TR STUK-YTO-TR 217 / DECEMBER 2006

SYSTEMATIC ANALYSIS AND PREVENTION OF HUMAN ORIGINATED COMMON CAUSE FAILURES IN RELATION TO MAINTENANCE ACTIVITIES AT FINNISH NUCLEAR POWER PLANTS

Kari Laakso

STUK
Säteilyturvakeskus
Strålsäkerhetscentralen
Radiation and Nuclear Safety Authority

STUK

STUK-YTO-TR 217 / DECEMBER 2006

SYSTEMATIC ANALYSIS AND PREVENTION OF HUMAN ORIGINATED COMMON CAUSE FAILURES IN RELATION TO MAINTENANCE ACTIVITIES AT FINNISH NUCLEAR POWER PLANTS

Kari Laakso
VTT Industrial Systems

STUK • **SÄTEILYTURVAKESKUS**
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FIN-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

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

ISBN 952-478-189-1 (print, Edita Prima Oy, Helsinki/Finland 2006)
ISBN 952-478-190-5 (pdf)
ISSN 0785-9325

LAAKSO Kari (VTT Industrial Systems). Systematic analysis and prevention of human originated common cause failures in relation to maintenance activities at Finnish nuclear power plants. STUK-YTO-TR 217. Helsinki 2006. 33 pp.

Keywords: maintenance, operability, human failures, common cause failures, testing, inspections, experience feedback, statistics, nuclear power plants

Abstract

The focus in human reliability analysis of nuclear power plants has traditionally been on human performance in disturbance conditions. On the other hand, human maintenance failures and design deficiencies, remained latent in the system, have an impact on the severity of a disturbance, e.g. by disabling safety-related equipment on demand. Especially common cause failures (CCFs) of safety related systems can affect the core damage risk to a significant extent. The topic has been addressed in Finnish studies, where experiences of latent human errors have been searched and analysed systematically from the maintenance history stored in the the power plant information systems of the Loviisa and Olkiluoto NPPs.

Both the single and multiple errors (CCFs) were classified in detail and documented as error and event reports. The human CCFs involved human, organisational and technical factors. The review of the analysed single and multiple errors showed that instrumentation & control and electrical equipment are more prone to human error caused failure events than the other maintenance objects.

The review of the analysed experience showed that most errors stem from the refuelling and maintenance outage periods. More than half of the multiple errors from the outages remained latent to the power operating periods. The review of the analysed multiple errors showed that difficulties with small plant modifications and planning of maintenance and operability were significant sources of common cause failures. The most dependent human errors originating from small modifications could be reduced by a more tailored planning and coverage of their start-up testing programs. Improvements could also be achieved by identifiying better in work planning from the operating experiences those complex or intrusive repair and preventive maintenance work tasks and actions which are prone to errors. Such uncertain cases in important equipment require a more tailored work planning of the installation inspections and functional testing. Such a planning case shall include a need evaluation of both the component and system level testing at the end of work.

In addition, the use of condition monitoring information helps in reducing the uncertainty about equipment operability after intrusive maintenance or modifications. An increased use of condition information for a situation specific steering of preventive maintenance actions could also help to avoid unnecessary predetermined preventive maintenance actions which have the potential to cause unnecessary failures. A more agile adjustment of work orders to correspond the new conditions identified by maintenance personnel locally during work was also found necessary to reduce human CCFs caused by e.g. missing testing or inspections.

The results emphasize the responsibility and requirements of versatility and specialisation of the planning and performance of maintenance and operability verification which brings this work to a knowledge work. For instance, flexibility is needed for the adaptation to specific conditions of the equipment and work as well as adhering to the rules and procedures is required. And mostly both a specialist knowledge of the equipment and a functional overview of the system are required. The event and error analyses of the multiple and single errors would help in training the maintenance, operation and technical personnel to identify better error mechanisms and prevent undetected human CCFs and errors, too.

An earlier and better defined examination of the CCF risks as a part of the failure reporting and repair and modification processes would also help to identify, investigate and prevent CCFs. Generally, operability verification of the work objects in plant equipment should be planned and implemented better as an integral part of the plant maintenance process requiring knowledge of both the maintenance and operation branches.

Methods for analysis of maintenance history information, examples of presentation of analysis results and further conclusions and recommendations for identification and prevention of latent human common cause failures, single errors and costly rework are also described in this report.

Preface

These studies have been performed within the Finnish research programmes on nuclear safety. The studies were financed by the Finnish Radiation and Nuclear Safety Authority (STUK) primarily, secondarily by the Ministry of Trade and Industry (KTM) and thirdly by the Nordic Nuclear Safety Research (NKS).

We are thankful to the maintenance, operation, safety and reliability personnel of the utilities Fortum Power & Heat and Teollisuuden Voima Oy, who have provided the maintenance history data and participated constructively in the interviews, analyses and work meetings during the studies. As well we are thankful to the STUK experts who have supported the studies by their safety knowledge and operational experience in commenting the methods, definitions and analyses during the studies.

Contents

ABSTRACT 3

PREFACE 5

1 INTRODUCTION 7

2 THE SCOPE OF THE STUDIES 8

3 ANALYSIS METHODS OF SINGLE AND MULTIPLE ERRORS 9

4 RESULTS FROM REVIEW OF THE BULK OF ERROR AND EVENT ANALYSES 14

5 CONCLUSIONS AND RECOMMENDATIONS 23

REFERENCES 32

1 Introduction

The focus in human reliability analysis of nuclear power plants has traditionally been on control room operator performance in disturbance conditions. In the area of maintenance activities, the emphasis has been on human reliability of non-destructive inspections. On the other hand, incidents have shown that errors related to maintenance and testing, which have taken place earlier in plant history, may have an impact on the severity of a disturbance, e.g. by disabling safety related equipment.

The human failures have often been complex event sequences, involving human, organisational and technical factors. Especially common cause and other dependent failures of safety systems may significantly contribute to the reactor core damage risk [Laakso, Pyy & Reiman, 1998]. The topic has been addressed in the Finnish studies of human common cause failures, where experiences on latent multiple and single human errors have been searched and analysed in detail from the maintenance history.

In the Finnish projects, one aim was also to promote the studies of human factors related to maintenance [Oedewald & Reiman 2003]. Another aim of the analysis was to support PSA by extending the applicability of human reliability analysis to study of the effects of wrong human actions in relation to maintenance [Pyy 2000] and by plant specific CCF data.

The main aim of the projects was identification, description and prevention of human originated CCFs and single errors in relation to maintenance by analysis, remedial actions and learning.

2 The scope of the studies

Case studies for identification and analysis of human common cause failures from the maintenance history in plant information systems have been conducted for the nuclear power plants Loviisa and Olkiluoto. Apart from the safety systems, the studies covered all steam and power generating systems of the plant units also. All plant systems were covered due to the fact that human error mechanisms may be similar at the different parts of the plant. Besides, all from the risk point of view significant systems are not classified as safety systems. Thus, a more extensive database of multiple error mechanisms was obtained for learning to prevent the significant human common cause failures.

The analysis of the Olkiluoto units 1 and 2 three-year experience during 1992–1994 covered 4400 fault repair work orders. Totally 334 human error cases were identified and among them the number of single errors was 206. The number of dependent human common cause failure event cases derived and analysed was 14 [Laakso, Pyy & Reiman, 1998]. In the corresponding study of the Loviisa nuclear power plant units 1 and 2 maintenance history during 1995–1997, the number of fault repair work orders was 14091.The number of single errors identified was 149 and of human common cause failure cases identified and analysed was 34 [Laakso & Saarelainen, 2003].

The numbers from the different plant sites are not directly comparable. In the Olkiluoto case all the 4400 fault repair work orders were studied. But the scope of the examined work orders was limited in the Loviisa plant case by creating a data screening procedure. The screening procedure had a hit rate of 2/3 in error identification in the detailed analysis of the studied fault work orders.

The studies also covered analysis of the weaknesses in the barriers aimed to reveal or prevent human originated common cause failures in relation to maintenance activities [Laakso, 2004].

3 Analysis methods of single and multiple errors

Introduction to terms. In order to enable a better understanding of the analysis results and the report, important failure and error related terms used in this study are firstly defined in Table I.

The power plant information systems. The power plant information systems in Finnish NPPs include work planning and fault, maintenance and operation place histories. The experience data is well documented and has a good coverage from the 80´s. The documentation and classification of the fault and repair history information is performed by the maintenance and operation personnel. Most

Table I. Definition of central terms.

Failure is the termination of the ability of an item to perform the required function. Failure is an event, as distinguished from "fault" which means a failed state [see e.g. EN 13306 1999]. The faulty item deviates from the wished standard of performance in its failed state or from the required function in its end state. If you do not wish to divide the used failure term into fault, failure or failure situation, "failure" can be used as a general term.
Human error. A human unintended or intended action that produces an unintended result. An omitted or erroneous action may trigger directly, or initiate a failure process leading to, a failed state or a failed end state of the equipment. E.g., omission of on-line return of equipment after maintenance work causes a failure of equipment to perform its function. Or, instrument pipelines may be crosswise connected during a modification or an intrusive maintenance action, due to deficient documentation or lacking knowledge, causing a failure of the pressure difference trip to operate. In some sources, human errors are divided into slips, lapses, mistakes, violations, omissions and commissions [see e.g. Swain & Guttman 1983, Reason 1990]. In this study, human failures are studied more from the technical point of view, what are the direct effects of errors on equipment and their function, and which are the root causes of the multiple errors.
Common cause failure. Common cause failures (CCF) are similar failure causes or mechanisms, that may apparently result or have resulted simultaneously in multiple functionally critical failures in redundant subsystems in real demand situations. Also as CCFs are defined multiple failures acting on parallel trains or circuits, if they are unable to fulfil correctly their required function. Multiple erroneous or omitted actions are triggers to human originated common cause failures.
Common cause non-critical failure. Common cause non-critical failures (CCNs) are similar failure mechanisms which result simultaneously into deviations from wished standard of performance of redundant or parallel equipment. They include defects on items which are not critical for the equipment function. The failures originating from outages are defined as non-critical, if the failures were detected and repaired before transfer to the plant operating states where the operability of equipment is required. Generally, if the deviations are getting worse, these precursors can develop into common cause failures. The CCNs can be regarded as an early warning of causes or mechanisms otherwise leading to CCFs.

