiedot, kunnossapito, inhimilliset tekijät, käyttökokemuspalaute, luotettavuus, yhteisviat, turvallisuus, tilastointi, laitosmuutokset, instrumentointi, tarkastukset, ydinvoimalaitokset.

TIIVISTELMÄ

Inhimillisen luotettavuuden analysointi ydinvoimalaitoksissa on perinteisesti keskittynyt ihmisen suorituskyvyn tutkimiseen häiriötilanteissa. Eräät tutkimukset ja tapahtumat ovat toisaalta osoittaneet, että häiriöitä edeltävät kunnossapitovirheet voivat vaikuttaa häiriön vakavuuteen esimerkiksi estämällä turvallisuuden kannalta tärkeän laitteiston toiminnan tarvetilanteessa. Erityisesti moninkertaiset turvallisuusjärjestelmien viat (dependent failures) voivat merkittävästi vaikuttaa reaktorisydämen vaurioitumisen todennäköisyyteen.

Tutkimuksen ensimmäinen tavoite oli tunnistaa ja tuottaa esimerkkejä moninkertaisista inhimillisistä virheistä, jotka ovat läpäisseet laitoksen moninaiset turvallisuuden puolustusrakenteisiin kuuluvat virheiden havaitsemis- ja tarkastusprosessit. Toinen tavoite oli tuottaa turvallisuuteen liittyviä tunnuslukuja kuvaamaan ja ennakoimaan kunnossapidon tehokkuutta. Yleisempi tavoite oli tunnistaa tarpeita kunnossapidon ja sen suunnittelun laadun kehittämistä varten.

Käyttökokemusanalyysin alkuvaiheessa etsittiin kunnossapidon yhteydessä tunnistettavia inhimillisiä virheitä käymällä läpi noin 4400 vika- ja korjausraporttia sekä erikoisraportteja kahdelta saman laitospaikan ydinvoimalaitosyksiköltä vuosina 1992–94. Erityisesti pyrittiin etsimään moninkertaisia inhimillisiä virheitä, koska ne seuraamuksiltaan ovat yleensä kaikkein vakavimpia.

Syvällinen perussyyanalyysi tehtiin 14 inhimilliselle moninkertaiselle virheelle, jotka käytiin läpi haastatteluina laitoksella kunnossapitotyönjohtajien kanssa ja analysoitiin seikkaperäisesti. Kunnossapidon yhteydessä havaitut yksittäisvirheet tutkittiin yksinkertaisemman menettelyn avulla. Tulokset esitettiin virheiden jakaumina muunmuassa sen suhteen, missä käyttötilassa virheet oli tehty ja missä havaittu; missä käyttö- ja työtilanteissa virheet oli havaittu sekä, missä laite- ja virhetyypeissä niitä oli esiintynyt. Tilastot esitettiin erikseen kunnossapidon yhteydessä esiintyneille yksittäis- ja satunnaisvirheille. Satunnaisvirheiden osalta tehtiin myös oman käyttöorganisaation suorittamien tarkastusten ja käyttötoiminnan kokeiden heikkouksia koskevia havaintoja.

Lähtöaineistona käytettyjen laitoskohtaisten kunnossapitoraporttien määrä oli suuri ja havainnoista keskusteltiin yksityiskohtaisesti laitoksen kunnossapitohenkilöstön kanssa. Tulosten mukaan instrumentointi on muuta kunnossapitotoimintaa alttiimpaa inhimillisille virheille, joista pääosa on peräisin vuosihuoltoseisokkijaksoilta, ja joista noin puolet havaittiin saman seisokin aikana kuin ne tehtiin. Laitosmuutokset aiheuttavat huomattavan paljon yhteisvikoja. Satunnaisvirheiden määrää voidaan jatkossa vähentää parantamalla muutostyöprojektien koordinointia ja katselmointia, sekä asennustarkastuksia, koulutusta ja käyttöönotto-ohjelmia.

CONTENTS

FOREWORD

This study was carried out within the research project "Reliability and risk analyses" (LURI) of the Finnish research programme "Reactor Safety" (RETU). The study was financed by the Radiation and Nuclear Safety Authority (STUK).

The study is a part of the Finnish contribution to the IAEA (International Atomic Energy Agency) co-ordinated research programme "Collection and classification of human reliability data for use in probabilistic safety assessments". The results of the study have also been reported to the Task Force "Human related common cause failures" of the CSNI/PWG 1 of the OECD Nuclear Energy Agency.

We are thankful to the maintenance, operation and reliability personnel of the utility Teollisuuden Voima Oy, who have provided the maintenance history data and participated in constructive interviews and meetings during the study.

1 INTRODUCTION

In the research concerning human behaviour and human error possibilities main attention has been traditionally focused upon the control room crew performance in disturbance and accident conditions. The control room operators have an essential role in disturbance and accident management. On the other hand, non-detected (latent) maintenance errors may have an impact on the severity of a disturbance by disabling safety related equipment. The chances of operators to manage the situation are worsened if there exist latent equipment failures due to imperfect test and maintenance activities. Especially common cause failures affecting several subsystems of a safety related system may have a significant contribution to the reactor core damage risk. Therefore, the dependence of errors between tasks performed in redundant subsystems of a safety related system is an issue of extreme importance.

Human maintenance related errors have been analysed in an earlier study in Finland [Reiman 1994]. This study is a continuation and an expansion of the previous one with more focused objectives, as discussed in the following. In the first phase of this study, maintenance related errors at the Olkiluoto BWR plant were analysed. In the second phase, the same analysis will be made for the Loviisa PWR plant.

The Olkiluoto I and II are identical 710 MWe designed by ASEA Atom BWR units. A power upgrading project of the two units is going on. The active safety functions of the units are divided into four redundant subsystems. The subsystems are separated physically from each other and each subsystem has a separate electrical bus. This design makes it possible to justify planned maintenance actions, making one subsystem unavailable for a limited time, during power operation. Due to this design, dependent failures are however an important contributor to the risk of the plant. Apart from the safety systems, this study focuses also to other systems of the plant units due to the fact that human error mechanisms may be the same. Also a more extensive database will be obtained, and all from the risk point of view significant systems are not classified as safety systems.

2 OBJECTIVES AND USED MATERIAL

The first objective of the study was to identify and give examples of the origin and appearance of such human related common cause failure mechanisms, which can penetrate the barriers of different detection and inspection procedures of the plants and, to find means to strengthen those barriers (see Figure 1). Where possible, statistical treatment was aimed at.

The second objective was to generate numerical safety indicators describing and forecasting the effectiveness of the maintenance performance. A more general objective was to identify needs of remedial measures to further develop the quality of the maintenance and its planning.

A kernel behind the study is that a component may be declared operable although it actually is not capable to fulfil all its functions. This may be due to many things, e.g., improper testing. It is useful to study which kinds of human errors can pass on to operable components and cause latent unavailability. The term unavailability is a probabilistic measure whereas the term operability is used in a deterministic sense in e.g. NPP Technical Specifications. For more information about the calculation of unavailability, see Appendix 1 and e.g. [ESReDA 1995].

The main database used in the study were the fault and repair history records of the Olkiluoto NPP units I and II. The records were obtained from the computerised maintenance history data system of the plant. The failure records covered about 4400 failure and repair cases from the calendar years 1992…1994.

The database was completed by some other reports and information sources, such as licensee event reports, annual outage reports and the quarterly reports. From this data, 334 human error candidate cases were screened for follow-up analyses.

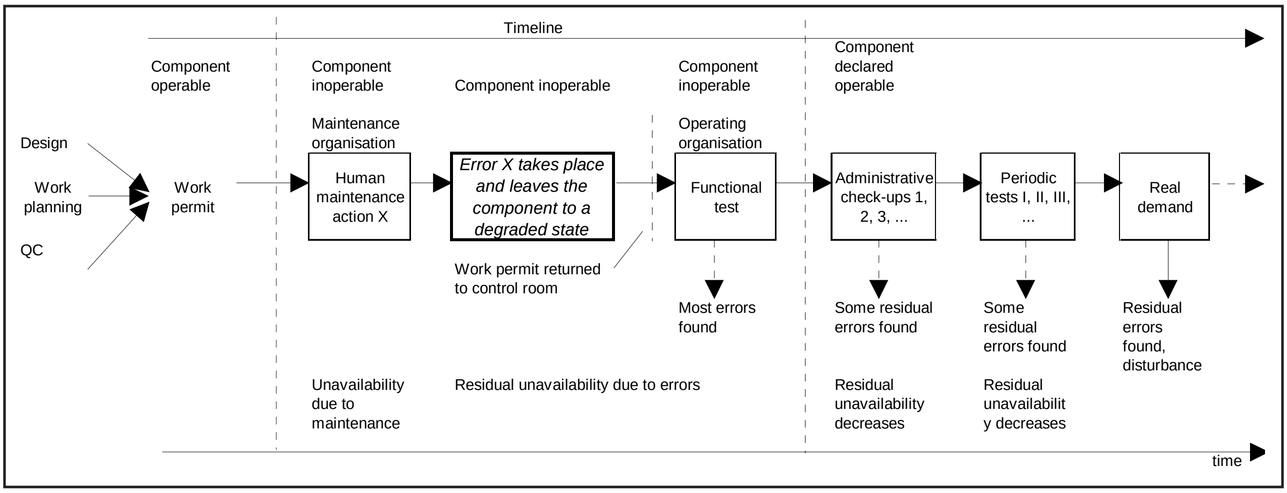

Timeline
Component operable
Component inoperable
Component inoperable
Component inoperable
Component declared operable
Design
Work planning
QC
Work permit
Maintenance organisation
Human maintenance action X
Error X takes place and leaves the component to a degraded state
Work permit returned to control room
Operating organisation
Functional test
Administrative check-ups 1, 2, 3, ...
Periodic tests I, II, III, ...
Real demand
Most errors found
Some residual errors found
Some residual errors found
Residual errors found, disturbance
Unavailability due to maintenance
Residual unavailability due to errors
Residual unavailability decreases
Residual unavailabilit y decreases
time

Figure 1. *Model of the birth of an error in a maintenance action and its consequences (component degradation) passing several barriers. The unavailability decreases in each barrier due to possibilities to detect the fault.*

3 BASIC TERMS AND DEFINITIONS

The concept human error is systematically used in this report, although the authors are knowledgeable about the complexity of the definition. In several cases, only the consequences of the action show whether an action is successful or not [Rasmussen 1979]. Similarly, contextual and cause-consequential factors may lead to an unwanted outcome despite the best efforts of the actor. Despite these facts the term, if interpreted as an action leading to an unwanted outcome, is sufficiently compact to be used in this report.

An important concept in analysing human errors is the dependence of human actions, i.e. how the success or failure on one task may be related to the success or failure on some other tasks. Two tasks A and B are independent, if the probability of failure (or success) of task B is the same regardless of the failure of task A. In all other cases, dependence exists.

The dependence between human actions can mean in the probabilistic sense that:

- the probability of repeated erroneous actions diminishes, when a person discovers an error and learns about it, or
- the probability of repeated erroneous actions increases, when a person learns a wrong way to perform actions.

Dependence between errors has been studied in psychological tests, which have shown that persons ”learned” to repeat errors that they had performed [Kay 1951]. If the indications about the unwanted consequences of an erroneous act are immediate, it is unlikely that the error will be repeated. Thus, the most important group of human actions causing dependencies are those that do not give immediate feedback of their unwanted consequences. Some Common Cause Failure -mechanisms, e.g. wrong grease and stiffening of valve stem, may even be undetectable in a test carried out immediately after servicing or overhaul.

The dependent human failures of concern in this study are divided into actual common cause failures (CCF) and common cause non-critical failures (CCN), as defined in the following. The non-critical common cause failures are of interest as potential precursors to actual common cause failures. They also reveal mechanisms, which can result in CCFs.

Single human errors, such as omissions or wrong settings, may only result in single component failures. The number of such single failures is high when compared to the CCFs. Their analysis is easier by using statistical techniques and the results facilitate the identification of recurrent error causes affecting specific equipment types. In special cases, also single human errors may cause multiple consequences due to, sometimes latent technical interactions between components and systems. They may be called human related shared equipment faults (**HSEF**s, see App. 1 and Section 5.3).

In order to enable a better understanding of the report and results, the most important failure related terms used are defined in Table I. The abbreviations **HCCF** and **HCCN** are commonly used in this report to denote the human related dependencies—both CCFs and CCNs—identified in the database. A distinction can be made between a HCCF and CCF in PSAs. The faults are usually regarded in PSAs as CCFs, if they cause unavailability in:

- standby components within the time frame of the surveillance test interval, and
- continuously running components within twenty-four hours (after an initiating event).

***Table I.** Definition of some central terms.*

Human error. A human unintended or intended action that produces an unintended result. For example, an omission of the on-line return of equipment after the maintenance work causes a failure of the physical item to perform its function. In some sources, human errors are further divided, e.g., into slips, lapses, mistakes, violations, omissions and commissions [see .e.g. Swain & Guttman 1983, Reason 1990].

Failure is the termination of the ability of an item to perform a required function. Failure is an event, as distinguished from fault which is a failed state.

Common cause failure. Common cause failures (CCF) are failure causes or mechanisms, that may apparently result or have resulted in multiple functionally critical failures in redundant components in real demand situations (they are unable to fulfil correctly their required function).

Common cause non-critical failure. Common cause non-critical failures (CCNs) are causes or mechanisms which result in a lack of, or deficiency in, a characteristic in functionally non- critical requirements of redundant components. If getting worse, these precursors can develop into common cause failures. The CCNs shall thus be regarded as an early warning of causes or mechanisms otherwise leading to CCFs.

A HCCF may fulfil the conditions of a CCF in PSA framework. However, longer time frames than 24 hours or test intervals have been considered in our study. This is due to, e.g., the fact that some faults may not be detected in the periodic tests or other planned checks due to their ineffectiveness. Similarly, non-critical HCCNs have been studied due to their precursor importance and due to similar error mechanisms as in HCCFs.

Our analysis of HCCFs, based on the plant-specific failure and repair reporting, is especially focused on human related maintenance dependencies between redundant subsystems. In PSA studies, a part of these CCFs are referred to as residual common cause failures, if they account there for the dependencies which are not explicitly included in the analytical fault tree and event tree models [NKA/RAS-470, 1990]. Explicit modelling of such CCFs has been increasingly introduced in the latest PSAs, but more analysis of operating experience is apparently needed to achieve a sufficient coverage of these models and data in PSAs.

4 USED METHOD

The failure records covered about 4400 cases from the years 1992–94. Reading through such a high quantity of records, however comparable with the number of similar reports from other Nordic NPP units [compare with TUD 94-11], was a very resource demanding task.

The reports had been readily classified by the utility maintenance foremen and included also a free text description. The procedure shown in Figure 2 was used in the analysis of the failure records. In addition, Figure 2 shows the number of records and failure cases studied at each phase of the analysis.