Table II. Cause coding of failures used in the plant work order system.

A	**Equipment and design**	**C**	**Consequence of operation**
AA	Design	CA	Exceeding a limit value
AB	Material	CB	Over-stressing
AC	Manufacturing	CC	Blockage, sediment, stagnation
AD	*Installation*	*CD*	*Foreign objects*
		CE	Normal wear of lifetime
		CG	Break, connection fault
B	**Personnel**	**D**	**Miscellaneous causes**
BA	Control or operational error	DA	Cascade failure
BB	*Wrong setting or control*	DB	External cause
BC	*Maintenance or repair error*	DC	Deficient work order or instruction
BD	Lack of or delayed action		
BE	*Human error*	**Z**	**Other (give extra description)**

of the plant personnel use the plant information system.

Failure cause and entry coding used in the work order reporting. The original cause coding used by the plant personnel in the failure and repair work orders in the Loviisa power plant information system is shown as an example in Table II.

The above cause classification coding of Loviisa NPP is also rather similar with the corresponding coding at the Olkiluoto plant. The cause coding together with study of written descriptions in the failure and repair work orders helps to identify candidates of human errors related to maintenance activities from the failure and maintenance history.

Screening of human error candidates from plant failure reporting. One specific and useful feature in the maintenance history reporting in one of the plants, the Loviisa plant, was the classification of the probable entry of the failure, see Table III. The following classification coding (especially 12 = during previous maintenance or repair) of the plant reporting helped to identify a subset of those failure and repair work orders which originate from previous maintenance actions or repairs.

In a detailed review of the failure repair work orders classified like so, a number of maintenance and modification related errors could be retrieved. The first screening of the error candidates from a very large number of work orders was performed by comparing the written descriptions on symptoms, causes and actions with the given cause classification codes (in Table II) of the work orders.Almost all identified single and multiple human failures were cause classified to originate from installation, wrong setting, maintenance or repair error, or human error. Then all the failure and repair reports

Table III. Coding of probable failure entry into equipment.

–	Undefined
01	Before previous test
02	Before previous maintenance or repair
11	During previous test
12	*During previous maintenance or repair*
13	During previous operation
21	After previous test
22	After previous maintenance or repair
23	After previous operation
31	Immediately before detection
32	After previous shift walk-around

belonging to these four cause coding classes, plus the work orders coded as probably introduced during previous maintenance or repair, were selected as candidates for further study. The screening criteria of the work orders for the complete study were verified by reviewing the sample human errors with the proposed screening criteria in expert sessions with the plant maintenance planners and regulatory body professionals.

Analysis and classification of human errors. Within the Olkiluoto plant case study detailed classification models for human errors in relation to maintenance were developed and used. The information from the maintenance work order database was utilised for analysis of the errors. In the later Loviisa plant study the error classification was enhanced to individualize better the quality errors related to maintenance, too. The idea at the Loviisa plant study was also to identify and verify the time and nature of the error origin in a more detailed way than in the earlier Olkiluoto case. The advancements of the classification of the maintenance related human errors have been applied only for the Loviisa plant. The used error classification

Table IV. Classification of direct errors on equipment.

Errors of Omission (missing human action)

1. Restoration errors of operability after work, such as omission of the realignment of process or instrument valves, disconnectors, breakers, fuses or limit settings. Omission of refilling of fluid or gas into lines, tanks or drainings
2. Disconnected cables or electronic or mechanical components not reconnected during work . Omission to install packing or adjusting device.Settings, adjustments, preventive maintenance or inspections omitted.
3. Foreign objects or impurities left behind inside the object of the work. Examples are dirt, garbage, metal shives, tools, scaffolds or covering material.

Errors of Commission (wrong human action)

Wrong order or direction

4. Wrong order, such as cables or instrument pipelines crosswise connected.
5. Wrong direction, such as reversed or twisted installation of valve or another sub-component. Wrong positioning of valve.

Wrong selection

6. Wrong place or object, such as cabling fixed on wrong connection, setting of wrong tripping conditions or draining of wrong pipeline. Item installed on wrong equipment place.
7. Wrong or mixed spare parts, parts, materials, tools, fluids or chemicals selected for work.

Wrong settings / adjustments / calibrations

8. Wrong settings of trip limits, limit switches, reference, indication or time delay values, or of adjusting devices. Deficient alignment of shaft, stem/spindle or pipe. Wrong setting of pipe support or packing.

Other quality problems

9. Too little force, e.g. loose connections of bolts, nuts, bonnets, cables or sensors
10. Too much force, e.g. excessive tightening or greasing
11. Damaging other equipment e.g. cabling, cable trays or small diameter piping by falling material or slugging/contacting. Can be due to carelessness and narrow spaces for work or transport.
12. Other carelessness (if 1–11 are not applicable). E.g. worn tools, falling material, deficient weld, solder joint or insulation. Unclear trips initiated during testing, installation or maintenance. Wrong subtitling or recording. Wrong timing.

in Table IV structures and describes how the direct effects of human errors in relation to maintenance appear on the equipment level.

In the detailed analysis of all human errors related to maintenance, including both the single and the multiple errors, were classified according to following explaining factors:

- Equipment type influenced by error,
- how the failure was detected,
- plant operating state at failure detection,
- direct error effects (see Table IV),
- erroneous task triggering the failure failure process or event,
- time instant and plant state when error occurred,
- whether the error was single or multiple.

In Table V, an example of an analysis of a human error in relation to maintenance is presented.

In the first column of the table, the equipment place is defined as a functional item at a level where an identification number and labelling such as 10RC51N001 (an ejector) or 10RC51 T001 (a temperature measurement) can be identified in the plant [TUD 94].

The identification of the erroneous work task as the “failure trigger” and its time instant was a demanding task for the analysis. The erroneous task was searched by scrolling through the preceding work history of the failed equipment place or its train from the plant information system. The identification of the erroneous task required maintenance experience and technical knowledge of equipment,

Table V. An example of a basic analysis of a human error in relation to maintenance.

Equipment place	Failure work order number	Date	Explanation	Cause, reported	Equipment type	Detection method	Plant state at time of detection	Error, type, direct	Erroneous task, error occurred	Multiple error ?
10RC51 T001 & T002	220691A	28.09.95	Temperature measurements 10RC51T001 and T002 after the ejectors 10RC51N001 and 10RC51N003 indicated too much because measurements had been crosswise connected in repair.	AD	IC	9	OPER	4	REPAIR, 16.04.1993, OPER	Yes. 1HCCN RC51.

Table VI. Classification and definition of root causes of multiple human errors in relation to maintenance.

1. *Maintenance and operability planning deficiency:*
   Incorrect, incomplete or unclear planning of maintenance or operability verification actions such as maintenance, repair, installation inspection or functional testing phases of work. Deficiencies in coverage of start-up tests or installation inspections of modi fications. Deficiencies in coverage of maintenance or inspection program. Deficiencies in definition or decision of work scope , work order, operation order or procedure.

2. *Design deficiency:*
   Error or deficiency in design or documentation of modification, equipment, system, installation or computer program. Documentation not updated to correspond changes. Lacking identification labelling of equipment place.

3. *Violation of procedure or order:*
   Violation due to insufficient knowledge or poor information. Deviations from procedure or order due to gradual organisational learning of "bad habits". Or conscious violation.

4. *Poor co-ordination, supervision or information transfer:*
   Poor project co-ordination or supervision of subcontractors, poor information transfer due to organisational changes or boundaries. Or weaknesses in experience feedback such as recurrence of events with known phenomena. Or poor quality control.

5. *Insufficient knowledge:*
   Lacking training, specialist or cross-functional knowledge for work or planning tasks.

and in some obscure cases expert judgements were needed to extract the probable task.

Analysis and classification of root causes of multiple failures. Apart from the observable effects of all errors on equipment, the underlying contributing factors are analysed and classified for the dependent human errors. The root causes and cause descriptions of the multiple errors (HCCF/ HCCNs) could be assigned to one of the following groups (Table VI).

The principles followed in the division of errors into single ones, HCCFs (human common cause failures), HCCNs (human non-critical common cause failures), HSEFs (human shared equipment failures) and OFD (other dependent failures) are presented in Table VII.

Event reports on human common cause failures. In addition to the basic analysis and classification of the single human errors, the human CCFs were analysed and classified also with respect

Table VII. Principles in division of errors into single and multiple failures.

Failure trigger	Failure in one single equipment place *)	Failures **) in parallel ***) and similar equipment places	Failures **) in cascading ****) equipment places
Similar repeated erroneous or omitted actions	Single errors	HCCF / HCCN or ODF****)	ODF
One error	Single error	HSEF	HSEF
Several different errors	Single errors	Single errors	Single errors

*) Equipment place is one by labelling identifiable operation place or equipment.
**) Failures in parallel or cascading equipment refers to time – equipment failed at the same time.
***) Parallel equipment refers to physically parallel train, sub or circuit, and cascading equipment to equipment in the same train, sub or circuit.
****) Other dependent failure, if errors detected and repaired before returning the work permit to control room.

Table VIII. An example of a maintenance event report.

Identifier marking	Work order time and numbers	Title and description of event	Operating event identifier
1HCCF YP12	1996-10-08	Deficient adjustment and testing of the actuators as implementing new motor operated blowdown valves in the pressurizing system	No
	238769D, 238769A 238769B 238769C	The gate valves 12YP12S038, 12YP12S039, and 11YP12S036, 11YP12S037 were not tight in hot state during power operation 1996-10-08. New motor operated gate valves (MOVs) had been installed during the preceding maintenance outage in September 1996. •The MOVs had to be closed as a corrective action by manual operations from the switch-gear during the power operation state at 1996-10-09. •The common cause setting errors had passed from the maintenance outage through to the power operation period, because the setting and testing of the limit and torque switches of the MOVs in the cold state were insufficient without hot start-up testing of the modification work.	

to root causes, and missed detection in operative or organisational defensive barriers.

This extension of the basic error analyses to event analyses was done in interaction with plant maintenance and operability experts based on identification of the multiple error candidates in the basic error analyses. The structured analysis facilitated to capture the "tacit knowledge" of the equipment place history before the fault detection and failure detection. The systematic event analysis helped to pinpoint the weak barrier functions (such as identified in installation inspections or component testing done by maintenance personnel or functional testing done by operation personnel) and thus resulted in latent faults.

The identified dependent human errors were analysed and summarised in condensed maintenance event reports which included a qualitative description of the:

- multiple error and its failure effects,
- originating erroneous or defective work task, and
- missed opportunity for detection, e.g. deficiency in operability verification, allowing the errors remain latent in the system.

One of the maintenance event reports prepared during the multiple failure studies is given as an example in Table VIII.

As can be seen from the above example maintenance event report, a combination of several fault repair work orders may be needed for identification of common cause failures. In the studies, in average about two fault repair work orders were combined to build up a CCF event. The similar multiple faults had to been searched within the time frame of the surveillance testing interval or shorter. But some CCFs could be identified from single fault repair work orders, too.

4 Results from review of the bulk of error and event analyses

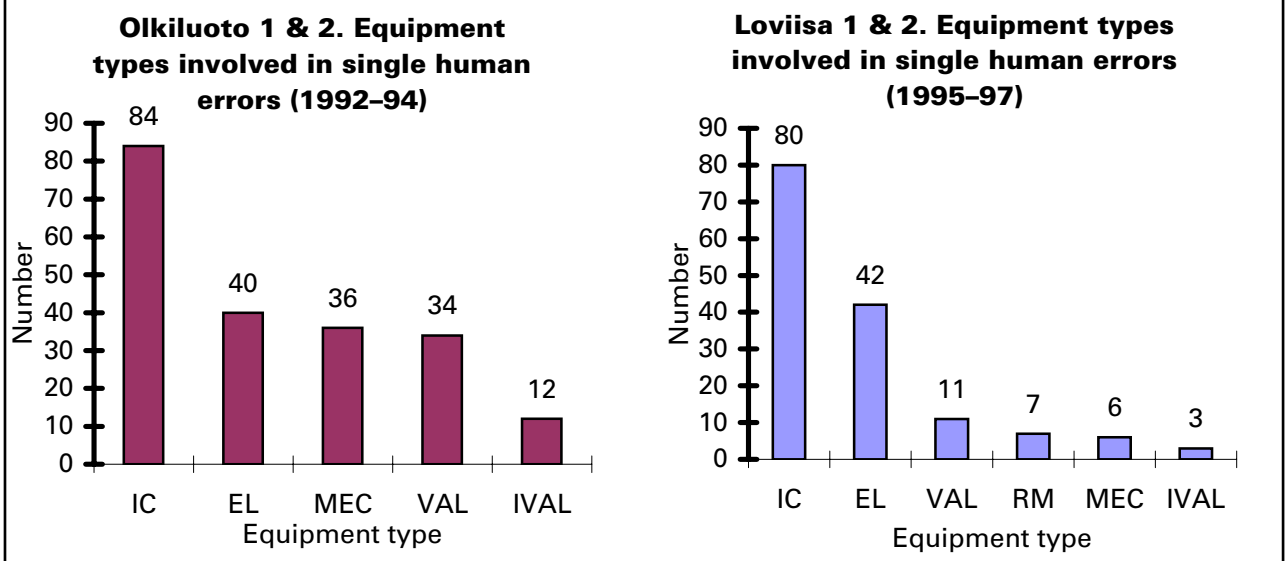
Introduction. The bulk of the multiple human errors (HCCFs and HCCNs), as well as single human errors, were statistically treated based on the classifications of the error and event analyses. Recurrence of the errors within different groups of the classification classes, such as combinations of equipment and error types, equipment and root cause types, and erroneous task and missed barrier types, were also searched in order to identify possible dominating problem areas. The underlying event or error analyses of the "possible problem areas" were thereupon reviewed qualitatively in order to identify recurrent problems and potential opportunities for remedial actions or practises.

Equipment affected by single errors. According to the review of the bulk of the analyses of single errors at the both plants, the instrumentation & control (IC) and electrical equipment were noticed to be more involved in human error caused failures than the other maintenance objects.

It should however be noticed that the more rare errors on mechanical equipment in safety related systems can however be serious and have caused forced plant outages in Finnish nuclear power units.

Multiple human error cases. In the following Tables IX and X, the identified and analysed functionally critical multiple error events (HCCFs) are listed together with a short description, the affected equipment type and individual plant units. Only the short descriptions of the HCCFs are given as an example of the multiple human error problems in the following.

No descriptive examples of functionally non-critical HCCNs (which are precursors to HCCFs) are given in the above Tables IX and X. The HCCNs



IC = Instrumentation & control equipment or software, EL = Electrical equipment, MEC = Mechanical equipment, VAL = Process valves, ventilation dampers or channel hatches, IVAL = Block or primary valves in instrument lines, RM = Radiation monitoring equipment

Figure 1. Equipment types involved in single human errors in relation to maintenance.

Table IX. Functionally critical human common cause failures at Olkiluoto NPP.

Nr.	HCCF	Maintenance event Human originated common cause failures (HCCF)	Equipment type	Plant unit
1	1HCCF531	The trip limits lowered on wrong neutron flux trip conditions.	IC	OL 1
2	1HCCF531e	Neutron flux trip limits left too low after valve self-closure test.	IC	OL 1
3	1HCCF656	Power cables cut to the supply pumps of the diesel fuel tanks.	EL	OL 1
4	12HCC712	Difference pressure measurements crosswise connected in mussel filters.	IC	OL 1 & 2
5	1HCCF747	Couplings broken between actuators and control valves.	IC	OL 1
6	12HCCF534	The actuation times too long due to mineral oil impurities in the anchors of the solenoid valves.	EL	OL 1 & 2
7	2HCCF327	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	OL 2 (& 1)
8	2HCCF713	Turning pieces of flow measurement devices mixed in assembly after cleaning.	IC	OL 2 (& 1)

Table X. Functionally critical human common cause failures at Loviisa NPP.

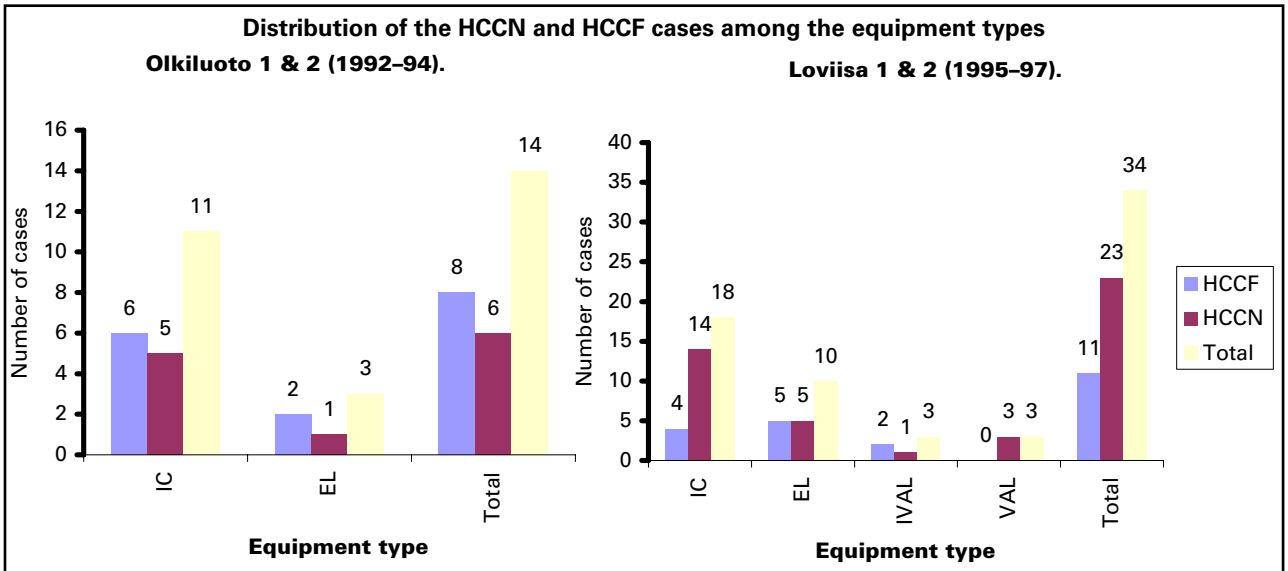
Nr.	HCCF	Maintenance event Human originated common cause failures (HCCF)	Equipment type	Plant unit
1	1HCCFRL30	The sensor cabling of the newly installed ultrasonic feed water flow measurements melted during plant startup due to wrong insulation.	IC	Loviisa 1
2	12HCCFVF62	The settings of the limit switches of the baffle valves in service water system were omitted after reinstallation of the disconnected valves during modification work in piping. The omission lead to leakege during operation.	EL	Loviisa 2 & 1
3	2HCCFRD50	Two of the closing valves in the HP steam extraction lines closed 3 minutes slower during the shutdown procedure because the hysteris of the signals in the circuit boards was lacking after the maintenance outage.	IC	Loviisa 1
4	1HCCFRN13	The settings of the replaced actuators of the closing valves in the auxiliary condensate system were performed at the cold state only leading to stiffness and torque switch trips in the warm operating state.	EL	Loviisa 1
5	1HCCFRQ11	The settings of the repaired actuators of the closing valves in the auxiliary steam system were performed at the cold state only leading to torque switch trips before limit switch tripping as the valves were closed during power operation.	EL	Loviisa 1
6	1HCCFSD72	The settings of the replaced actuators of the closing valves of the ejectors in the auxiliary condensate system were performed deficiently at the cold state only leading to torque switch trips as closed in the warm operating state.	EL	Loviisa 1
7	1HCCFYP12	The setting and testing of the new blowdown valves in the presssurizer system were deficient as performed only in cold state at the end of the modification work. This resulted in leakage of the valves during power operation.	EL	Loviisa 1
8	2HCCFTB33	The flow measurements of the boron feed pumps did not function during pumping during power operation due to omission to open the closing valves of the instrument lines after the outage modification works.	IVAL	Loviisa 2
9	2HCCFRD11	The primary closing valves were forgotten in closed position in the insrument lines of the level measurements of the HP feed water heaters after the maintenance outage 1997.	IVAL	Loviisa 2
10	12HC-CFTH50	Uncertainties in work planning and management caused simulataneous unavailabilities in temperature measurement chains of the strainer pits during their periodic equipment testing	IC	Loviisa 1 & 2
11	1HCCFUW23	The reconnection of printers in the air- conditioning control room was forgotten until power operation after the maintenance outage preventive maintenance.	IC	Loviisa 1

have however been included in the following statistical treatment together with the functionally critical HCCFs. This has been done in order to facilitate a larger database of multiple human error mechanism which may be found recurring, and thus pinpoint potential opportunities for remedies. From the Tables IX and X you may directly identify that at least four HCCF mechanisms have been recurrent because they have occurred at the both units of a plant.