The screening principle was that a case was included in the final number of errors—single or multiple—if it had been found after returning the work permit into the control room, in the functional testing or later (see Figure 1). This is due to that returning the work permit means the end of a maintenance task and, e.g., the functional testing is normally carried out by the operating organisation. Another reason for this, more extensive, distinction is that more data became studied thoroughly, although at the stage of the first functional test a component cannot often be regarded as operable.

4.1 Screening of the fault data

The first analysis phase actually contained the search of potential information sources, a preliminary screening based on the utility records and the first classification of errors.

The failure history database was chosen due to the fact that it had proved to be feasible in an earlier study [Reiman 1994]. At the outset of this study, the scope was expanded in order to complete the data with the root cause reports available. A similar decision was made by the analysts to study all the app. 4400 failure records instead of only concentrating upon the pre-classified human errors (classes B and DC, see Table II). This analysis procedure produced considerably more human error candidates, app. 500 altogether, than concentrating upon fault record classes B and DC solely (see Table VI).

Table II. *Cause coding of failures at the Olkiluoto nuclear power plant [TUD 1994].*

A FAILURE IN INSTALLATION OR EARLIER	C CONSEQUENCE OF OPERATION
A Design	A Exceeding a limit value
B Material	B Unplanned stress
C Manufacturing	C Blockage, sediment
D Installation, erection work	D Foreign objects
	E Normal usage of lifetime/normal phenomena
B OPERATING AND/OR MAINTENANCE PERSONNEL	**D MISCELLANEOUS CAUSES**
A Operator error	A Cascade failure
B Deficient setting, control (mech.)	B External cause
C Deficient setting, control (electr.)	C Deficient procedure or order
D Error of own personnel in work	D Unclear cause
E Lack of maintenance	
F Work of external personnel	**Z OTHERS (description)**

The first screening phase was performed by two analysts in a sequential order. Thus, independent views on the failure cases were obtained. At the end, the results were summarised and the preliminary classification of the candidates across the cause classes was obtained. The cause coding of the equipment failures used at the plant is shown in Table II.

4.2 Review of the data with maintenance personnel

After the candidates of human errors were extracted from the data base, the next phase was to determine which proportion of these app. 500 records were real human errors. There are at least two sources of biases that made this task difficult. From one point of view, the text descriptions in the maintenance history are short ones and, in some cases, even contradicting to the cause classification. This may be due to the experienced difficulty to follow the fault classification scheme.

Another problem is that people may be reluctant to report human errors, which may lead to absence of a number of actual cases. But on the contrary, a number of records originally classified at the plant as caused by "Operating and /or maintenance personnel" could be screened out from the human error types. To avoid an underestimation, in total about 500 candidate records were chosen comprehensively in order not to neglect potential human errors from the next analysis steps.

The knowledge of the plant maintenance foremen was used to facilitate determining the real human errors amongst the candidates in the form of interviews. During these interviews, all the questionable human error candidates were discussed, and those actually being other than human related failures were screened out. This analysis effort resulted in 334 human error candidate cases, of which amount 5 cases originated from other sources than the fault history data (See Figure 2).

Further investigation revealed that, from these 334 cases, 126 fault history records could be further combined into 37 different dependence cases (HCCFs, HCCNs, HSEFs, etc). This reduction was due to the fact that multiple fault records in the database often referred to a similar and simultaneous cause mechanism. Furthermore, 2 fault records were found in the interviews to be

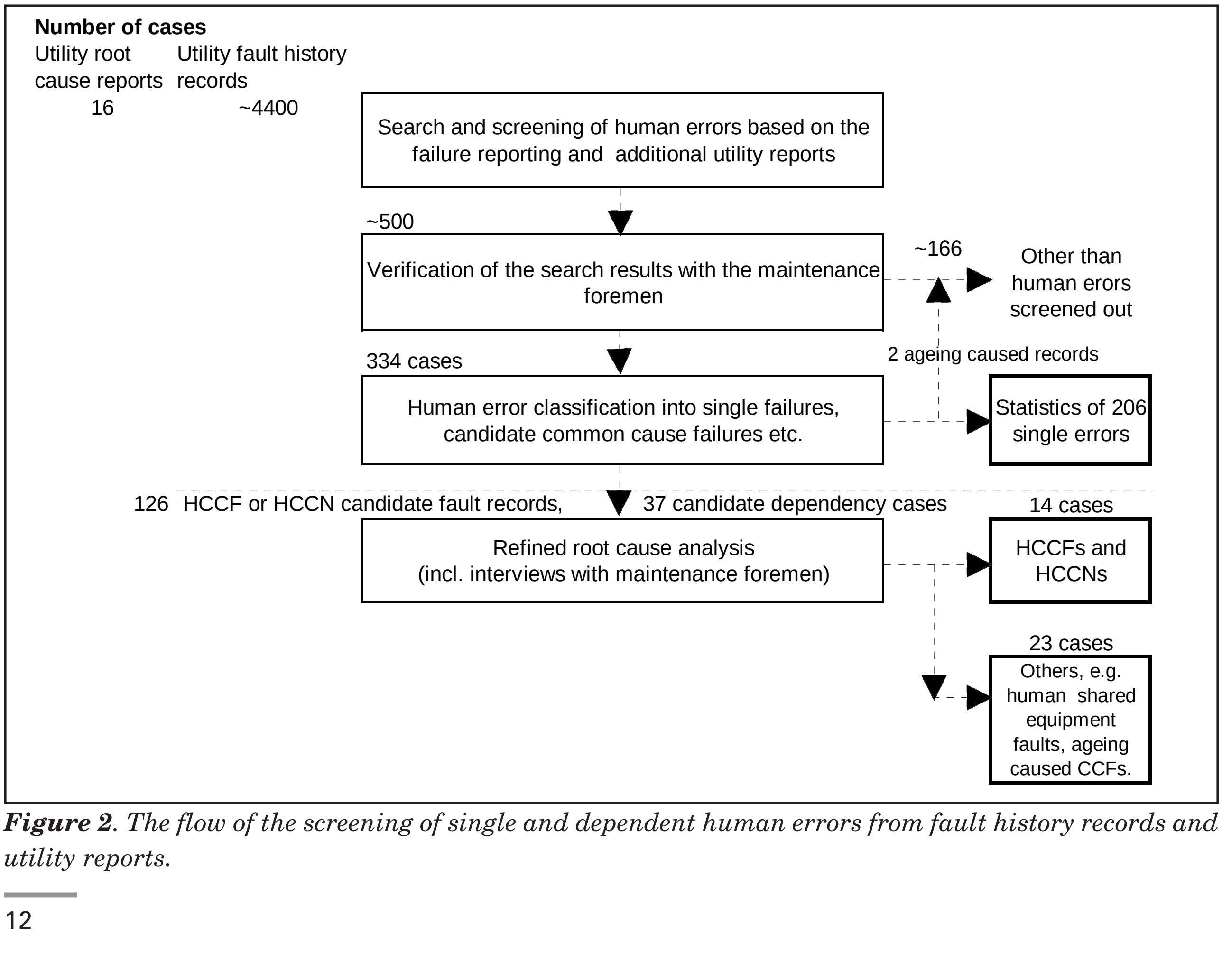

Number of cases
Utility root cause reports
16
Utility fault history records
~4400
Search and screening of human errors based on the failure reporting and additional utility reports
~500
Verification of the search results with the maintenance foremen
~166
Other than human erors screened out
334 cases
2 ageing caused records
Human error classification into single failures, candidate common cause failures etc.
Statistics of 206 single errors
126 HCCF or HCCN candidate fault records,
37 candidate dependency cases
14 cases
Refined root cause analysis (incl. interviews with maintenance foremen)
HCCFs and HCCNs
23 cases
Others, e.g. human shared equipment faults, ageing caused CCFs.

__Figure 2__. The flow of the screening of single and dependent human errors from fault history records and utility reports.

Table III. The classifications used in the statistical review of the data.

Direct causes of human errors	
Omission (incl. Restoration errors)	OM
Commission (wrong position, wrong direction)	COM/WD
Wrong settings SET	SET
Other commission error (e.g. too much/little force incl. carelessnes)	COM/OTH
Not classified	N-CLASS
Types of equipment affected by human errors	
Process valves, ventilation dampers or channel hatches	VAL
Block or primary valves in instrument lines	IVAL
Mechanical equipment (other than valves)	MEC
Instrumentation & control equipment and software	IC
Electrical equipment EL	
Time period of error origin	
Refuelling outage period	SHUT
Power operation period	OPER
Not clear (Design etc.)	NCLEAR
Types of operational situations at fault detection	
A. Type of detection	
Independent check or test (preventive)	PREV
Otherwise	OTH
B. Operating states	
Refuelling outage prior to start-up	OUT
(During) Plant start-up	STUP
Power operation	POW
(During) Plant shut-down	SNDN
Disturbance	DIST

caused by ageing rather than human errors, as shown in Figure 2. Thus, the number of single human errors found in the fault history was 206. The single human errors are discussed more in Section 5.1 and the dependent human errors in the Sections 5.2 and 5.3.

The human errors, their detection and remedial measures of the dependence cases were in the root cause analysis phase checked through with maintenance foremen. Most of the dependence cases were also checked through with STUK inspectors.

4.3 Re-analysis and classification of the data

After the preliminary verification of the human errors with the plant staff, other classifications than the original made by the utility personnel became possible. Questions, to build up statistics according to these classifications, were already included in the interviews of the plant personnel. Mainly, the idea was to verify the time and nature of both the error origin and the detection.

In that purpose, the 334 candidate cases were classified according to the following explaining factors: direct cause of the error, type of equipment affected, plant state at the error origin, type of error detection and operational state at detection of the error.

The breakdown of these classes is given in Table III. Multiple correspondence across these classes was also studied. Also underlying causes of human errors were studied, but this analysis was not very accurate and its results are only briefly discussed in Section 5.2. Some of these classes were also used in the analysis of dependent human errors, but their analysis allowed more accurate classifications.

By using these explaining factors, the general model presented in Figure 1 was used as a basic model of this study. The human error type classification is based on the NUREG/CR-1278 Handbook [Swain & Guttmann 1983], that makes the distinction between omission and commission errors. Here a breakdown of commission errors into mispositioning including wrong direction and order errors, e.g. leading to wrong wiring, reverse installation of items or reverse rotation, and into other commissions is used. The latter ones include a great variety of wrong actions stemming often from carelessness, use of excessive force or too feeble use of force. Timing errors have been, generally, classified under omissions in our study. As a specific error type we have chosen the wrong settings, often found in the instrumentation & control, due to its importance from safety point of view and its expected frequency in the HCCFs [Reiman 1994]. The consequences of the human errors on the components define the affected equipment category, e.g. electrical equipment, in the classification.

The results of the follow-up analyses of both single and candidate dependent errors were in each case presented in the form of a table allowing statistical studies. In Table IV, an example of a single follow-up analysis is given (classifications from Table III).

4.4 Analysis of the dependent human errors

The analysis of the 37 candidate dependent human error cases (HCCFs and HCCNs in redundant subsystems), consisting of 126 fault records, was much more detailed than that of the single failures. An analysis of the originating tasks, mechanisms, possible ineffectiveness of the defensive barriers and remedial measures, was performed for them.

The principle followed in the division of of the errors into single ones, HCCFs, HCCNs, HSEFs and other dependent failures (ODFs) is presented in Table V.

A component is here understood as a functional item at a level where an identification number such as 327P002 or 531K951, and a component category such as a pump or a sensor, can be identified [TUD 1994]. In order to simplify the analysis, several similar errors caused inside a defined component boundary have been defined as other dependent failures (ODF), although in some cases giving parallel unavailability of redundant items within the component exists.

In a few cases, after having extracted dependent errors from the database, patterns were recognised in the data that obviously were due to recurrent problems, error prone circumstances, etc. situational factors. This kind of mechanisms are always present in the data and it is extremely difficult to determine their exact mechanisms and the degree of dependence. After having identified the potential residual dependence mechanisms to be insignificant an assumption of the independence could be made for these single errors.

Statistics were made both for single and for dependent errors. The flow chart of the analysis of dependent human errors is shown in Figure 3 and the results are discussed in Section 5.2. An example of a root cause analysis of a human related common cause failure analysis (HCCF) is shown in Appendix 2.

Table IV. The follow-up analysis of a human error in relation to maintenance.

Component place	2.327P002
Failure record number	34281
Date	O7.O5.1992
Explanation	Card 6.D18.326) faulted mechanically in a modification task (327P002/SS13)
Plant state at the time of error	SHUT
Equipment code	IC
Cause, reported	BF
Cause, direct	COM
Dependence	HCCF
Plant state at the time of detection	OUT
Additional information	HCCF root cause analysis 2hccf327.doc.

Table V. Principles followed in the classification of human error data.

Causing mechanism	Unavailability in one single component	Unavailability in several components (or systems)	Parallel ** unavailability in redundant components	Sequential ** unavailability in redundant components
Similar repeated erroneous actions	Single errors*/ODF(3	Single errors*	HCCF / HCCN/ODF(4	ODF(5
One error	Single errors	HSEF(6	HSEF	HSEF
Several (different) errors	Single errors*	Single errors*	ODF(7	Single errors*

* Wrong direction errors—single errors. Human actions are seen as completely dependent, but do not cause unavailability in redundant components.

** Parallel and sequential refer to time—components may become unavailable in parallel or errors may be repeated after redundant components have been made operable.

(3 Other dependent failures (ODF), if several similar errors, but caused inside a defined component boundar

(4 Other dependent failure, if parallel dependence was detected while working (prior to returning work permit into the control room).

(5 Listed as other dependent failure, if not causing parallel unavailability.

(6 Components not redundant.

(7 Consequential effects due to functional dependence.

5 RESULTS

In the following, the results of the study are discussed with regard to totally 206 single and 14 HCCF/HCCN multiple error cases. In addition, the 12 HSEF cases are briefly discussed. These groups are discussed separately due to their very different nature. The authors recognise that human errors are a controversial topic and thus other classifications are possible, too.

5.1 Single human errors

Cause coding at the plant and the share of human error records. As can be calculated from the Table VI, a portion of about 7,4 % of all the failure records could finally be identified as human error related. Human errors can be found in all cause coding categories classified at the plant.

Under the category B (operating and/or maintenance personnel), about 47% of the records were really human errors in relation to maintenance. But also about 16 % human errors were identified under the category A (failure in installation or earlier). The broad distribution of the human errors between the categories supports the conclusion that it is rather difficult to use the coding of human errors used at the plant. Another interesting feature in these results is that human errors were seldom found under the category D (miscellaneous), only about 12 % of D totally. This is controversial to the findings from some earlier studies and the topic is discussed more in the Chapter 6. The category D includes however more than one third of all human error records, but also the total number of the records in the category is large. It should be observed that no case in the fault history records was classified under the category Z (others) requiring a specific text description.

The Table VI also shows the share of the single human error records of all the human error records. As seen from the table, there were no dramatic differences in distribution between the two plant units. However, the Chi-square test

Table VI. *The number of the single human maintenance errors distributed according to the cause coding given by the plant maintenance personnel.*

Reported cause code	Number of failure records (unit I + II)	Number of all human error records	Percentage of human error records of all [%]	Number of single human error records	Percentage of single errors of all error records [%]
A Failure in installation or earlier	279 +221 = 500	40 + 41 = 81	16,2	29 + 21 = 50	61,7
B Operating and/or maintenance personnel	113 +101 = 214	55 + 45 = 100	46,7	44 + 27 = 71	71,0
C Consequence of operation	1250 + 1491 = 2741	15 + 17 = 32	1,7	10 + 3 = 15	40,6
D Miscellaneous causes	505 + 447 = 952	43 + 70 = 113	11,9	23 + 47 = 70	61,9
Total	**4407**	**326***	**7,4**	**204****	**63,2**

* the amount excludes 2 cases later found to be ageing related and 6 cases coming from other utility reports

** the amount excludes 2 reports not coming from the maintenance records, together 206 single human error cases.

suggests that the records come from two different distributions (p(29.2,3)~1E–6). The result could be forecasted due to the fact that different persons classify the data at different units and classifying data is difficult. It is interesting to compare the result to that of human error records (p(6.38,3)~0.09). Thus, it is not excluded that their distributions come from the same source. One possible explanation is that it is easier to classify human errors than the rest of the fault data. Further discussion of the differences between the plant units is left outside the scope of this report.

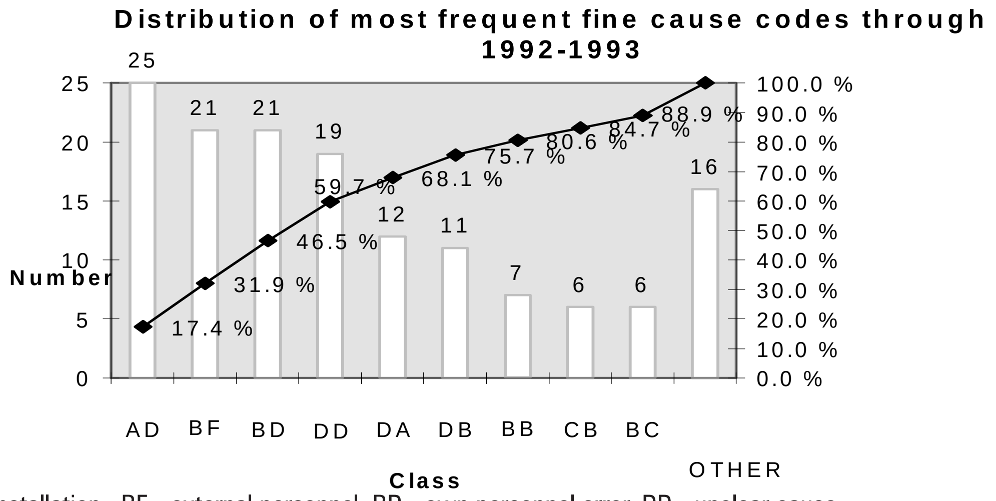
The distribution of single human errors between the finer fault cause code classes in 1992–1993, given by the plant personnel, is presented in Figure 4. A detailed classification for the year 1994 was not possible because the utility decided to give up the detailed cause coding following the principles in Swedish NPPs (See Chapter 6 and TUD 1994).

The Figure 4 shows that 25 single human error cases were identified under the class (installation/ erection work, code AD, 17 % of the total). Other frequently used classes were: own personnel (BD, 21 cases or 15 % of the total), external personnel (BF, 21 cases or 15 % of the total) and unclear cause (DD, 19 cases or 13 % of the total). These groups correspond to about 60 % of the total number of the fine cause classified cases (144) through 1992–1993.

Errors stemming from installation are salient in the Figure 4. An interesting observation is also that the class DC (deficient procedure or order) does not appear in the most frequent cause codings but the class BF (external personnel) does. It is important to note the fact that different categories are not mutually exclusive, and e.g. the code AD includes both foreign and own labour. Therefore, too firm conclusions should not be drawn based on the Figure 4.

Equipment affected by single human errors. The utility classification in the fault records did identify the component category faulted. Thus it was rather easy to conclude the equipment category affected by the human errors based on this coding and the free text description.

As seen from Figure 5, instrumentation & control (84 cases) plus electrical equipment (40 cases) dominated as objects of single human errors with the share of about 60 %. An interesting observation can be made with regard to the process valves, dampers and hatches. Their maintenance errors and wrong alignments are modelled often in PSAs but, here, their share is rather low (17 %). This supports the idea that more safety emphasis should be put to complex systems including instrumentation, control, protection and electric power supply and drives.

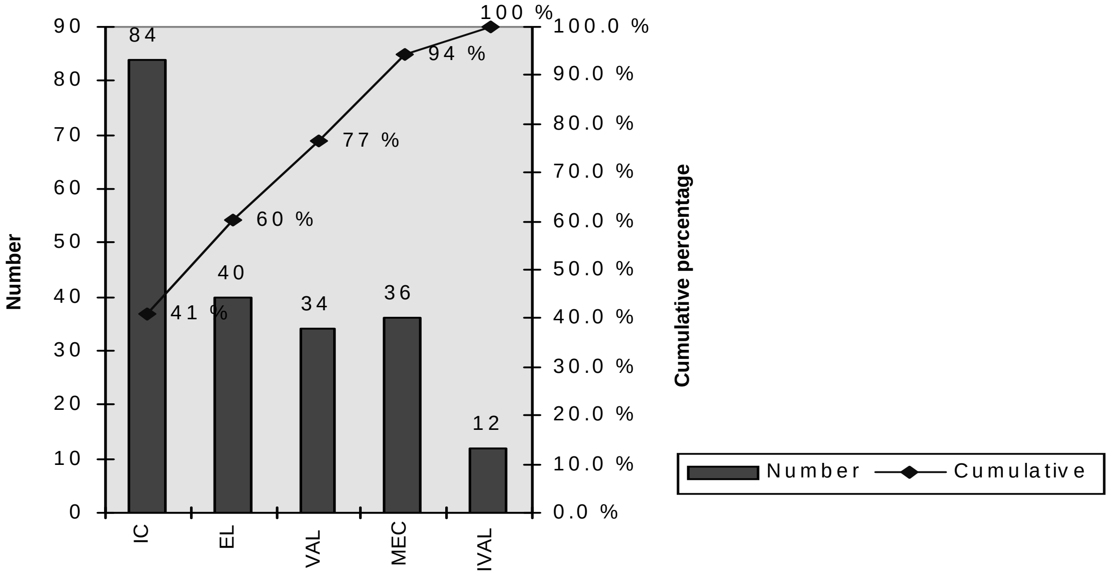


AD=Installation , BF=external personnel, BD=own personnel error, DD=unclear cause, DA=cascade failure and DB=external cause. Together 144 cases were fine classified, together 151 cases.

Figure 4. *Fault cause classification used by the plant personnel through 1992–1993 in the single human error cases.*

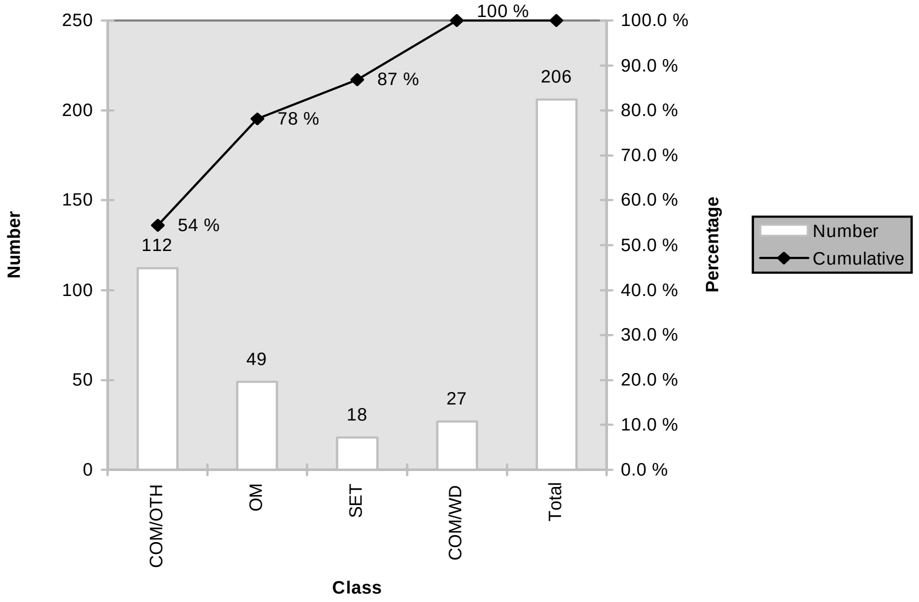
Direct causes of single human errors. The following Figure 6 presents the distribution of the direct causes of errors among different human cause categories. As seen, errors classified as commission errors dominate. Other commission errors COM/OTH dominate with 54 % of the total. This dominating cause category consists of several types of wrong actions such as: carelessness, or using too much force causing broken pieces in the nearby equipment or in the equipment maintained, use of too little force causing loose connections or untight bolts etc. Some of them could have been classified also under the category wrong direction (COM/WD) or omission (OM) errors, since both classes apply. Wrong direction, order or position errors (COM/WD) have here been identified with 13 % of total.

The finding related to COM/OTH type errors is understandable against the background that single human errors as causes of single component



Instrumentation & control equipment and software (IC), Electrical equipment (EL), Process valves, ventilation dampers or channel hatches (VAL), Mechanical equipment (other than valves, MEC), Block or primary valves in instrument lines (IVAL).

Figure 5. *Equipment types involved in single human errors 1992–1994, together 206 cases.*



Carelessness etc (COM/OTH), Omissions (OM), Wrong settings (SET), Wrong direction errors (COM/WD).

Figure 6. *The direct causes of single human errors through 1992–1994.*

Table VII. The distribution of human single error causes among the equipment categories.

	I&C	MEC	EL	VAL	IVAL	TOTAL
COM/OTH	49	26	14	19	4	112
OM	13	7	14	7	8	49
SET	11	0	5	2	0	18
COM/WD	11	3	7	6	0	27
TOTAL	**84**	**36**	**40**	**34**	**12**	**206**

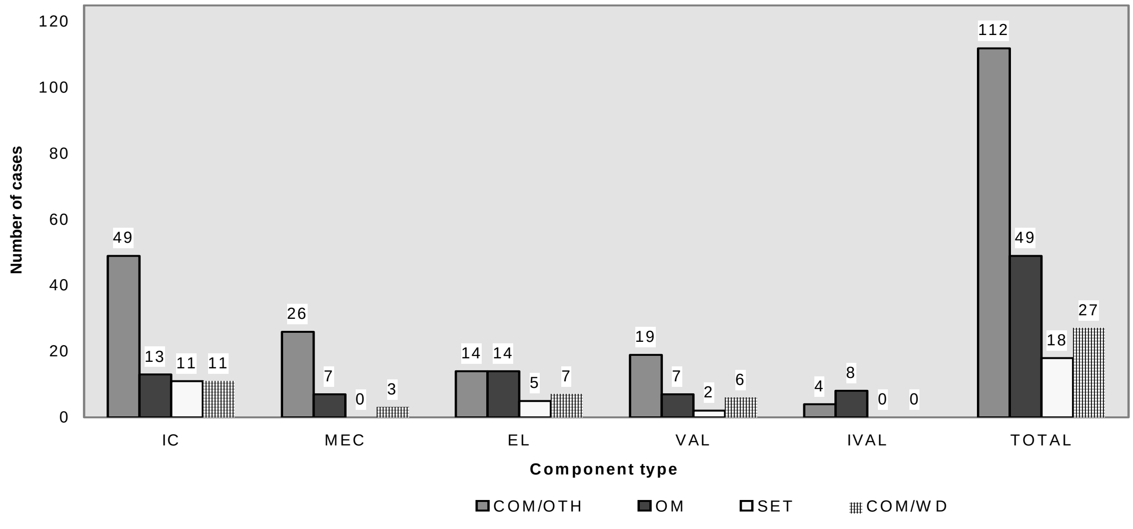
Instrumentation & control and software (IC), Mechanical equipment (other than valves, MEC), Electrical equipment (EL), Process valves, ventilation dampers or channel hatches (VAL), Block or primary valves in instrument lines (IVAL).

failures are likely to include many unintentional acts—such as lapses of memory, using too much force or simply crushing an object. However, due to the fact that HRA studies often concentrate upon omissions (OM) and, possibly, wrong settings, the finding has a certain value. The inclusion of COM/OTH types of erroneous actions may, still, be difficult due to their large spectrum of phenotypes and, mostly, small safety significance. In PSA purposes, the important issue is, whether the error consequence is critical or not. For the background of omission and commission error classification used, see [Swain&Guttmann 1983].

As discussed earlier, determining all the underlying causes of the single errors was not possible. However, it seems that in many cases a better design or layout of the equipment from maintainability point of view, or a better work planning, could have prevented the occurrence of the errors.

Direct error types against equipment categories. It is interesting to study the distribution of different error mechanisms against the equipment types affected. Based on results in the Table VII and Figure 7, the share of commission errors in I&C is exceptionally high. In contrast to that, a rather large share of the omissions take place in actions on instrument line block valves (67 % of all IVAL error modes). With regard to the instrument valves, the result could be expected. The amount of wrong settings in I&C and electrical equipment was only approximately 12–13 % of the total, which can be regarded as rather expected.

Here, it is noted the rather high share of qualitative commission errors (COM/OTH) in mechanical equipment (MEC) and valves. In addition, some wrong direction (COM/WD) errors were identified in the group valves (VAL). This was caused by e.g. wrong installation or assembly of components.



Carelessness,other commission errors (COM/OTH), Omissions (OM), Wrong settings (SET), Wrong direction errors(COM/WD)

Figure 7. The distribution of single human error causes among the equipment categories through 1992–1994.

Operational situations at error origin and fault detection. In the following Figure 8, the distribution of single human errors with regard to the assessed plant operating period at their error origin is shown. This question is not an easy one since for the latent single human errors it was very difficult to judge the exact occurrence time. The start-up and shut-down phases are not partitioned in this judgement, because very little maintenance in the plant units takes place during these states of the unit annual operating cycles.

Since most preventive maintenance and modification activities take place during the annual refuelling outage, it is not astonishing that most (app. 62 %) fault records also seem to stem from that period. The conclusion would be hesitating that these human errors are without safety significance knowing the recent Shutdown PSA results [e.g. IPSN 1990, Pyy & Himanen 1993] showing high risk levels during an outage. The more appropriate question is, whether these errors were found before a component was declared operable or, at least, before the plant start-up after the outage. We discuss the latter item more in the following.