Distribution of multiple errors into different equipment. As seen in Figure 2, the dominance of the instrumentation & control control equipment, accompanied by the electrical equipment, already seen in the single errors, also applies to the multiple human errors (HCCFs and HCCNs).

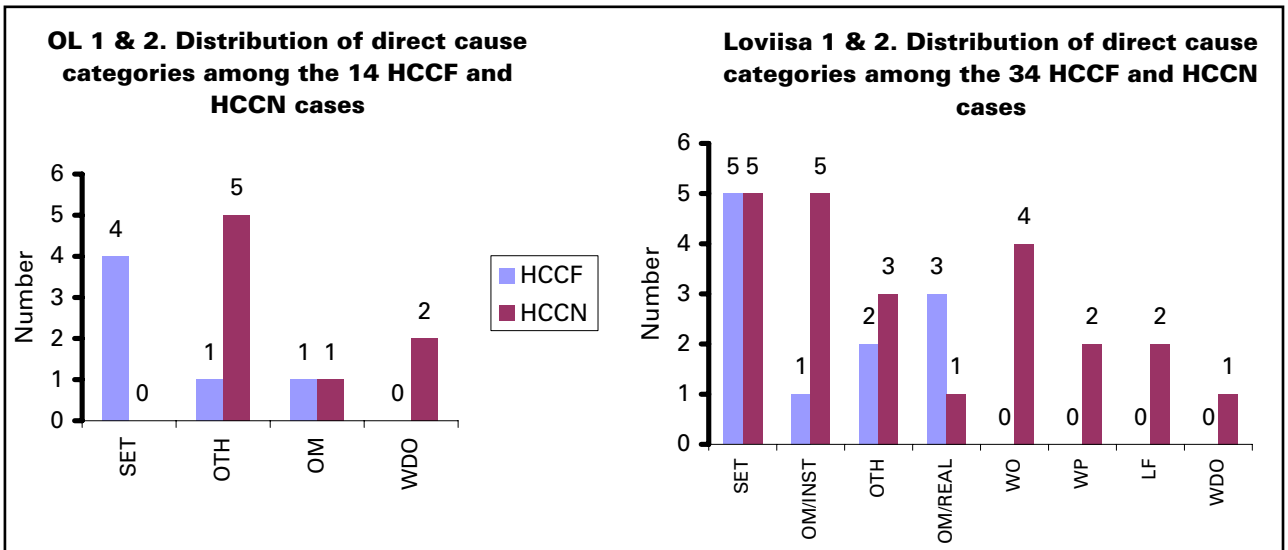
The dominating involvement of the IC equipment in multiple and single errors should not depend on the IC's error proneness only. The dominance comes from the high number of IC maintenance objects, and from the evident functional effects of such errors on IC, too. But this result emphasizes the responsibility and requirements of both the versatility and specialisation of the design, maintenance and operability planning, as well as the needs of instrument mechanician's skills and knowledge of instrumentation and automation and its functional effects.

Direct causes of multiple errors. The dominant error category of the human common cause failures was wrong setting at the both plants (see Figure 3). In the second plant Loviisa, the omissions to install connections and to set can in addition be itemized as dominating direct effects of the errors at equipment level.



IC = Instrumentation & control equipment and software, EL = Electrical equipment, IVAL = Block or primary valves in instrument lines, VAL = Process valves, ventilation dampers or channel hatches.

Figure 2. Distribution of multiple human errors among equipment types.



SET = wrong settings, OTH = other errors of commision, OM = errors of ommission, WDO = wrong direction or order, COM = errors of commission, COM/INST = installation omitted, OM/REAL = realignment omitted, WO = wrong order, WP = wrong place, LF = too little force.

Figure 3. Distribution of direct error categories among the multiple error cases.

Origins of the human common cause failures. The sources of the common cause failures (HCCFs and HCCNs) could be searched in expert sessions from the plant information systems. The probable origin of the common cause failures was identified and evaluated by examining the earlier tasks from the work order history of the concerned equipment operation places or trains. In a number of the analysed multiple error events, the plant modifications appeared to be the main origin, but also the predetermined preventive maintenance was found to be a significant source, especially in the Loviisa plant, see Figure 4.

Underlying causes of human common cause failures. Apart from the origins and direct causes, also the underlying "root" causes were studied for the human CCFs and human CCNs. The distributions of the root causes to the HCCFs and HCCNs at the both sites are to be found in the following Figure 5.

Weaknesses in planning of maintenance and operability verification seem to contribute as underlying causes into the occurrence of human common cause failures in the half of the cases at the both sites. The most of these problems occurred in relation to modifications, but also in preventive maintenance during outages.

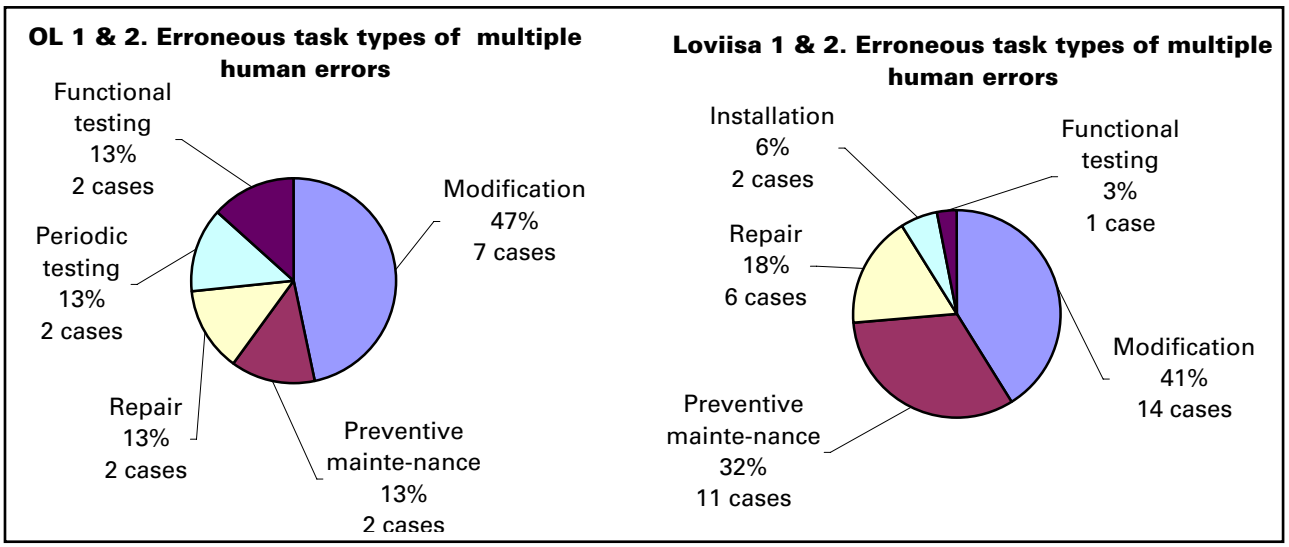


Figure 4. The types of erroneous tasks leading to HCCFs and HCCNs.

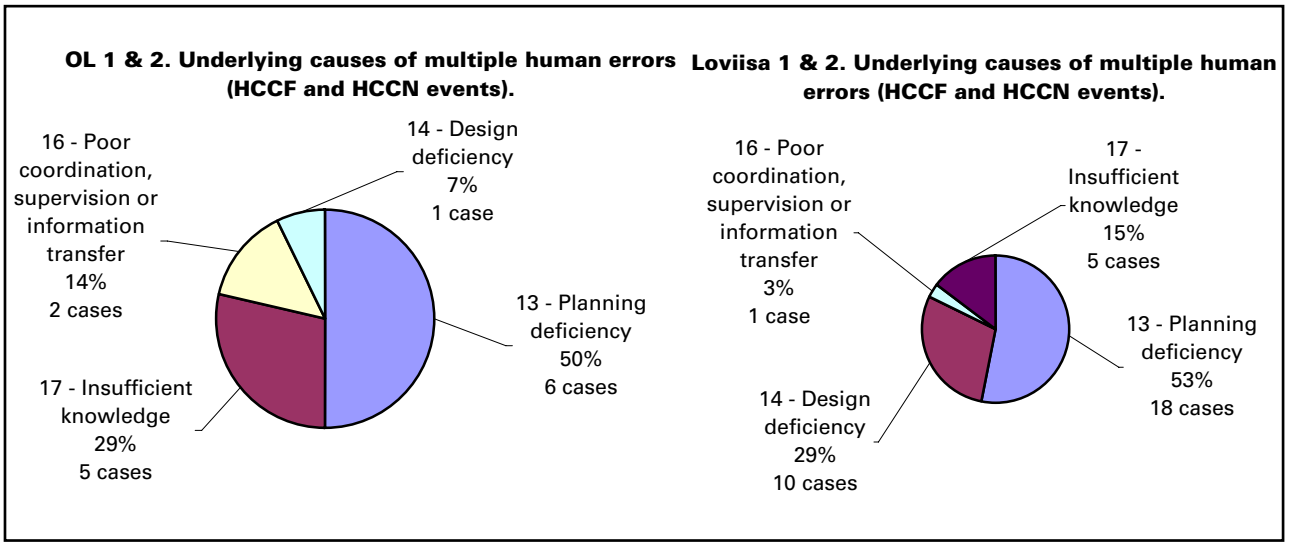


Figure 5. Underlying causes to human CCFs and CCNs.