The following Figure 9 shows the distribution of the plant operational situations at the time of fault discovery. The judgement of the discovery situation is based on comparison with the historical time instants from the realised time schedules which are presented in the plant annual outage reports. When compared to the earlier Figure 8, the situation is somewhat reversed. Only about 32 % of all single human errors are detected during an outage, whereas app. 60 % during the power operation and 7 % during the plant start-up.

Our reclassification of the type of discovery (preventive/others) originates from the detailed classifications in the plant fault records on the ways of fault detection. Preventive actions such as periodic or functional tests or preventive maintenance actions seem to reveal only approximately 20 % of the single human errors. This low ratio may be explained by the fact that many of these human errors are not directly critical from the safety point of view. The errors are mostly noticed by alarms or through displays in the control room or during plant walk-arounds in various purposes or while working nearby.

It is interesting to compare the detection of the errors that are committed during an outage to those committed during the power operation. The situation becomes clear in Figure 10, where we compare the detection timepoint of those two groups together.

Approximately 51 % of errors induced are also discovered during the outage—indeed, most of them during the same one. However, the residual app. 49 % of the errors remain latent until the plant start-up or even app. 39 % until the power operation. The errors passing into power operation show rather similar distribution into equipment categories as all single human errors. Preventive actions are not very effective, only app. 24% of the errors were detected by them. These results may partly be explained by the fact that a large share of these errors are rather negligible from the safety and economy point of view. However, these faults exist in safety systems, too.

The conclusion drawn with regard to the single errors introduced during an outage yields also to errors during the power operation—about 94 % of them are also discovered during the power operation, but very few in preventive activities. Again, this result can be easily explained by the sample—many single human errors are noticed by alarms, through displays or by chance during routine plant tasks.

The results of the birth of the single human errors and their detection showed that a major part of them follows the formula: birth in outage – detection in outage or remaining latent into the power operation. This result will be compared with the results of the dependent human error analysis in the Section 5.2.

It is interesting to study the time periods from which the single errors done by plant own personnel or foreign contractor personnel originate (cause classes BD and BF, see also Figure 4). It appears that more than 75 % from the errors caused by the foreign labour (class BF) originate from outages. With regard to the single errors classified in the class BD (own personnel), more than 63 % stem from the power operating period, and approximately 18 % were dealing with instrument line block valves.

These figures are significantly more than the

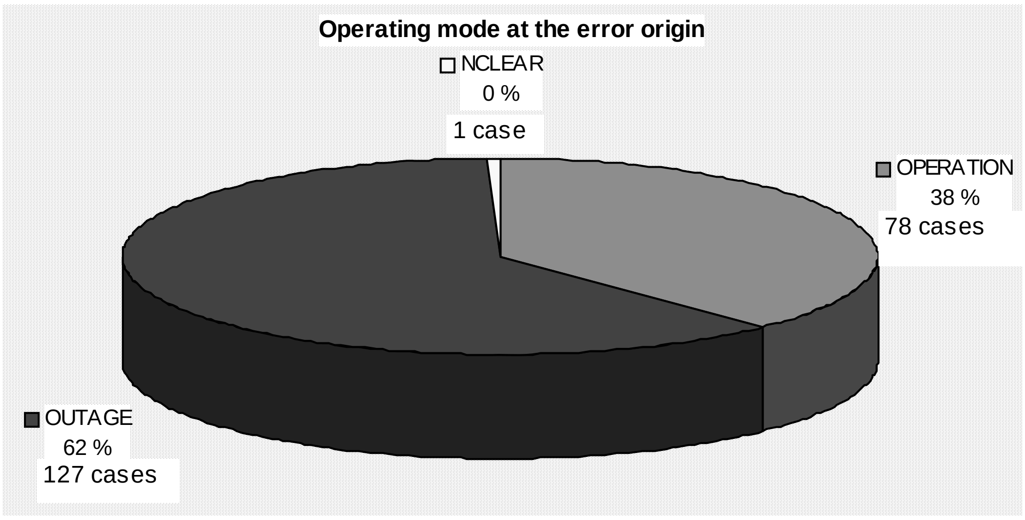
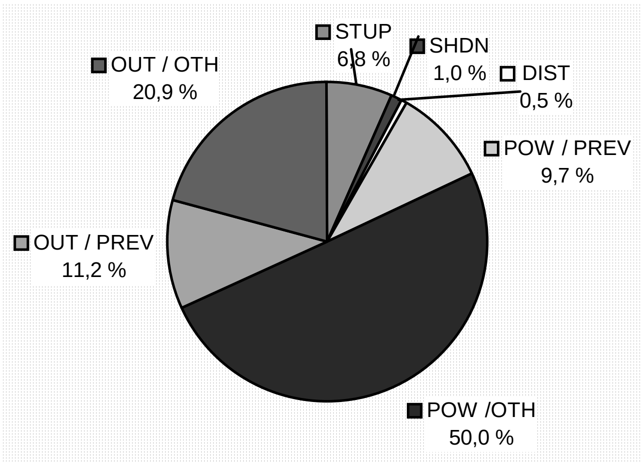


Figure 8. *Plant operating period at the time of error origin, years 1992–1994.*



Type of detection: testing or preventive maintenance (PREV), otherwise (OTH).
Operating states: refuelling outage prior to start-up (OUT), plant start-up (STUP), power operation (POW), plant shutdown (SHDN), disturbance (DIST). The types of error detection are not partitioned in the start-up, shut-down or disturbance states due to the limited share of these states. Totally 206 cases.

Figure 9. *Plant operating state at the time of error discovery, years 1992–1994.*

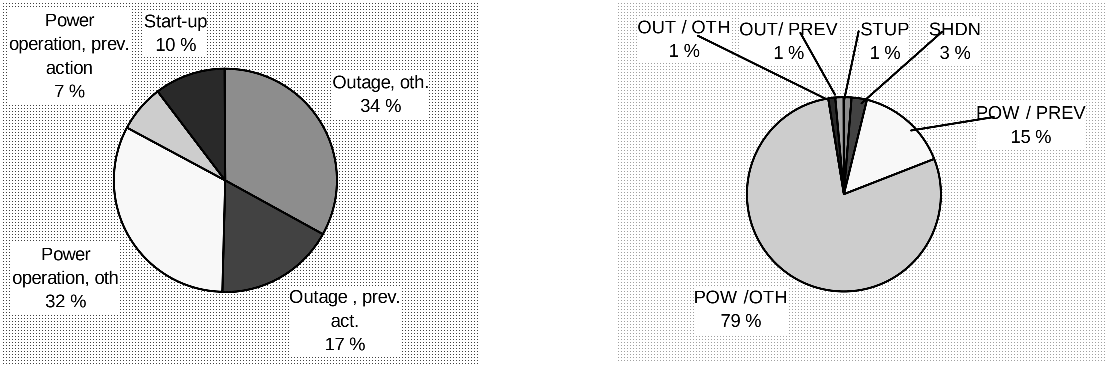


Figure 10. *Plant operating state at the time of detection of 127 single human errors stemming from outages (left) and 78 errors stemming from the operating period (right).*

average for the total 206 single error cases. Otherwise, the distribution of explanatory variables followed roughly that of the total. The results are understandable against the background that the contractors are extensively used during the annual refuelling outage. Moreover, the plant own personnel carries out tests and, to a limited extent, maintenance during the power operation. The small sample size and the overlapping cause categories do not allow any further conclusions.

One further interesting observation was, against the prior belief, that the foreign labour does not cause problems only in non-safety equipment. About 70 % of the BF classified errors were found in safety related systems or in systems that could be used to back-up the safety functions. However, the affected equipment was not critical in all cases and the errors were detected during the outage in more than half of the cases.

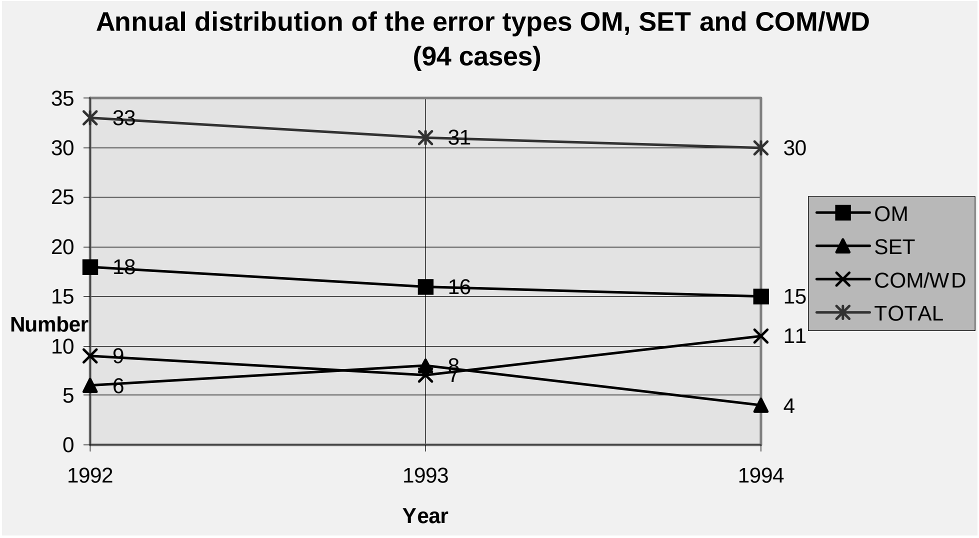
Trends of causes of human errors. One of the aims of the study was to observe the annual trends of the error cause types. The annual numbers are shown in Figure 11.

As seen from the Figure 11, the number of omissions (OM), wrong direction/sequence errors (COM/WD) and wrong settings (SET) remained quite stable through 1992–1994. The annual distributions obtained for OM and COM/WD types of errors are somewhat higher than what was presented in [Reiman 1994]. Reiman discovered in average approximately 10 omissions and 4 wrong direction commissions per year through 1981–1991, whereas the findings of our study are 16 and 9 single errors, correspondingly. This difference is mostly due to the more extensive scope of this study, since the search for human errors covered all the maintenance records and not only those preclassified as human errors at the plant. In the search for human maintenance errors, thus, all fault cause categories should be investigated in order to avoid underestimation.

Although not presented in Figure 11, somewhat less other qualitative commission errors (COM/OTH) were detected in 1994 than for the calendar years 1992–1993. The comprehensive reason for this is hard to tell, although the utility simplified the fault cause classification in the same time. The rougher cause classification in the fault records since 1994 may have made the searching of the human errors more difficult. Due to the short observation period, no firm conclusions about the trend can be drawn.

5.2 Dependent human errors

The analysis of dependent human errors revealed three types of dependencies affecting redundant subsystems. They are human related common cause failures (HCCFs), human related common cause non-critical failures (HCCNs) and human (error induced) shared equipment faults (HSEFs). The two first types can be regarded as real multiple human failures, whereas HSEFs are single human errors leading to multiple



Annual averages: Wrong settings (SET) = 6, Wrong direction errors (COM/WD) = 9, Omissions (OM) = 16,3.

Figure 11. *Annual distribution of selected single human error types through 1992–1994.*

Table VIII. Identified dependent human error related records and their distribution among dependence cases and reported cause categories.

Reported cause category	Fault records	Records referring to human errors, total	Records referring to single human errors	Records referring to HCCFs/ HCCNs	Dependent human error cases HCCFs/ HCCNs	Number of records/ dependence case
A Failure in installation or earlier	500	81	50	12	4	3
B Operating and/or maintenance personnel	214	100	71	13	6	2,2
C Consequence of operation	2741	32	15	8	1	8
D Miscellaneous causes	952	113	70	10	2	5
Total	**4407**	**326***	**204****	**43****	**13*****	**3,3**

* The amount excludes 2 cases later found to be ageing related and 6 cases originating from other utility reports.

** The amount excludes 2 reports not coming from the maintenance records, together 206 single human error cases.

*** Excludes 1 case not identified in the fault history records—no cross-classification inside the dependence case was found.

consequences due to the system design.

The number of HCCFs and HCCNs discovered is compared to the total number of fault records and single human errors in Table VIII. HSEFs are discussed briefly in Section 5.3 (Shared equipment faults and other dependencies).

Apart from these, some recurrent errors and errors taking place in different systems or non-redundant components, were found in the course of the HCCF identification. According to the principles presented in the Table V, they were classified as single failures. A thorough investigation of all these other dependence mechanisms would have required still considerably more resources, which was evaluated not to be justified in this study when compared to their safety significance.

Dependent human error related records. As seen from Table VIII, dependent human error cases can be found in all cause categories (A,B,C, and D) used by the utility maintenance foremen. The results suggest that an approximate number of fault records covering human related dependencies (HCCFs and HCCNs) is about 1 %. However there are in average more than 3 fault records per revealed dependence case.

In this number the single human errors, introducing multiple consequences due to e.g. system interdependencies or shared equipment faults (HSEFs), are not calculated.

In the following Table IX, the identified and analysed HCCFs and HCCNs are listed together with a short title description, the affected equipment type and the individual plant unit.

Dependent human error cases. The division of the human related dependent errors (HCCFs and HCCNs) into the different plant units was rather difficult. This difficulty was caused by e.g. the differences in the coverage of the reporting of the corresponding errors influencing the both units.

At least in 3 cases similar dependence mechanisms on redundant components appeared at the both units. Four HCCFs and one HCCN were identified to affect only the unit I. Two HCCF cases plus four HCCN cases were identified in the unit II, solely. The both HCCF cases affecting the unit II solely also led to single failures in the unit I.