The review of the results of the root causes of the analysed human common cause failure events indicate also that planning of maintenance work phases and operability verification actions is a very demanding task due to the complex planning environment of different objectives, safety requirements and instructions, and needs of multifunctional plant technical, maintenance and operability knowledge. The planning problems indicate also that operability verification after work in plant equipment and systems should be planned and implemented better as an integral part of the maintenance planning process and that it requires a combined knowledge of the maintenance and operation trades.

The significant number of contributing causes "insufficient knowledge" exhibit the need of specialist understanding and experience of specific components at the personnel of the utility and contractors supervising and performing specific maintenance activities.

When considering remedial actions, it has to be taken into account that also interactions in work between different trades have contributed to the appearance of the multiple errors on equipment belonging to another maintenance trade than the faulty equipment.

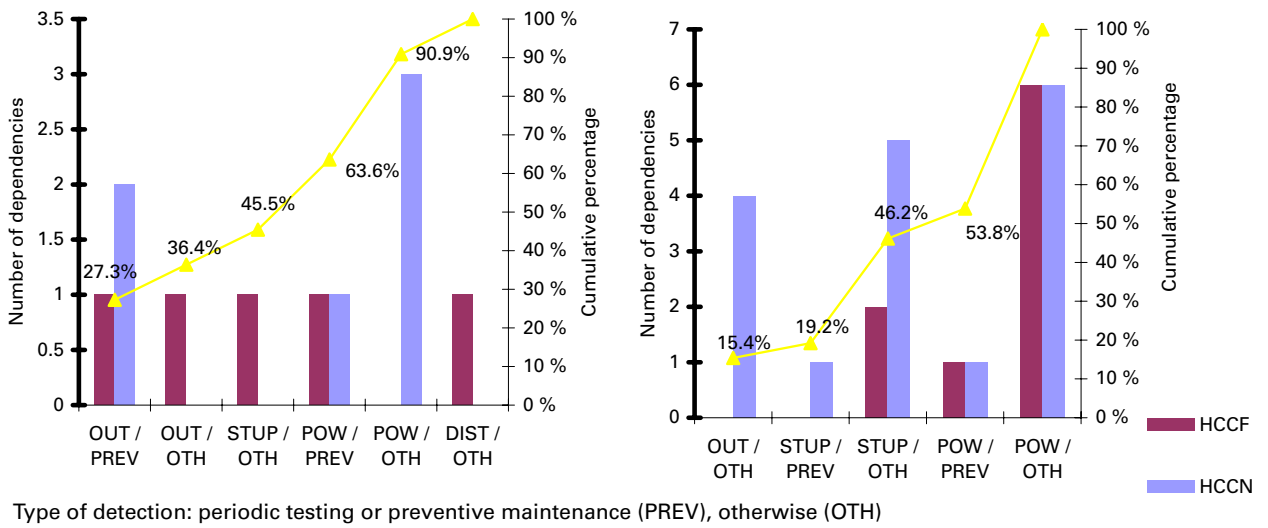
In addition in the second plant Loviisa, design deficiencies of IC (instrumentation and control) concerning documentation of modifications and of maintainability also contributed to a significant number of functionally non-critical common cause failures.

Multiple human errors stemming from refuelling and maintenance outages. The review of the analysed set of both single and multiple human errors (HCCFs and HCCNs) at the both sites showed that most errors in relation to maintenance stem from the refuelling and maintenance outage periods. This is a natural result because the dominating part of the modifications is performed during the annual outages.

Distribution of the plant operational states at failure detection, when the common cause failures originated from the refuelling and maintenance outages, is shown in Figure 6.

The more on left in the Figure 6 the operational states of the detection of the multiple failure events are, the better is the outcome of maintenance planning and operability verification.

The analysis shows that more than half of the multiple human errors remained latent after the start-ups from outages to the power operating periods at both sites. At the Olkiluoto site about a third of the common cause failures were identified promptly during the same outage before the start-up of the plant. The first 15 percent of all the common cause failures which were detected during the outage at the Loviisa plant did not become



Type of detection: periodic testing or preventive maintenance (PREV), otherwise (OTH)
Operating states at detection: power operation (POW), refuelling outage prior to start-up (OUT), hot shutdown (HOT), cold shutdown (COLD), plant start-up (STUP), plant shutdown (SHDN)

Figure 6. Distribution of fault detection states of human common cause failures born during maintenance outages.

functionally critical before their detection. They (HCCNs) however disturbed the plant start-up preparations at the end of the outage. At the Loviisa site, about 30 percent of the common cause failures could however be detected during the rather lengthy plant start-up following the outage before the power operation state.

The contents of the Figure 6 could represent a direct performance indicator of the quality and outcome of the maintenance and operability verification planning at the nuclear power plants. Although this database of the HCCFs and HCCNs is rather small, it can however be concluded from the set of the thorough event analyses that a too large proportion of the common cause failures born during the outages remain latent in the technical systems up to the power operating periods. Thus there are development needs in maintenance and operability verification planning for prevention of CCFs at the both NPP sites.

Detection activities of the human common cause failures. In the following Figure 7, the distributions are shown of the detection activities of the failures which were identified as human originated common cause failures (HCCFs and HCCNs).

The Figure 7 reveals that a small proportion of the common cause failures was detected in periodic testing, preventive maintenance or condition monitoring. At the Loviisa plant only 12 percent, i.e. four common cause failure (CCF) cases were identified in such periodic activities as periodic testing, periodic preventive maintenance or periodic condition monitoring. At the Olkiluoto plant, one third (5 cases of 14) of the CCF cases were detected in periodic testing (4 cases) or preventive maintenance (one case).

When the failure detection activities are studied of those common cause failures which have passed through from the outages to the power operating periods (see also Figure 5), the following observations can be done. Two failure cases of totally 5 cases detected at power operation at the Olkiluoto plant, were detected in periodic testing or periodic preventive maintenance. In turn, at the Loviisa plant, only two cases of totally 14 CCF cases born during the maintenance outage and passing through to the power operation could be identified in a periodic test or periodic preventive maintenance activity. When the failure detection was studied of those common cause failures which were born during the operating periods, similar observations on periodic activities could be done. For instance, at the Loviisa plant eight common cause failures were born during the operating periods. None of these six HCCNs or two HCCFs were detected in periodic testing or maintenance, but by chance, through alarms or on demand.

The detection of such a small proportion of the common cause failures in periodic testing activities indicates that operability verification (i.e. installation checks, functional testing, start-up testing) at the end of the complex maintenance works and the modifications in important systems should be improved. The planning of the coverage and contents of the operability verification requires in such cases tailoring instead of performing the standard

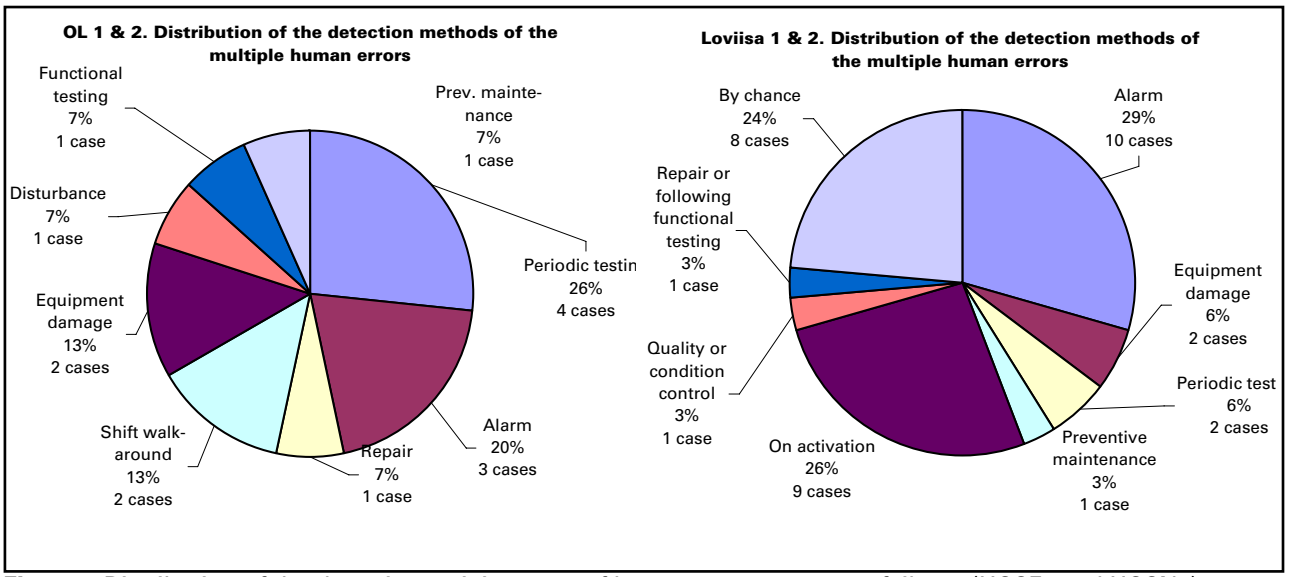


Figure 7. Distribution of the detection activity types of human common cause failures (HCCFs and HCCNs).

periodic tests of the equipment at the end of work.

It can also be concluded that maintenance and modification related errors originating from power operation are more inconvenient to detect immediately by proper installation checks, functional or start-up testing (which are more suitable at the end of outages and the plant start-ups) because of operational disturbance risks and restrictions.

Weaknesses in the operative defensive barriers. An analysis of the broken operative barriers against human common cause failures was performed as a part of the thorough "maintenance event" analyses. For statistical compilation of the broken operative barriers one front-line broken barrier per HCCF and HCCN case was selected. The analysed set of human common cause failures showed that the most missed primary opportunities for detection were in the installation checks and inspections of maintenance work, repairs and modifications, and in start-up testing of modifications. Thus there are most development needs in installation checks including component tests performed by the maintenance branch, and in the start-up tests of modifications performed by the operation branch, see Figure 8.

In addition, at the Loviisa plant the functional tests at the end of preventive maintenance or repairs performed by the operation branch were identified as significant contributors to the weaknesses in the operative defensive barriers against the common cause failures.