Equipment types affected by the dependent human errors. In the following Figure 12, the equipment types affected by the dependent human errors are presented. As seen, the dominance of the instrumentation accompanied by the electrical equipment, already seen in Section 5.1, also applies to the dependent human errors. No other equipment types than these two are present in the

Table IX. *List of analysed HCCFs and HCCNs through years 1992–1994.*

Nr.	TITLE OF THE CASE	UNIT
	Human related Common Cause Failures (HCCF)	
1.	The trip limits lowered on wrong neutron flux trip conditions. (IC)	Olkiluoto I
2.	Neutron flux trip limits left too low after valve self-closure test. (IC)	Olkiluoto I
3.	Power cables cut to the supply pumps of the diesel fuel tanks. (EL)	Olkiluoto I
4.	Difference pressure measurements crosswise connected in mussel filters. (IC)	Olkiluoto I + II
5.	Couplings broken between actuators and control valves. (IC)	Olkiluoto I
6.	The actuation times too long due to mineral oil impurities in the anchors of the solenoid valves. (EL)	Olkiluoto I + II
7.	Simultaneous work in two subsystems of the auxiliary feedwater system during the refuelling outage of unit 2. No experience feedback to the refuelling outage of unit 1. (IC)	Olkiluoto II (+TVOI)
8.	Turning pieces of flow measurement devices mixed after cleaning. (IC)	Olkiluoto II (+Olkiluoto I)
	Human related Common Cause Non - critical failures (HCCN)	
1.	The temperature measurement values of the bearing pads of the turbine set too low. (IC)	Olkiluoto I
2.	The protective coverings broken in the power supply cables of solenoid valves. (EL)	Olkiluoto II
3.	Air left in instrument lines of the pressure difference measurements 323K201-K204 of the suction strainers. In addition unnecessary alarms. (IC)	Olkiluoto II
4.	Wrong settings of the piston position indications of the operating oil pressure accumulators 416A502 and A504 due to start-up problems. (IC)	Olkiluoto II
5.	The signal lights of the operating oil pressure accumulators 416A501.20 - A504.20 do not indicate due to wrong settings. (IC)	Olkiluoto II
6.	The air pressure correction was lacking in the calibration method of the temperature monitoring limit switches. (IC)	Olkiluoto II+I

Type of equipment given in Italic. Single error in the other plant unit given in parenthesis.

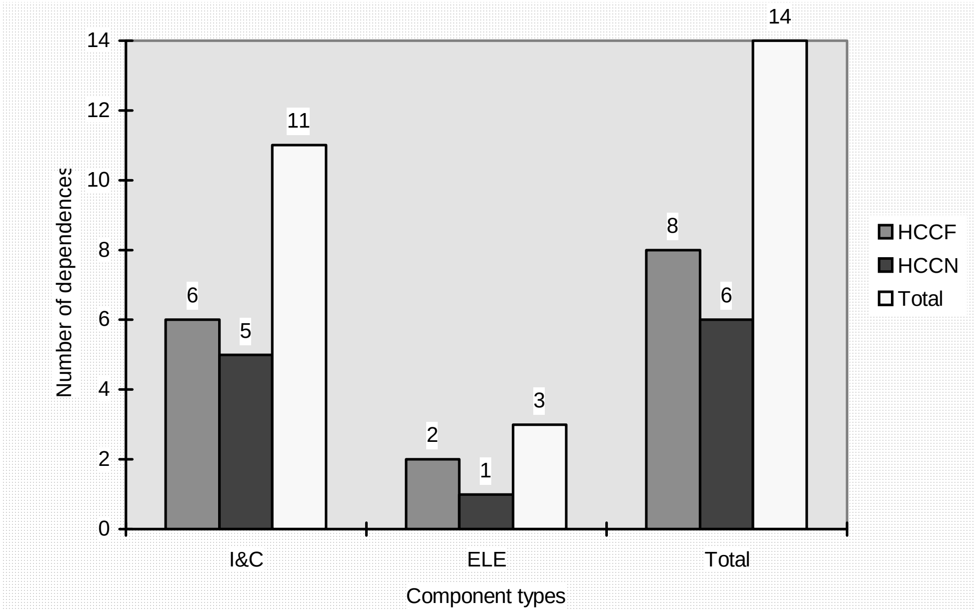


Figure 12. *Distribution of the HCCF and HCCN cases among the equipment types. All of them belonged to either instrumentation or electrical equipment.*

identified HCCFs and HCCNs. The results underline the need to put more emphasis on these equipment types and systems in future safety studies.

When considering remedial actions, it has to be taken into account that, due to complex organisational interactions, that also personnel from other trades than those pointed out have contributed to the origin and appearance of these dependent errors.

Direct causes of dependent human errors. As regards to the error cause categories, some differences exist when compared to the single human errors (Section 5.1, Figure 6).

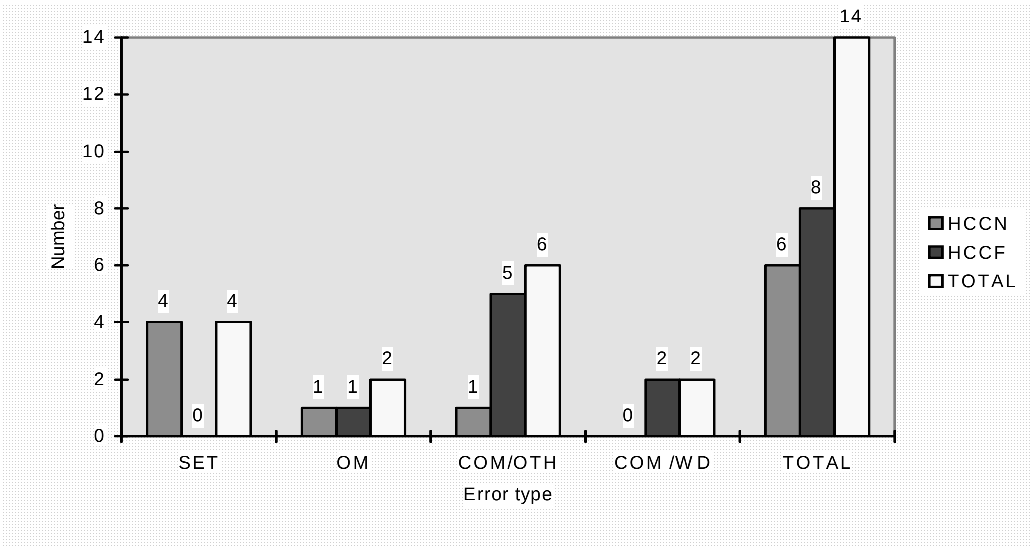
The dominant error category is, again, commission. Consequently, the category of commission errors (COM/OTH), exhibiting qualitative and coordination problems, appears as the most frequent direct cause (6 cases, 42 %, of which 5 HCCFs). Also dependent wrong direction and order errors (COM/WD) appear in two HCCF cases. In addition dependent wrong settings (4 cases, 29 %) is a usual category, but all those cases appear to be non-critical HCCNs.

The results show that the role of the wrong settings is, anyway, more important on the dependent errors than on the single errors. It is worth mentioning that, in the course of detailed analyses and interviews of this study, many dependent mechanisms, first regarded as wrong settings, could be screened out. This was due to the fact that they, actually, were found to be caused by ageing and lack of preventive maintenance, too. In the utility fault records, they were originally classified as deficient settings. Should their analysis be carried out on a superficial level, the wrong settings would have dominated as the causes of the dependent human errors.

Operational situations at fault detection. The following Figure 14 presents the detection states of the dependent human errors in the case that they were born during the outage time.

No graphical presentation is given to those 3 dependent error mechanisms born during the power operation, although they were HCCFs. Two of these HCCFs were introduced in relation to modifications installed during the power operating period. One of them was detected in a periodic test and the two others by help of alarms as a part of routine activities, during the power operation. The detection modes of the dependent errors born in outages are very interesting. With regard to the single human errors, about 40 % remained undetected until the power operation even after startup (Section 5.1, Figure 10). A larger part of dependent errors seems to remain latent, since from all dependent errors, as well as from the HCCFs, about 60 % remained undetected at least until the start-up, which appears somewhat surprising.

However, one has to bear in mind that the



SET = Wrong setting, OM = Omission, COM / OTH = other qualitative commission error,
COM / WD = Wrong direction error.

Figure 13. *Distribution of the cause categories among the HCCF and HCCN cases.*

database is rather small, when dependencies are studied. This limitation does not overrule the fact that a large proportion of the dependencies has remained undetected and even one of them has been discovered through a reactor scram and another by alarms bringing repeated stops to the start-up of the unit.

Origin and detection of the dependent human errors. A thorough treatment and analysis of the dependent human errors allowed to make further inference about their birth and discovery mechanisms. Modifications seem to be an important source of dependencies with the share of about 50% (7 cases). The distribution among other source activities is more even as can be seen in the Figure 15.

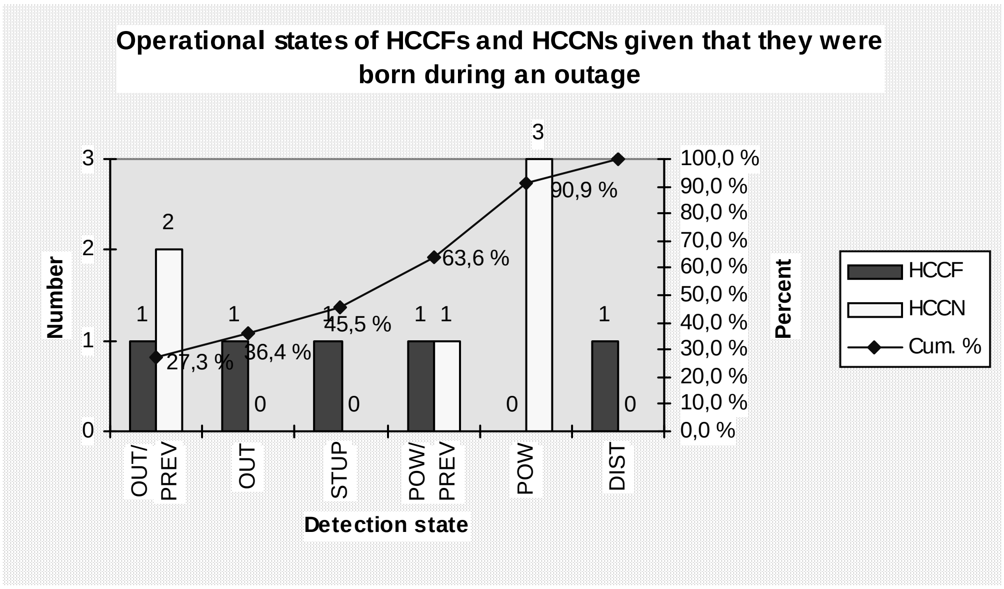
The result is interesting from the safety point of view, because it is difficult to know which kind of hazards are due to new equipment requiring new designs, system interactions, skills and practices. However, utilities carry out extensive start-up tests on their new equipment. In future, even a more comprehensive project coordination, design and start-up testing of the backfittings and modifications would, apparently, facilitate better results.

It has to be kept in mind that all the equipment affected by these dependence mechanisms were I&C or electrical related. Therefore, especially the installation, maintenance and design of these equipment and their interrelationships with other items, including also instrument lines and mechanical parts, deserve more attention.

Another side of the above Figure 15 is the detection situation of the dependencies, completing the Figure 14. Although periodic testing causes sometimes dependencies, it reveals here more than induces. Thus, the discussion on whether the amount of testing should be decreased does not receive support from this study without a further effort. Otherwise, central alarms and shift walk-arounds through local alarms have contributed to detection of a significant share of the dependent errors.

Apart from the detailed original error modes, also the underlying contributing factors were studied, as shown in the following Figure 16.

Weaknesses in work management and planning seem to contribute as underlying causes into occurrence of dependent human errors in the half of the cases. In the most cases these problems occurred in relation to modifications, but also



OUT/PREV = Detected by preventive action during outage, OUT = Otherwise detected during outage, STUP = Detected by start-up, POW/PREV = Detected by preventive action during power operation, POW = Otherwise detected during power operation, DIST =Detected through plant disturbance.

***Figure 14.** Distribution of the fault detection states of the human related dependencies given that they were introduced during an outage period (11 cases).*

through preventive maintenance actions during an outage. These underlying causes are partially interrelated with weaknesses in project co-ordination and poor designs from the maintainability point of view. The underlying contributing causes “insufficient knowledge” exhibit the usefulness of the available knowledge of specialist technical personnel at the suppliers or the utility in problem solving.

Significance of dependent human errors. An important topic to study is the safety significance of the dependent human errors. This evaluation can be based on many criteria, such as PSA importance measures and safety classification of the equipment. From the dependencies studied here, 9 of the 14 cases were related to safety systems. 6 of these 9 dependence cases were related to instrumentation. In addition, 6 of the 8 HCCF cases were in safety related systems. In the light of these results, the risk significance of the dependent human maintenance related errors should not be underestimated.

A closer look at the distribution of dependencies showed that in at least 3 cases both the plant units were affected by them. Two cases were HCCFs in safety related systems. Besides, in at least 2 cases more than one system and in at least 10 cases more than 2 components were affected by the dependence mechanisms (including the prementioned classes). This manifests the fact that, in I&C systems, a dependence mechanism may result in a wide spread of consequences.

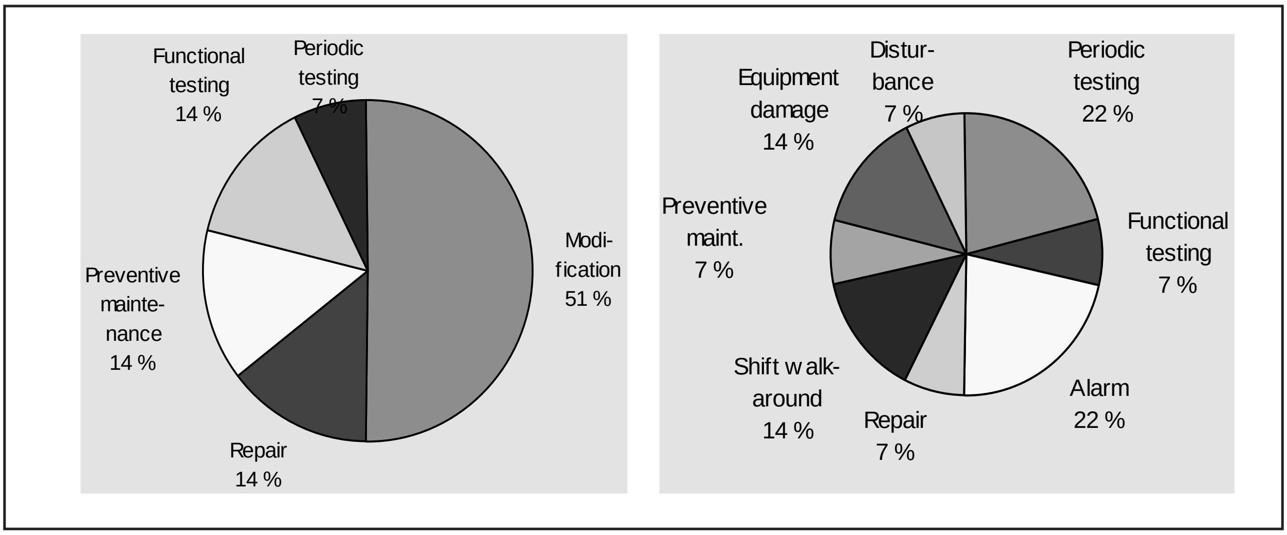


Figure 15. The erroneous task (left) and detection activity types (right) of the dependent human errors.