Weaknesses in the organisational defensive barriers. The organisational defensive barriers against dependent human errors are checks, re-

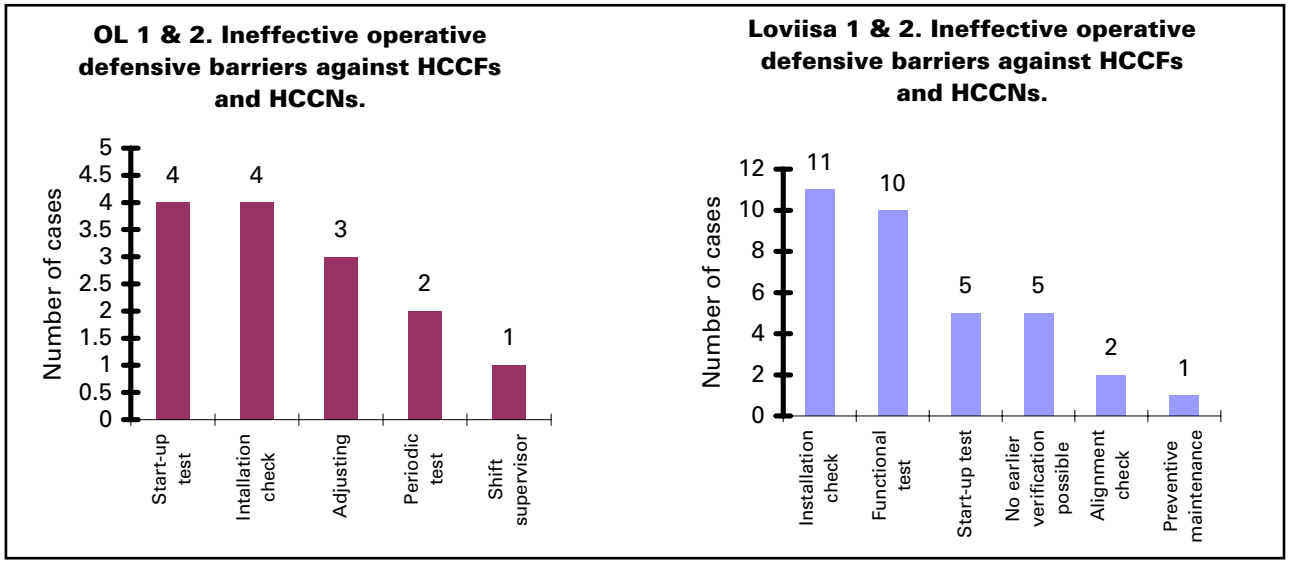


Figure 8. Weaknesses identified in operative defensive barriers against human CCFs.

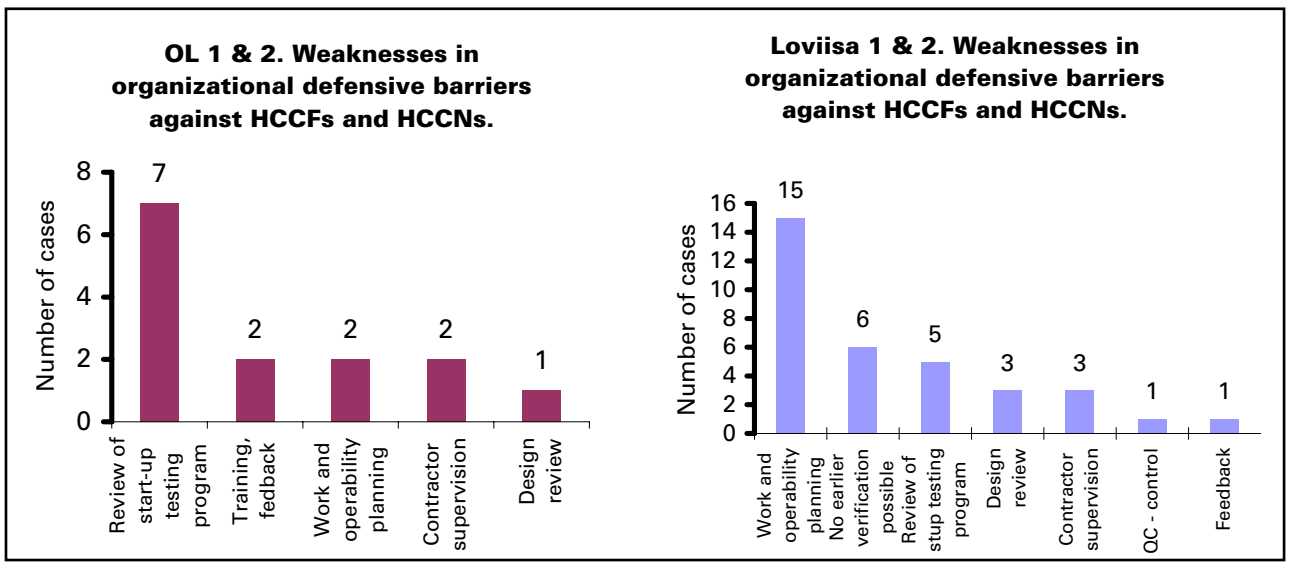


Figure 9. Weaknesses identified in organisational defensive barriers against common cause failures.

views and proactive actions performed by engineers, managers, safety and quality control personnel or contractor supervisors not directly involved in the operative or the same work in the plant units. In this simplified barrier analysis, it was looked for one broken organisational barrier per each HCCF and HCCN case (see Fig. 9).

The results indicate that an adequate review of the start-up testing programs of the modifications would have offered the best opportunity to strengthen the organiational barriers against common cause failures at the both sites. Also an appropriate review of the work and test planning of the work orders would have offered significant opportunities to correct weaknesses in the organisational barriers against common cause failures. In addition, weaknesses in contractor supervision and knowledge were in some specific cases identified as contributors to common cause failures.

Also weaknesses in the design review have in some specific cases allowed deficient technical dicumentation to pass through to use thus contributing to common cause failures in connection to modification or repair work. The non-closure of the experience feedback loop was also considered here as a broken organisational barrier in such recurrent cases where a similar HCCF/HCCN mechanisms occurred at both units of the plant and no corrective actions were inbetween implemented.

The number of human originated common cause failures. The annual average of the number of human common cause failures (sum of HCCFs and HCCNs) through the studied calendar years is app. 5 cases per year at Olkiluoto plant and app. 11 at Loviisa plant. The annual numbers of the events are shown in the Figure 10.

When comparing the numbers of the different plants Olkiluoto and Loviisa, the annual averages of the functionally critical human CCFs are 2,67 resp. 3,67, i.e. in the same order of magnitude. The significant differences in the amount of the multiple human errors come from the higher number at the Loviisa plant of the functionally non-critical human common failures (HCCNs). HCCNs are, as earlier mentioned, precursors to the functionally critical common cause failures (HCCFs).

It should also be noticed that the figure shows the year of detection of the HCCFs and HCCNs. The multiple human errors have in the most cases born during the same year, but in a part of the cases during the earlier years.

Because of the limited analysis periods of the multiple human errors, no conclusions of their timely trends can be drawn. Despite the variations in the annual numbers, the averages of those annual numbers can be used as reference values when similar analyses for evaluation of the performance of maintenance and operability planning, and of the recurrence of the human common cause failures, are done in the future.

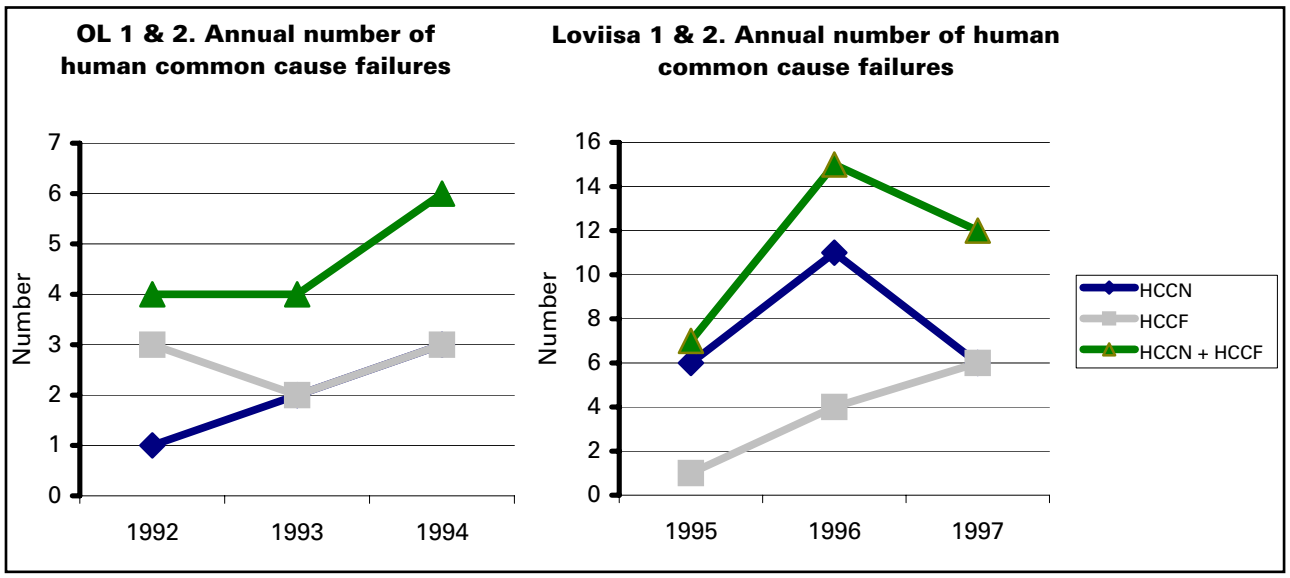


Figure 10. Annual distribution of HCCFs and HCCNs through 3 calendar years.

Suitable performance indicators for the future evaluation of the human originated common cause failures in relation to maintenance could thus be:

- The number of human common cause failures (HCCFs and HCCNS) stemming from the maintenance outages and passing through to the operating periods (see Figure 6),
- The moving average of three years of the annual number of the human common common cause failures (HCCFs and HCCNs) in relation to maintenance,
- The annual number of HCCFs and HCCNs in the safety related systems (subjected to requirements in the Limiting Conditions for Operation of Technical Specifications).

In addition, the annual number of maintenance rework covering both single and multiple errors would be a good indicator on human performance and quality in maintenance work and planning. Prevention of human errors in maintenance and repairs is prevention of rework.