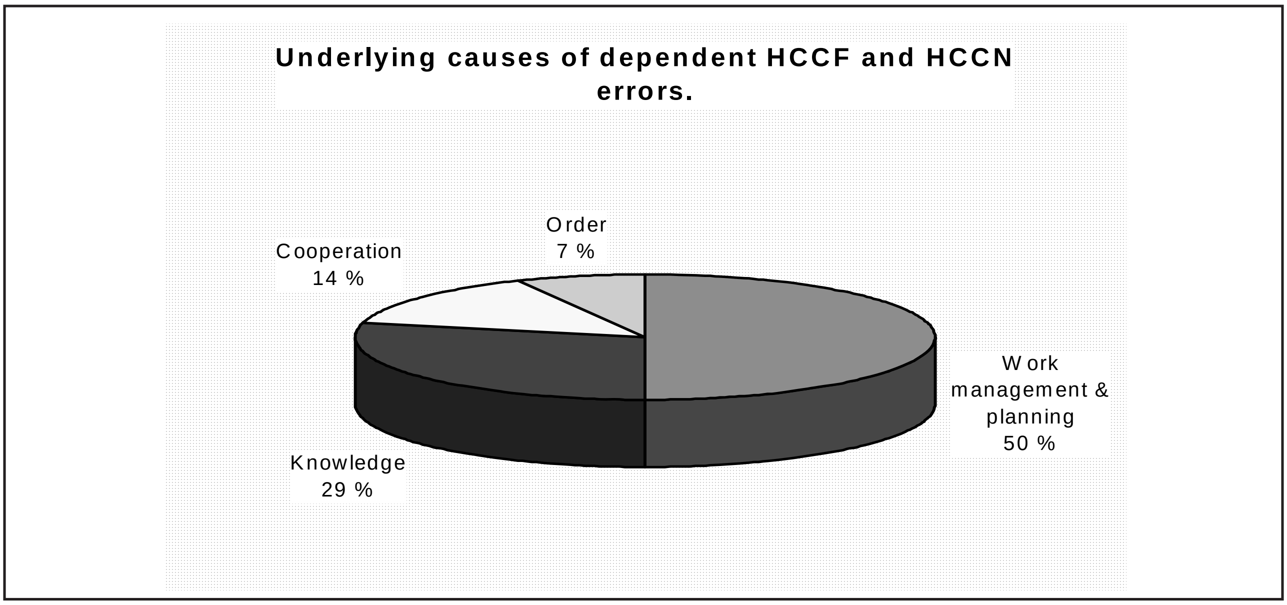


Figure 16. Underlying causes of dependent human errors (14 cases).

The number of the dependent human errors. The annual average of the dependent human errors (sum of HCCFs and HCCNs) through 1992–1994 is app. 2,3 cases per year, as shown in the following Figure 17. One almost similar HCCN mechanism was reported during two different calendar years, and it is, consequently, counted twice.

It is interesting to compare the results obtained here to those of [Reiman 1994]. That study reported the annual average of approximately 2,4 dependent human errors from the 11 year long observation period. The small difference may be due to the fact that multiple human errors are mostly reported also in other forms than fault records, which shows a good safety culture of the utility.

In the Figure 17 a slightly increasing trend appears in the number of dependent human errors (HCCFN = HCCF + HCCN). However, it is too early to make such a conclusion in the light of the small sample and the short observation period. It should be noticed that the above Figure 17 also presents the number of the identified human related shared equipment faults (HSEF). The HSEFs are discussed in the following section 5.3 of this report.

Weaknesses in the protective barriers. In the following Figure 18, the occurrences of ineffective operative and organisational barriers against human related dependencies (HCCFs and HCCNs) are compiled. The operative barriers are checks and tests performed by the personnel directly involved in these preventive tasks.

In the thorough analysis of the dependent human errors it was searched for broken operative barriers in the HCCF and HCCN cases. For the statistical compilation of the cases one broken barrier per case was selected. As can be seen from the Figure 18, and understood from the root cause analyses, the highest potential for enforcement of the operative barriers can be identified in the start-up testing of modifications and in the installation checks of the maintenance actions in connection to the outages times.

The organisational protective barriers against dependent human errors are checks, reviews and proactive actions performed by engineers, managers or safety and quality control personnel not directly involved in the operative work in the plant units. In this simplified barrier analysis, it was looked for one or two broken organisational barriers per each HCCF and HCCN case.

An enhancement of the coverage of the start-up test programs, for better detection of failure modes introduced in relation to modifications, has a significant potential to reduce the consequences of dependent human errors. In addition, an enhanced feedback of experiences from commission errors in preventive maintenance actions into the training of contractor personnel, could reduce the occurrence of specific maintenance related multiple human error cases in the future. Also some specific weaknesses in the work management and work order processes have facilitated errors to pass through into dependent failures. The identi-

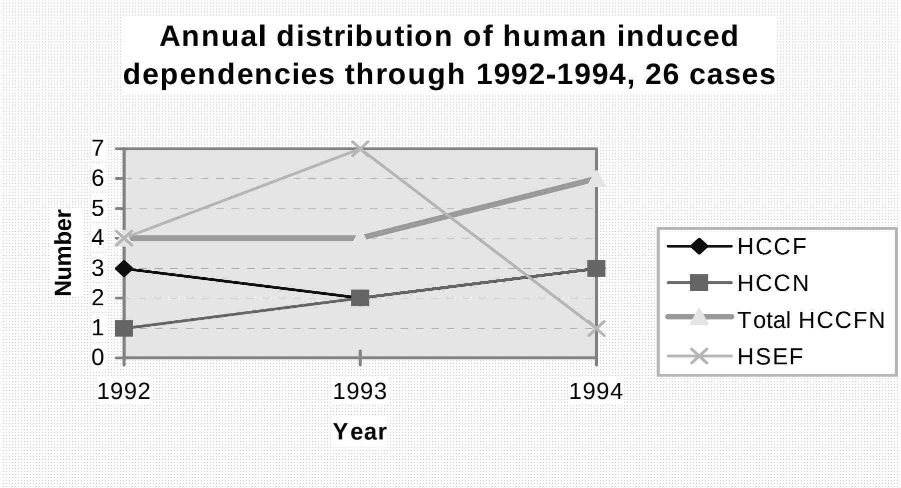


Figure 17. *Annual distribution of HCCFs and HCCNs through 1992–1994. Totally 14 cases, since one almost similar HCCN mechanism was distributed over two years of time.*

fied specific weaknesses in the organisational protective barriers against multiple human errors exhibit also a potential opportunity to enhance the project co-ordination and review from the design up to and including the start-up testing of modifications.

5.3 Shared equipment faults and other dependencies

Apart from the analysed single human errors and dependent human errors, the studied data contained several cases that could not easily be classified into either class. As discussed earlier, a number of ageing mechanisms, contributing to wrong settings in instrumentation and electrical equipment, were found. Also lacking preventive maintenance and poor design were identified as contributors to some ageing related dependent non critical failures in mechanical equipment. Moreover, two software errors and some other human induced mechanisms, causing parallel faults or initiating events, were discovered. Since the detailed treatment of such dependent failures does not belong into the scope of this study, they are not discussed in the following.

Human related shared equipment faults. In specific cases, single human errors affecting shared equipment have caused multiple consequences on different subsystems or parallel components. Those single human errors that have caused multiple component faults were classified as human shared equipment faults (HSEFs). A part of the HSEFs are also cascade failures, e.g one single loose joint of a manometer has resulted recurrently in nitrogen pressure drops in parallel operating oil accumulators. Also cables belonging to two different direct current subsystems within one electronic cubicle, or four LPRM detector cables collected into bundles, have been affected by careless single actions during maintenance or testing performed in limited work spaces. In order to simplify the presentation of these additional analysis results, the critical or non-critical shared equipment faults were treated as one HSEF group in the following statistics.

Together 12 HSEFs were identified, of which 3 cases were omissions and 7 cases other commissions than wrong direction errors. All the omissions were cases, where one single error, e.g. forgotten restoration (mentioned in work permit) or missed section in instructions, led to multiple consequential omissions. Otherwise the distribution of error types and equipment involved roughly follows the distribution of other single human and dependent errors (HCCFs and HCCNs), as shown in Figures 6 and 13. Again, it should be noticed that the HSEF type errors affecting instrumentation have not only occurred in the work which is specific for the maintenance group of I & C.

A graphical presentation of the annual number of HSEFs was already shown in Figure 17. The low number during 1994 may be due to incomplete identification, as already discussed in relationship to Figure 11 of this report.

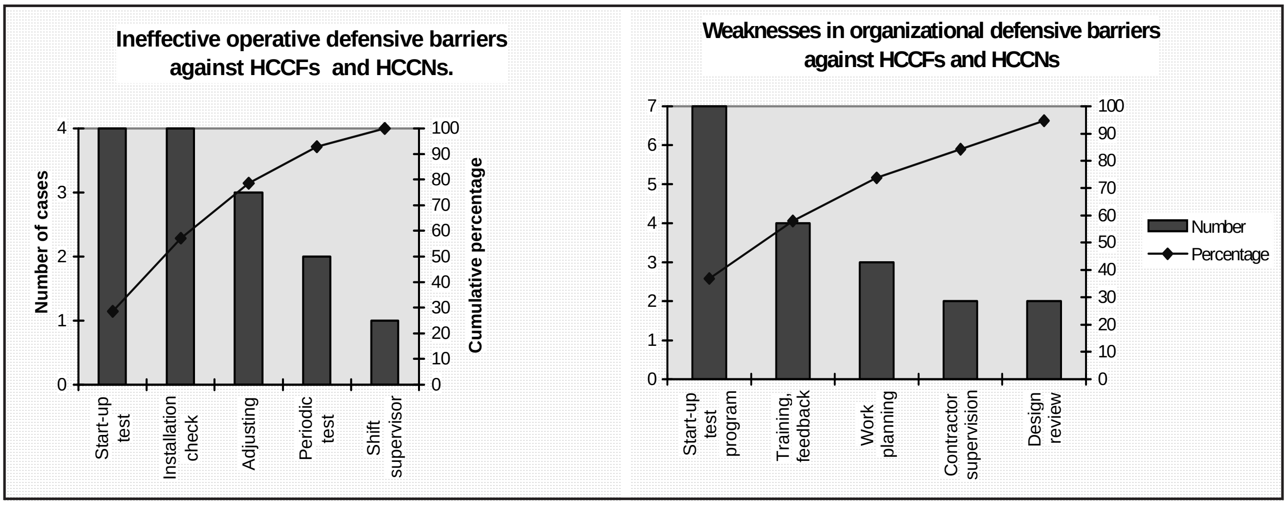


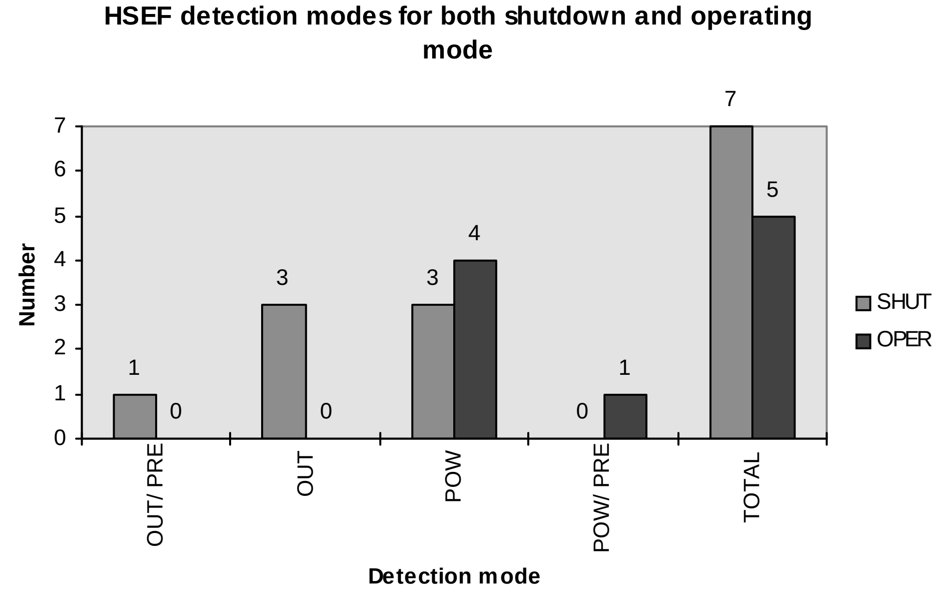
Figure 18. Weaknesses in operational and organisational barriers identified in relation to dependent human errors (14 cases of HCCFs and HCCNs).

Table X. Annual number and distribution of human related shared equipment faults (HSEFs) into equipment types, error types and fault detection states.

Year	Number	Equipment type	Number	Error type	Number	Detection state	Number
1992	4	I & C	10	SET	1	POW/PREV	1
1993	7	EL	1	OM	3	POW	7
1994	1	VAL	1	COM/WD	1	OUT/PREV	1
				COM/OTH	7	OUT	3
Total	**12**		**12**		**12**		**12**

The Table X shows that eight HSEFs have been identified during the power operating state. However, as seen from Figure 19, only 3 cases (42 %) of those born during an outage have remained latent until the power operation. All those HSEFs caused during the power operation were also detected in that operating state. As an analogy to single errors, preventive actions have been rather insignificant detection means with only a share of 17 %.

Apart from the aforementioned mechanisms, many recurrent faults or problems and vague situations allowing multiple interpretations were found in the database. Based on the “Principles followed in the classification of human error data” in Table V, some of the human induced dependent failures could not be regarded as HCCFs, HCCNs or HSEFs. In three cases, where the human origin of the dependence was evident, the decision to classify them into the class “other dependencies” was made. Examples of such cases are: the wrong direction in welding of reactor scram system degasing valves (discovered before the work permit was returned), forgetting to tighten the handweels of two valves belonging to two different cylinders of one boron pump (dependent errors inside the component boundary) and wrong line-up of a drainage valve after modification (two rooms contaminated). In the cases, where the dependence remained unclear even after the interviews, single errors were assumed.



SHUT= refuelling outage period, OPER= power operation period

Figure 19. Distribution of the fault detection states of human induced shared equipment faults according to the plant state at the birth of the error.

6 DISCUSSION ON DATA UNCERTAINTIES

The number of faults and errors. The fault records read through covered about 4400 cases from the years 1992–94. This number of the records seems superficially to be very high, but is as evaluated closer comparable with the amount of similar reports from the other Nordic NPP units (compare with TUD 94-11). However significant differences in the number of the failure records between different Nordic plant units are found due to the different number of components per unit, different strategies on preventive maintenance and different criteria for the coverage of the reporting of failures, degradations and other findings in the "fault" records.

Uncertainties in cause coding and identification of errors. The most significant uncertainties in the results of this work are related to the data and its uses, i.e., identifying human errors based on the fault records and classifying them afterwards. The aim of the descriptive text documented in a fault record is to report briefly the fault discovery for consideration and preparation of a work order and to describe briefly the corrective maintenance action performed. Therefore it is often difficult to identify the human errors as fault causes from the text of the failure reports only, as discussed in the Section 4.2 of this report.

The detailed cause coding in the work order feedback information, when correctly defined, supported in many cases the identification of the human errors from the years 1992–93. The detailed scheme was abandoned in 1994, based on the changes done in the reporting requirements for new Nordic Nuclear Power Reliability Data System [TUD 1994]. The simplification in the cause classification left only the rougher cause categories A, B, C and D in use, but the fault type "human error" was added into the related classification list of fault types. But the human errors contribute to technical faults which are mostly suitable to be selected from the classification scheme of the fault types. In Figure 20, the origin of identified 206 single human error cases from the four different cause categories is shown for the calendar years 1992–1993 and 1994 respectively.

As seen in Figure 20, the number of single human errors decreased in 1994. Especially, this meant that the cause category B, "Operating and/or maintenance personnel", was identified less than in 1992–1993 as a fault cause. This may be explained by the fact that the use of the rough classification only may confuse the personnel, since the rough cause categories without an explanatory breakdown are heavily overlapping, at the first sight. Another generic factor will also decrease the credibility of the classification in overall: The personnel who perform the classification based on the feedback of the fault (after the repair), seem not to have any feedback from the utilisation of their cause classification. This was taken into account by screening all the faults instead of the pre-classified "Operating or maintenance personnel" related faults only, which contributed to an identification of a larger number of single human errors than expected in 1992–1993. However, it should be noticed that the quality and contents of the used plant maintenance records is very good when compared with the experiences achieved during international studies such as [NEA/CSNI 1995].

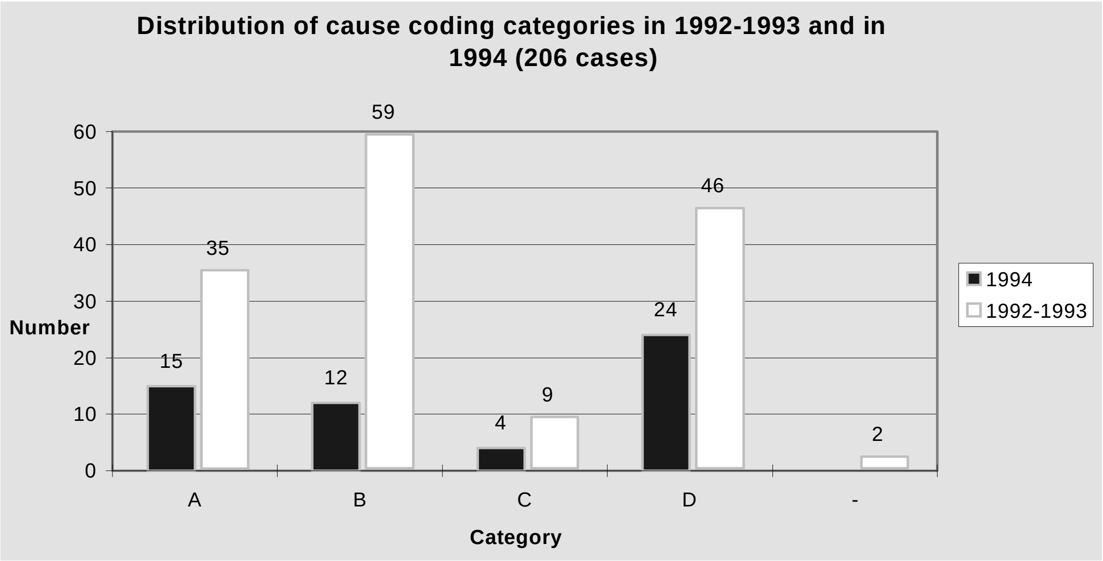
Another observation was that the decrease in COM/OTH type errors (other commission errors than the wrong direction errors) explains almost solely the decrease of the identified single human errors in 1994 (see also Figure 11 and the text in relation to that). On the other hand, the number of reported dependent human errors has remained rather stable through 1992–1994. A further analysis of this phenomenon is left outside this report, since no single factors can be found contributing significantly to the effect.

The cause categories in the fault records do not address the contemporary (simultaneous) faults in redundant or similar components. This may partially contribute to the fact that some dependent mechanisms remain unnoticed at the plant unit and in our follow-up analyses of fault records. Such dependent error mechanisms are difficult to identify, if they were not identified in relation to the periodic tests of safety systems as susceptible CCFs or analysed otherwise in relation to significant operational or damage events. Besides, at the outset of the study the target was set to identify dependent human errors causing faults in redundant components or subsystems. This led to the result where otherwise correlated dependence mechanisms where left outside an accurate consideration and may in some cases appear as single errors. Finally, it has to be said that in some cases the amount of correlation between some human errors was rather difficult to define and, consequently, they were classified as single ones.

The human error type classification used in our study was not very detailed. More detailed taxonomies, presented in e.g. [Reason 1990], would have required still more work and the classification results, might still have been rather uncertain for the single errors.

Other data sources. The authors wish to express that there are also other data sources that may be used to complete the results, e.g., quarterly reports, annual outage event reports, scram reports, test and calibration protocols, control room log books, detailed work orders and modification data. This information was utilised to a limited extent or not at all in the study. The reason for this was to limit the effort. For example, finding evidence from the calibration protocols requires a great deal of resources of an experienced researcher.

Detailed statistical significance testing was left outside this report. This is supported by the fact that in most cases the influences were clear and could be inferred otherwise. In future, some statistical tests may be carried out in order to study the information further as a basis for the PSA data.



A=Failure in installation or earlier, B= Operating or maintenance personnel, C= Consequence of operation, D= Miscellaneous causes, - = Not included.

Figure 20. *The origin of the identified single human errors from the plant classified cause categories.*

7 CONCLUSIONS AND RECOMMENDATIONS

Conclusions. The study was capable to produce useful results as pinpointing areas for justified consideration of remedial measures. Also interesting results for the organisational learning, experience feedback and training were achieved.

The single and dependent human errors showed rather similar behaviour with regard to the explanatory factors on instrumentation and electrical equipment. Instrumentation, automation and electrical equipment seem to be prone to human errors, partly due to their vulnerability and partly to the complexity of their influences. Human errors and human common cause failures related with instrumentation dominated the results. This supports the view that more emphasis should be given to the safety and work management of complex instrumentation and protection systems and equipment. It should also be noticed that the mechanical equipment was affected by single maintenance related errors only, but significantly by qualitative human errors including use of too much or too little force.

When considering remedial actions, it has to be taken into account that also personnel from other trades than instrumentation have contributed to these instrumentation related errors. Many of the results were expected, e.g. that the most maintenance related errors stem from the refuelling outage period. But it was surprising that many of the faults remain undetected until the power operation. In the common cause failures, the plant modifications are an important source class. That is the main reason, why enhanced project coordination, post-installation check-ups and start-up testing programs are suggested to further decrease the amount of dependent errors.

Partially this objective, and an enhanced information transfer between the different organisational branches, could be achieved by e.g. introduction of formal turn-over and acceptance procedures, consisting of checks and reviews, between the project phases of the modifications in a rather similar way as applied for the technical systems during the erection and start-up phase of the plant. An enhanced responsibility and involvement of the operation and maintenance personnel in the decisions and reviews during the early phases of the modification projects could also support better the erection, operability and maintenance targets of the modification.

In addition, the ongoing equipment responsibility related developments of the utility have a potential to enhance the commitment of the maintenance personnel and thus reduce further the human errors in relation to maintenance. The safety related training of maintenance personnel is however more heterogeneous than the one the operating crews receive, and the need of better training has often been discussed.

In a limited number of specific cases, single human errors have caused multiple consequences on different subsystems or parallel components. Those so called human shared equipment faults are of interest both from the safety and potential design improvement point of view. E.g. multiple components in limited work spaces, and technical dependencies of parallel equipment of shared components, have contributed to multiple failure consequences of single maintenance or testing errors.

The safety significance of the human errors in relation to maintenance. A significant number of human errors and common cause failures took place in safety related systems, but not all of them were functionally critical. E.g. 6 of 8 cases of the human related common cause failures, and 3 of the 6 human related common cause non-critical failures, were in the safety systems. It should be noticed that 6 of the 9 dependent error cases were in the safety related systems. In 10 of the 14 dependent error cases more than 2 components were affected. In at least two human common cause failure cases in safety systems two plant units were affected.

Although no risk increase factors by using PSA models [NKA/RAS-450 1990] were calculated, it can be concluded that human errors in relation to maintenance and modifications apparently may have a significant safety influence. But much more safety degradation would be caused if no maintenance took place, which is shown by e.g. the ageing related common cause failures due to lack of preventive maintenance identified during this study. Modifications were shown to be complex and error prone and thus enhancement of the principles of their decision making and their review should apparently be considered .

Experiences from the study. The study was rather unique since a large amount of plant specific maintenance data, and practical knowledge from the maintenance and operation personnel, was used as source information for systematic search and analysis of human errors and common cause failures.

The maintenance history database of the utility was very useful. The constructed EXCEL based database on follow-up analyses of the utility's maintenance history records was very flexible and allowed many kinds of information retrievals and sorting.

A number of ageing mechanisms, contributing to parallel wrong settings in instrumentation and electrical equipment, were found in this work. Also lacking preventive maintenance, often in interaction with poor design assumptions, were identified as contributors to specific ageing related dependent non-critical failures in mechanical equipment. Although left outside the scope of this report, these degradation mechanisms should preferably be studied in detail in other ageing and maintenance related R& D projects.

Identification, description and classification of fault causes is a controversial topic possibly due to limited possibilities of the maintenance foremen to thoroughly investigate the faults locally in the plant and analyse the root causes. In addition, the multiple failures should preferably be introduced in the classification list of the fault records. The ongoing equipment responsibility and maintenance analysis developments of the utility have the potential to increase the motivation of the maintenance and operation personnel for enhanced experience data recording and fault investigation. However, the use of advanced classification taxonomies cannot be the responsibility of the maintenance foremen, but these tasks belong to the systematic maintenance follow-up analyses more suitable to be started by other personnel responsible for maintenance, availability and safety assessments and developments.

The amount of the development, screening, analysis and reporting work in this study was more extensive than expected. Based on these developments and experiences a less resource demanding and simplified screening and analysis model could be defined for routine use.

Thorough analyses of the origin and dependence of the errors, and identification of the weaknesses in the operative and organisational protective barriers against them, were done for the dependent human errors for learning and statistical treatment purposes.

The available data analysis bases allow additional analyses of human reliability data, shared equipment faults and ageing caused dependent failures for PSAs and quality developments of maintenance activities and modification projects. The constructive co-operation of the maintenance and operability personnel of the utility has shown that a wider utilisation of this kind of accumulated maintenance experience and knowledge base can be recommended in the future.

REFERENCES

Berman, J. 1994. Human error dependency. HFRG Human error dependency subgroup. SRD Association Symposium on Human Factors in Safety and Reliability: Risley. 26 May 1994. 15 p.

IPSN 1990, A probabilistic safety assessment of the standard French 900 MWe pressurized water reactor EPS 900. Main Report, Institut de protection et de surete nucleaire,April 1990. 257 pp.

ESReDA, 1995. Guidebook on the effective use of safety and reliability data. SFER, Paris, France. ISBN: 2-9509092-1-3. 399 pp.

IEC 50(191) 1990. International electrotechnical vocabulary (IEV). Chapter 191: Dependability and quality of service. First edition 1990-12. 112 p.

Hänninen, S. Laakso, K. 1993. Experience based reliability centred maintenance. An application on motor operated valve drives. STUK-YTO-TR 45 report. March 1993. 51 p. + app.

Jänkälä, K., Vaurio, J., Vuorio,U. Plant specific reliability and human data analysis for safety assessment. In proceedings of the International Conference on Nuclear Power Performance and Safety. IAEA - CN-48/78. Vienna. 28 Sept.–2 Oct. 1987.

Kay, H. 1951. Learning of a serial task by different age groups. Quarterly Journal of Experimental Psychology 1951:3.

Laakso, K., Simola, K., Pulkkinen, U. 1993. Assessing the reliability of maintenance. Features in Nuclear Europe Worldscan 9–10/1993. p. 36.

Laakso, K. 1984. Systematisk erfarenhetsåterföring av driftstörningar på blocknivå. (A Systematic Feedback of Plant Disturbance Experience in Nuclear Power Plants.) Thesis for the degree of Doctor of Technology. Helsinki University of Technology. Institute of Energy Engineering. Otaniemi. Finland. 1984. (In Swedish. 15 p. executive summary in English).

Maqua, M. et al, 1996. Human factor related common cause failure, Part 1. Report from the Expanded Task Force on Human Factors. Principal Working Group 1 of the Committee of the Safety of Nuclear Installations. OECD Nuclear Energy Agency. La Seine Saint-Germain. Report NEA/CSNI/R(95)/Part1. General distribution OCDE/ GD(96)8. 25 p.

Mokka, R. 1966. O&M Cost Management in TVO NPP. Nuclear Europe Worldscan. Vol. XVI. No. 11-123, November–December, 1996. P. 46.

NKA/RAS-450. (1990). Optimization of technical specifications by use of probabilistic methods. Final report of the NKA project RAS-450. Prepared by a team consisting of : Laakso, K., Knochenhauer, M., Mankamo, T., Pörn, K. NORD 1990:33 report. p. 32–54. ISBN 87 7303 422 3.

NKA/RAS-470. 1990. Dependencies, human interactions and uncertainties in probabilistic safety assessment. Final report of the NKA project RAS-470. Edited by Hirscberg, S. NORD 1990:57 report. p. 2-1-2-65. ISBN 87 7303 454 1.

Norros, L. 1995. An orientation-based approach to expertise. In Hoc J-M. Cacciabue, P.C., Hollnagel, E., Expertise and Technology: Cognition and human-computer co-operation. Hilsdale, NJ. Lawrence Erlbaum Associates.

OECD/NEA/CSNI/R(92)18. 1993. State of the Art of Level-1 PSA Methodology. A task report prepared by a task force of PWG No 5 of CSNI. Edited by R.K. Virolainen. Restricted OECD Nuclear Energy Agency report. France. January 1993.

OECD/NEA/CSNI/R(95)9. 1995. Evidence of ageing effects in certain safety related components. Volume 1: Summary and Analysis. A Generic study performed by Principal Working Group 1 of the Committee on the Safety of Nuclear Installations. September 1995. 68 p.

OECD/CSNI/R(95)10/Part 1. 1996. Human factor related common cause failure, Part 1. Report from the expanded task force on human factors. OCDE/GD(96)8. 25 p.

Paula, H. 1995. On the definition of common-cause failures. Technical note. Nuclear Safety. Vol. 36. No1. January–June 1995. P. 53–57.

Pyy& Himanen 1993. Shutdown risk analysis—lessons and views, SRA Europe, Fourth Conference, Rome, Italy 18th –20th October, 1993.