Safety significance of the human common cause failures in relation to maintenance. A significant number of human errors and common cause failures took place in safety related systems. For instance at the TVO plant 6 of the 8 cases of the human originated common cause failures, and 3 of the 6 functionally non-critical human cause failures were in the safety related systems. In turn at the Loviisa plant, 5 of 11 cases of human CCFs, and 9 of the 23 human CCNs, were in safety systems.

At the Olkiluoto plant, in 10 of the all 14 multiple human error cases more than two components were affected. In turn at the Loviisa plant more than two components were affected in 9 of the all 34 multiple human error cases.

Although no risk increase factors using PSA models [NKA/RAS-450 1990] were calculated, it can be concluded that human common cause failures in relation to maintenance and modifications apparently have a significant safety influence. But much more safety degradations would have been caused, if no preventive maintenance or renewal of equipment took place. This is shown by e.g. ageing related common cause failures which occurred due to lacking preventive maintenance identified during the earlier study [Laakso, Pyy & Reiman 1998].

In addition to the safety systems, all other plant systems were covered in the search and analysis of the human common cause failures due to the fact that human error mechanisms may be similar at the different parts of the plant. Thus, a more extensive database was obtained for learning of multiple error mechanisms to prevent the significant human common cause failures.

5 Conclusions and recommendations

Conclusions, proposals for remedies and recommendations on improvement needs are presented in the following chapter based on findings from the studies and maintenance R&D concerning the both nuclear power plants.

Quality of maintenance planning and operability verification. The review of the analysed set of both single and multiple human errors (HCCFs and HCCNs) at the both sites showed that most errors in relation to maintenance stem from the refuelling and maintenance outage periods. This is natural because a larger part of all modifications is installed during the annual outages than during operation. The earlier Figure 6 shows the distribution of the plant operational states at failure detection, when the common cause failures originated from the refuelling and maintenance outages.

The analysis shows that more than half of the multiple human errors (HCCFs and HCCNs) remained latent after the start-ups from outages to the power operating periods at the both sites. The contents of the Figure 6 could represent a direct performance indicator of the quality and outcome of the maintenance and operability verification planning at the nuclear power plants. Although the event analysis database of the HCCFs and HCCNs is rather small, it can however be concluded from this set of thoroughly and systematically performed event analyses that a too large proportion of common cause failures from the outages remain latent in the technical systems to the power operating periods. The analysis results also showed that the multiple human error events revealed during power operation were detected in periodic testing or periodic maintenance only in two cases at each plant. This suggests improvement needs in planning of the maintenance and installation inspection, functional testing and operability verification phases connected to the work actions during outages on important equipment and systems.

But at first we start with a description of requirements on activities and knowledge on maintenance management and work.

Requirements on maintenance activities and work practises. The detailed analysis, classification and statistical treatment of the maintenance related errors have provided information for focusing organisation-psychological studies into most relevant aspects in maintenance and operability. The aim of the organisation- psychological studies in Finnish NPPs has been to develop a model for the maintenance core task and assess the maintenance culture. The case studies started at the Loviisa and continued at the Olkiluoto and Forsmark nuclear power plants [Reiman, Oedewald & Rollenhagen 2005].

The critical demands of maintenance and the instrumental demands needed to respond to the critical demands were conceptualised by a maintenance core task analysis. The model depicts maintenance as balancing between the three critical demands of *Anticipating, Reacting* and *Monitoring & Reflecting* as well as between the instrumental demands.

The organisational core task model was used to assess the safety and efficiency of organisational cultures of the maintenance organisations by help of interviews, observation, survey and workgroups. Among others, in the analysis of the interview data and group working sessions at the nuclear power plants concerning the maintenance core task demands in one's own maintenance work following tensions could be identified:

- situational judgement vs. generally applicable rules,
- certainty vs. uncertainty about the effects of maintenance actions,
- specialisation vs. maintaining overview.

In the assessment of the maintenance culture, the idea was that if the instrumental demands (*Flexibility, Methodicalness and Learning*) are carried out well in the organisation, you can suppose that the maintenance organisation is able to fulfill the critical demands. In the Figure 11, the maintenance management and work practises (such as prioritisition of work tasks, coordination of tasks between different technical disciplines and activities, definition of responsibilities, planning of maintenance program, information management, transparency of actions & documentation of work and findings, verification of operability, adhering to work permit procedures, and restoring of operability) needed for the implementation of the critical demands of maintenance are also shown [Oedewald & Reiman 2003].

The critical demand *Anticipating* of the maintenance activity refers to the intention to anticipate the condition of the equipment and the state of the plant and the effects of the maintenance actions, and to plan the needed maintenance tasks and resources in advance. *Reacting* refers detecting and diagnosing deviations and acting accordingly. It requires thus readiness to restore the operability of equipment and systems after sudden failures of critical equipment, expected failures on non-critical equipment or findings in periodic testing of equipment or systems. *Monitoring and reflecting* refer to the uncertain nature of the knowledge concerning the condition and state of the equipment and systems. *Reflectivity* means a critical reviewing of the effectiveness and results of the maintenance actions and of the bases on which the maintenance tasks are founded.

The organisational core task model depicts knowledge creation and problem solving activity as being inherent in the maintenance activity and brings thus the demands of the maintenance management and work close to that of knowledge work. In the following sections, recommended improvements and proposed actions originating from the results of the human common cause failure and error studies are given to the maintenance management and work tasks. In the recommendations and proposals, a reference is also given to the (often) conflicting critical, instrumental or knowledge demands of the tasks concerned.

Planning of operability verification in relation to small or ordinary modifications. The review of the analysed multiple errors showed that difficulties in planning of the necessary testing and

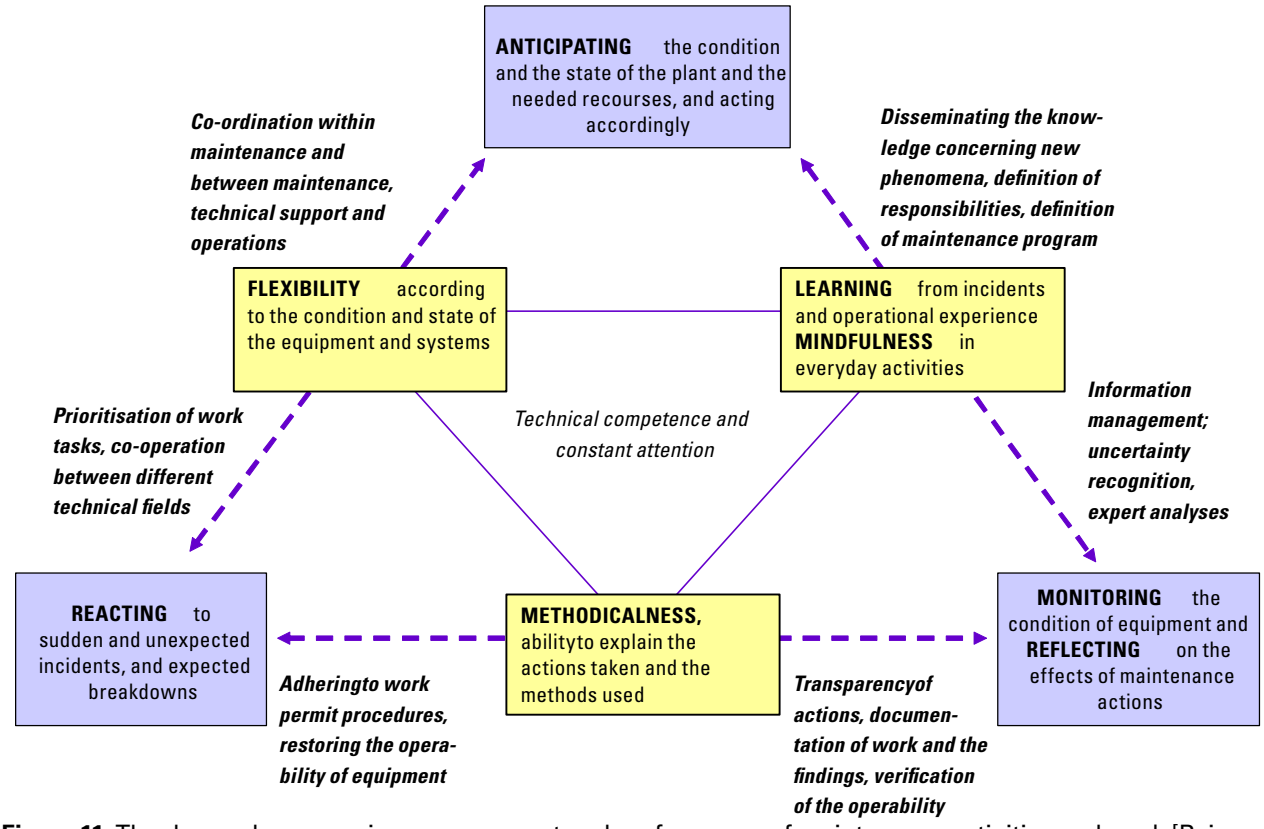


Figure 11. The demands concerning management and performance of maintenance activities and work [Reiman, T. et al 2005].

installation inspections of small and ordinary (not big) plant modifications were significant sources of common cause failures. More than half of the human common cause failures from outages remained latent into the power operating periods. The most multiple human errors originating from small or ordinary modifications, such as e.g. renewals of actuators, motor operated valves and solenoid valves, changes in transformers, or introduction of difference pressure measurements, position indications or switches as modifications or as a part of them, could be reduced by a more tailored definition and coverage of their start-up testing programs.

In planning the modifications in parallel trains of important equipment, the needs of staggered implementation, the real operating conditions such temperatures, pressures or pressure differences for testing, and the multiple train risks should be evaluated and considered.

After modifications or intrusive maintenance in important equipment condition monitoring would be recommended for reducing the uncertainty about equipment operability or reliability.

The operability planning and verification tasks of small or ordinary modifications are complex and are subjected to the critical demands of both Anticipation and Monitoring & Reflecting and require thus balancing between the Methodicalness and Flexibility as well as Learning. The planning task requires both a functional overview & technical specialist knowledge as instruments for quality results.