Pyy, P., Saarenpää, T. 1988. A method for identification of human originated test and maintenance failures. Presented at the IEEE 4th Conference on human factors and power plants: Monterey. California. 5.–6.9.1988. NKS/RAS-450 report. 5 p.

Rasmussen, J., 1979. On the structure of knowledge—A morphology of mental models in man-machine system context. Tech. Report No. RisØ-M-2192. Roskilde, Denmark: RisØ National Laboratory.

Reiman, L., Norros, L. 1994. Organizational assessment of maintenance department at a nuclear power plant. In proc. of the PSA II. March 20–24, 1994. San Diego. 107:7–12.

Reiman, L. 1994. Expert judgment in analysis of human and organizational behaviour at nuclear power plants. Helsinki: Radiation and Nuclear Safety Authority (STUK). Thesis for the degree of Doctor of Technology. STUK-A118 report. 226 p. ISBN 951-712-012-5.

Reiman, L. 1996. Latent failures of safety significant systems at Finnish NPP´s. STUK work report for CSNI PWG 1 generic study on undetected failures of safety systems. Helsinki. February 9, 1996. 14 p.

Rutledge, P.J. , Mosleh, A. Dependent-failures in spacecraft: Root causes, coupling factors, defenses and design implications. Paper presented at the 1995 reliability and maintainability symposium. USA.

Reason, J. 1990. Human Error. Cambridge University Press. Cambridge.

Rasmussen, J., 1979. On the structure of knowledge. A morphology of mental models in a man machine context. RisØ-M-2192.

Samanta P.K., O´Brien J.M., Morrison, H.W. 1985. Multiple-sequential failure model: evaluation of and procedures for human error dependency. NUREG/CR-3637. Brookhaven National Laboratory. May 1985.

Swain, A.D., Guttmann, H.E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Sandia National Laboratories, Albuquerque, USA. 554 p.

TUD. 1994. Information system for reliability, maintenance and operation. TUD 94-04. 11 p. + 7 app.

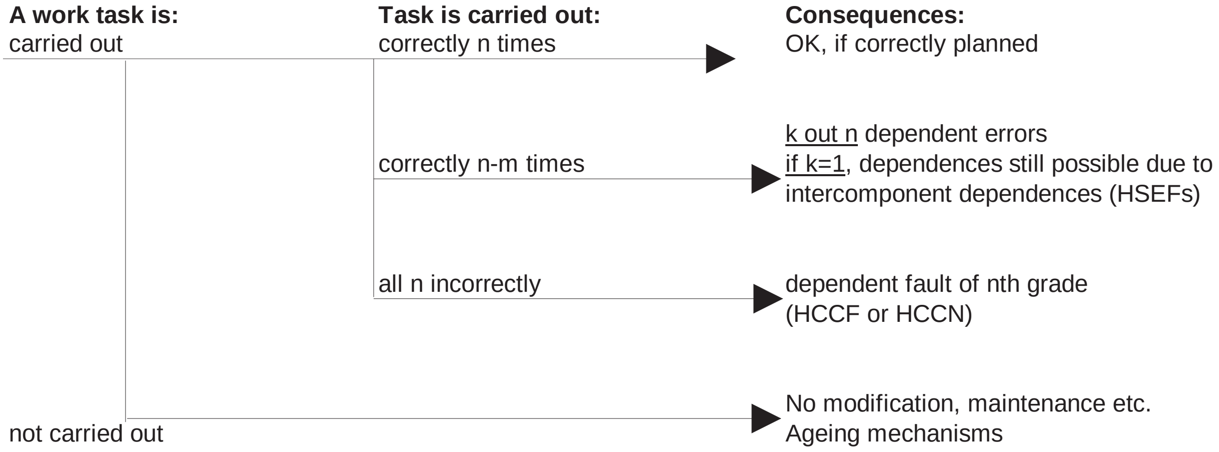
TUD 94-11. T-boken. Version 4. Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer. (Reliability data for component in Nordic power reactors). Prepared in swedish by TUD-kansliet, Studsvik Eco&safety and Pörn Consulting. Sweden. 237 p.

USNRC 1983. PRA procedures guide. Report NUREG/CR-2300. US Nuclear Regulatory Commission. January 1983.

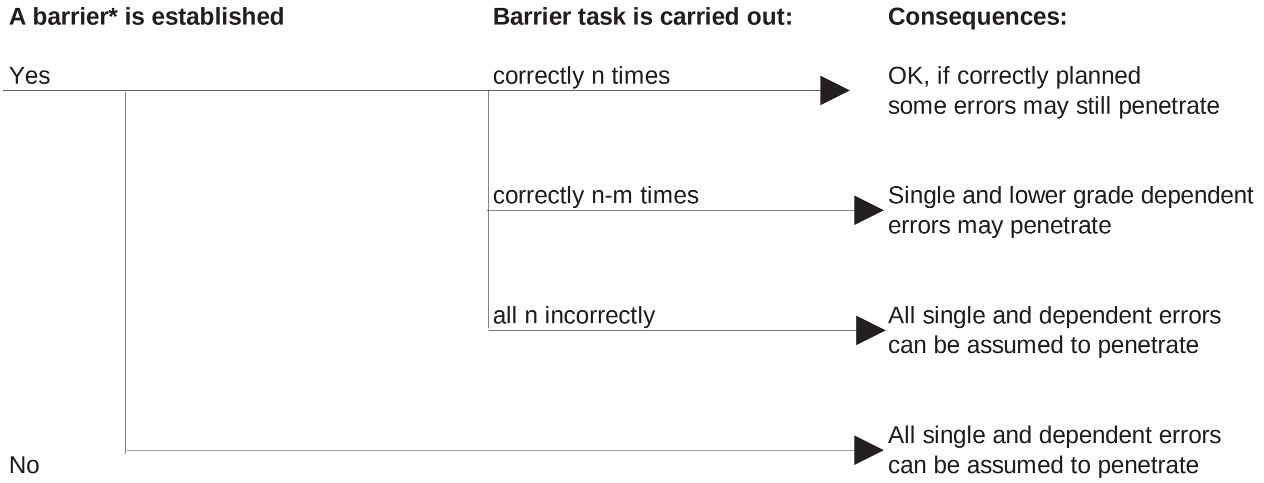
Van den Berghe, Y. 1994. Belgian contribution to task 4 of ETF (PWG1). Human factors related common cause failures in Belgian NPP. 21.12.1994. 26 p.

APPENDIX 1

The following graphs illustrate the birth of dependencies both through omissions (OM) of actions and erroneous actions (COM/WD, SET, COM/OTH). Note that a task may be carried out correctly according to the plans, but the plans or the design in itself may be deficient or wrong. Similarly, a single human error may cause multiple effects dur to system and component interdependencies.



NPPs have many inspection procedures and tests defined in TechSpecs and other check-ups to detect component faults and malfunctions. They are nominated as barriers, in the following graph. The idea of these barriers is to timely detect hazardous faults and human errors. To be able to cause safety effects, an error has to penetrate several barriers without detection. In some cases, even a duly performed test cannot discover all the error or fault mechanisms.


A barrier* is established
Yes
No
Barrier task is carried out:
correctly n times
correctly n-m times
all n incorrectly
Consequences:
OK, if correctly planned
some errors may still penetrate
Single and lower grade dependent errors may penetrate
All single and dependent errors can be assumed to penetrate
All single and dependent errors can be assumed to penetrate

* barriers are either operational (tests etc.) or organisational (reviews etc.)

The unavailability i.e. probability of a component being inoperable, caused by an error penetrating several barriers, is obtained from formula (1):

$$U_{rest} = q \cdot p_0 \cdot \left[\left(T_0 + \sum_{i=1}^{n} T_i \prod_{j=1}^{i} p_j \right) \Big/ T_{total} \right] \qquad (1)$$

where q=probability of an error (causing unavailability), $p_{0,1,2,.}$.= probabilities for passing barrier point j, T_i=time after barrier point i and T_{total} is the total—yearly or test—time period.

APPENDIX 2 HCCF ROOT CAUSE ANALYSIS FORM

Title: POWER CABLES CUT TO THE SUPPLY PUMPS OF THE DIESEL FUEL TANKS

I. INFORMATION IN THE FAILURE REPORT/WORK ORDER OF THE PLANT

(Identification of the plant, equipment, fault, date and repair time):

TVO I ☒II □ Equipment place identification number: 656 T003 Work number: 45738, (45739, 45740)
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):

1. *656 K433 L2 T3 low level alarm. T3 will not be filled*
2. *The power cabling to the outdoor pump cut at the erection work place of start-up transformers.*
3. *Failure reports 1245739 and 1245740 done.*

The cause classification in the failure report (1-2 types): A □ B(F) ☒ C □ D □ W □

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

II. IDENTIFICATION OF THE ERROR TYPE

Type of direct human error (1-2 types) : omission (incl. restoration errors) □ mistake among alternatives □ wrong setting □ other erroneous action (incl. installation errors) ☒ dependent failure (deeper analysis) ☒

Type of root cause to human error if identified: design deficiency ☒ poor work planning or management ☒ deficient information transfer or co-operation □ rule based error □ knowledge based error □

Type of equipment involved: Process valves, ventilation dampers or channel hatchces □ block or primary valves in instrument lines □ other mechanical equipment □ instrumentation, control or software □ electrical equipment ☒

The human error was introduced within: refuelling outage period □ power operation period ☒ not clear □ (if cannot be directed to the periods as above).

The error was detected in (1-2 types): independent check or test ☒ otherwise ☐
plant shutdown period prior to start-up ☐ plant start-up ☐ power operation ☒
plant shut-down ☐ plant disturbance ☐ otherwise ☐

Candidates for dependent failures (based on time relation or functional connections of "single failures") are:

1. *656 P031 / failure report 45739 / 26.08.92 and 656 P011 / failure report 45740 /26.08.92*
2. *The power supply cables cut to the fuel supply pumps 656 P031 and 656 P011 of the two day fuel tanks of the emergency diesel generators (report).*

Terminate the analysis of single failures over this line. Continue the analysis under this line for the candidate dependent failures only.

III. INFORMATION ON THE TASK BY WHICH THE FAULT WAS DETECTED

Detection method_ unclear ☐ Fault possibly detected in ☐ certainly detected in ☒ the task:

1. *Periodic loading and running test of the diesel generator.*

The detection method was : alarm ☒ operation supervision in control rooms, how ____________________
☐ functional testing after maintenance ☐ periodic testing (e.g acc. to technical specifications) ☒ scheduled preventive maintenance ☐ repair ☐ shift walk-around or alignment) ☐ equipment worked not on demand ☐ other authority inspection (e.g. NDT) ☐ other check or test ☐, which____________________________ Date:26.08.94 Interval: 4 weeks

Operational state and situation at detection (1-2 types): cold shutdown of reactor ☐ refuelling ☐ hot shutdown of reactor ☐ nuclear heating ☐ hot standby of reactor ☐ power operation ☒ start-up ☒ shutting down ☐ plant disturbance ☐ other ☐ which ___________________________

Complementary information (e.g. identification number of techspec test or preventive maintenance action):

APPENDIX 2 HCCF ROOT CAUSE ANALYSIS FORM

IV. INFORMATION ON THE WORK TASK WHERE THE ERROR OCCURRED

Cause of the fault unclear □ Fault possibly caused in □ Fault certainly caused in ☒ the action:

1. *Cable charts outside the wall of the plant not kept up to date during the construction period of the plant.*
2. *Own maintenance worker cut as ordered the "extra" 380 V cables at the erection work place of the additional start-up transformers (612).*
3. *The cut was done in order to facilitate the erection of the additional 110 kV cabling.*

The action was (1–2 types): preventive maintenance □ repair □modification ☒ periodic test □ interval________weeks functional test □ other □ date (possible or certain): 19.08. 1992

Complementary description:

1. *The power cables were encapsulated but not documented and the cables thus thought to be "out of use" cables needed during the earlier plant construction period only.*
2. *The "unexpectedly" found cables had no voltage due to standstill of the related fuel supply.*

The causing action occurred during (1–2 types) : old shutdown of reactor □ refruelling □ hot shutdown of reactor □ nuclear heating □ hot standby of reactor □ power operation ☒ starting up □ shutting down □

Complementary information (e.g. description of how the fault occurrence could have been avoided):

V. THE ORIGIN AND DEPENDENCE OF THE FAULT

Type of human error (1-2 types):omission (also restoration errors) □ mistake among alternatives □ wrong setting □ other erroneous action (carelessness errors etc.) ☒ dependent failure ☒

The originating mechanism of the error and dependence is (1-2 types) : (design deficiency e.g. documentation not updated ☒) (rule based error, e.g. deficient procedure) or order or rules not followed ☒ , insufficient knowledge, e.g. due to lacking training □ , poor work planning or management, e.g. in definition of work scope or supervision of subcontractors ☒ poor information transfer (e.g. due to organizational changes or poor experience feedback) □ , poor tools (selection, maintenance or QC) □ other □ , ______________________________(or complementary information on which organizational unit or personnel category):

HCCF ROOT CAUSE ANALYSIS FORM **APPENDIX 2**

The error was additionally caused by: equipment close to each other (e.g. same room) ☒ , administrative easiness (e.g. sequential tasks feasible soon after each other) □ same group (e.g. similar tasks on similar components □ deficient preventive maintenance (e.g. the effects of ageing not avoided by prompt inspection or replacement of degrading components) □ heavy work load or tight time schedule □ equipment not uniquely identified (e.g. due to poor identification or name plate) ☒

Explanatory description:

1. Cable charts outside the plant walls were not kept up to date.

2. In addition, unnecessary cables from the plant construction period were known to lie under the earth level.

Consequences of the error (e.g. unavailability 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): about 168 hours.

Total unavailability time: about 174 hours.

Complementary information (e.g description of consequences):

VI. NOTES ON POSSIBLE INEFFECTIVENESS OF DEFENSIVE BARRIERS

Error not detected in the operative check (check following after the work action, 1-2 types): preventive maintenance □ adjusting □ functional test □ alignment □ start-up test □ periodic test □ interval ____________ (other check ☒ poor installation check-up which was ineffective _____ date__________ plant state, which ___________

Complementary information (e.g. identification number of TechSpec test or preventive maintenance task or explanation, if checking task existed):
Error was not detected in organizational check (independent QA and QC, performed prior, during or after 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 error):

VII. PROPOSAL OF ALTERNATIVE REMEDIAL MEASURES

The problem can be corrected (or already corrected and the success possibly evaluated) by:

1. Cable charts concerning areas outside the plant walls were prepared to an up to date status.

2. Procedures were prepared for identification of cables found during digging work and for cutting off power cables. The procedures are in use (e.g. cable radar, cutting needs work order.)

3. An increase of the fuel margins in the day tanks for the diesels was implemented by making the tank level L2 higher.