Planning of maintenance and operability of complex or intrusive preventive maintenance and repairs. Improvements could also be achieved by identifying better in the work planning from the operating experiences those complex or intrusive repair and preventive maintenance work tasks and actions which are prone to errors and can introduce unwanted changes in the function of equipment or systems. Such uncertain cases in important equipment require a tailored planning of the coverage of the installation inspections of their instrumentation, automation and electrical equipment and the functional testing of equipment effected. This planning case shall include a need evaluation of the functional testing at both component and system level. The tension between the situational judgement and the generally applicable routines is manifested in this concrete planning situation where it is no longer clear if the normal periodic testing task can be defined as the sufficient operability verification action in the work order. Generally for important equipment, a functional test should be added as a planned task into its preventive maintenance programme to assure the functional operability after work.

In planning the test arrangements of important equipment in parallel trains, the needs of staggered testing , the real operating conditions and the multiple train risks should be evaluated. and considered. For instance, at the second of the plants maintenance and testing actions in parallel redundancies was recently replanned to different weeks and a trains' crossing effects inspection by control room is obligatory in exceptions.

The operability planning and verification tasks of cumbersome or intrusive repair and preventive maintenance works are complex and are subjected to the critical demands of both Anticipation and Monitoring & Reflecting and require thus balancing between the Methodicalness and Flexibility as well as Learning. The planning task requires both a technical specialist & functional overview knowledge as instruments for quality results.

Spare part changes or minor changes in parts to be identified as minor modifications. Some events demonstrate that minor modifications are sometimes introduced unknowingly, when a new spare part, component or part contains changes as compared to the earlier versions [NEA/CSNI/R(2004)17, NEA/CSNI/R (27.4.2005)]. Spare part changes or minor changes in parts should be better identified as minor changes in maintenance planning and work. Changes in material, size, form or lubrication of the parts can be such minor modifications which have a deviating failure effect on the equipment or system function. Examples can be e.g. wrong screws, fuses, relays, switches, cables or guards. Such minor changes in important equipment should be subjected to the plant modification process, instead of the repair or maintenance process only, to allow a proper technical and safety review and functional test planning before implementation into operation.

This identification and planning task is subjected to the critical demands of both Anticipation and Monitoring and requires both Learning and Methodicalness as well as technical specialist knowledge down to a detailed level as instruments for quality results.

Planning and decision of modifications. The review of the analysed multiple errors showed that difficulties with small and normal plant modifications and in planning of their operability were significant sources of common cause failures. A modification in an operating plant should be considered as a risk. Thus modifications in old plants should always be very well justified. Thousands of small or ordinary technical modifications were implemented at the studied plants during the analysis periods. It is in the design and implementation difficult to cover all latent functional relationships, failure modes and effects of the modifications without a good functional analysis of interdependencies and well planned and comprehensive start-up testing programs. The testing program of modifications shall correspond to the real operating conditions and cover both the component and system levels.

Modifications which are needed to provide significant safety, reliability, capacity, efficiency or maintainability remedies of shortcomings or enhancements, including related auxiliary system changes, are naturally justified. As well, the obsolete technology which exhibits missing spares and know-how has to be replaced. However to select the best decision option, a risk evaluation of e.g. teething problems of the design and function of the modification should be included in the decision criteria.

This complex planning and decision task is subjected to the critical demands of Anticipation and Reflecting and requires both Methodicalness and Learning as well as the functional overview & specialist knowledge as instruments for quality results.

Turn-over procedures. Distinct turn-over and acceptance procedures of the technical modifications and their documentation between the different modification project phases are recommended for consideration. Distinct turn-overs from the design & delivery phase to the installation phase at plant, and from the installation phase to the start-up testing & operation phase between the responsible organisational units (both internal suppliers and customers) are proposed. Such strict acceptance practises were applied before the turn-overs of single technical systems during the installation and start-up testing phases of the latest Nordic BWRs. These procedures would help as organisational defensive barriers to prevent better the unfinished modifications and deficient procedures or documentation from passing through into installation and operation.

Living Probabilistic Safety Analysis (PSA). A significant number of human errors and common cause failures took place in safety related systems. For instance at the TVO plant 6 of the 8 cases of the human originated common cause failures, and 3 of the 6 functionally non-critical human cause failures were in the safety related systems. In turn at the Loviisa plant, 5 of 11 cases of human CCFs, and 9 of the 23 human CCNs, were in safety systems.

In addition to the safety systems, all other plant systems were covered in the search and analysis of the human common cause failures to obtain a larger database and understanding of such human error mechanisms that can lead to safety significant human common cause failures.

A check of the coverage of the identified multiple human errors in the common cause failure models, mechanisms, event sequences and data in the PSA studies of today is therefore recommended.

Although no risk increase factors using PSA models [NKA/RAS-450 1990] were calculated during the studies, it can be concluded that human common cause failures in relation to maintenance and modifications apparently have a significant safety influence and that living PSA can be used for determination of the safety importance of parallel equipment prone to CCFs in relation to maintenance.

This interactive PSA analysis task requires both Methodicalness and Learning as well as a good overall knowledge of the functional relationships as instruments for quality results.

Grading of planning requirements and review of work orders. Grading the planning requirements of the maintenance objects based on their safety and availability importance or work complexity would also help to prioritise the resource allocation for planning. At both utilities a grading of equipment into four different maintenance classes based on plant level safety, availability and cost objectives is already available. This prioritisation could also help to select the work orders and plans which should be reviewed before the work permit. For instance nowadays, at one of the utilities the operation maintenance coordinators, operation technicians and maintenance foremen review the work orders of the next week in weekly meetings. These reviews can lead into requirements to improve the

work description, object definition or testing in individual work orders.

The complex and multitechnical repair or preventive maintenance actions should be identified in planning. One should therefore review from the maintenance information system, whether the repair or maintenance actions are according to operating experiences prone to errors or could imply changes in the function of the equipment or system. Such cases in important equipment would require a larger or a tailored coverage of installation inspections and functional testing.

This management and planning task is subjected to the critical demand of Anticipation and requires both Learning and Methodicalness as well as functional overall & specialist technical knowledge as instruments for quality results.

Planning of effective preventive maintenance tasks. Maintenance strategies and effective maintenance tasks for prevention of failures on equipment and systems can be selected by the experience based RCM planning approach [Laakso, Simola & Hänninen 2002]. In planning the maintenance strategies, tasks and actions, the dependability requirements of different equipment are specified based on the importance of the equipment for fulfilling the plant level objectives of safety, availability and cost.

In the operating plants, the EBRCM method utilises the maintenance history data in the planning of changes into the preventive (condition based and predetermined) maintenance tasks and intervals , including small redesigns, to reach the reliability and maintenance objectives. Identification and planning of effective preventive tasks for detection and prevention of common cause failures and errors, and for operability verification, connected to the preventive maintenance work of the important equipment shall be integrated to the PM planning approach and defined in the PM programs.

Definition of the maintenance strategies of equipment and systems- definition of the bases on which and when preventive tasks need to be done- reduces also the potential for error by improving the meaningfullness and motivation of the work and by reducing sometimes inadvertent initiators.

This complex maintenance management and programme planning task is subjected to the critical demands of Anticipation and Reflecting and requires both Methodicalness and Learning as well as the functional overview & specialist knowledge as instruments for quality results.

Use of condition monitoring for identification of deviations and maintenance steering. A survey of the use of condition monitoring information for maintenance planning at three Nordic nuclear plants indicates that condition monitoring is increasingly implemented, but very selectively and in a rather slow pace for condition based preventive maintenance. A combined strategy of condition based preventive maintenance and predetermined preventive maintenance is applied for important

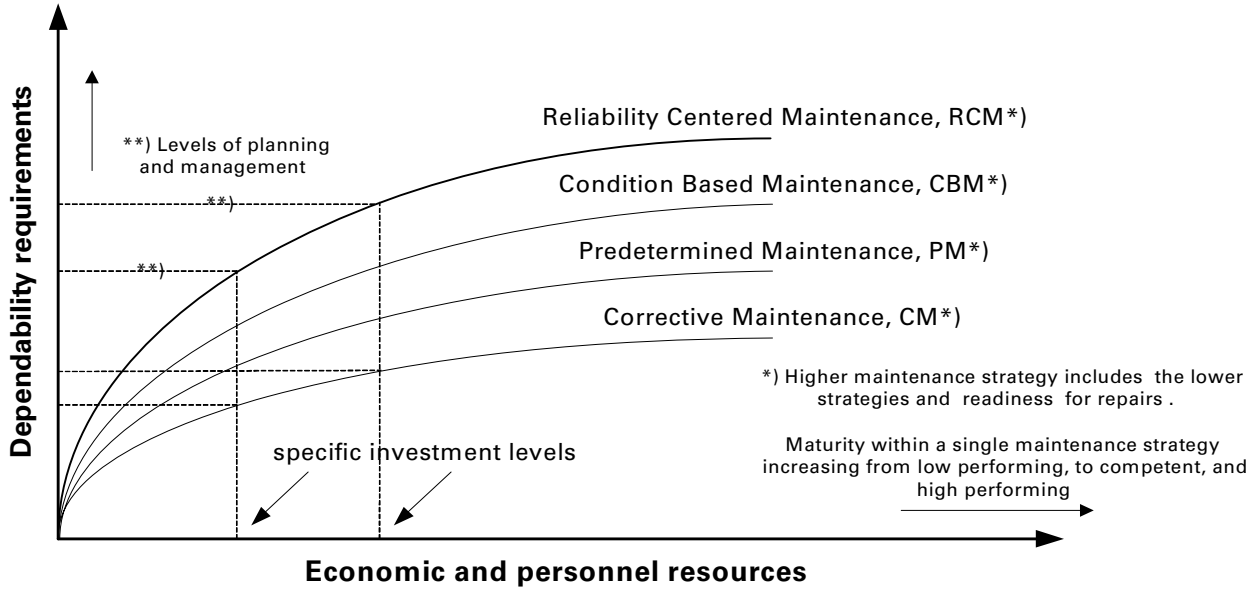


Figure 12. Effectiveness of distinct maintenance strategies to reach the dependability objectives of equipment and systems.

equipment such as main circulation pumps, generators, steam turbines and turbine condensers and to some extent for motor or pneumatically operated closing valves [Laakso, Rosqvist & Paulsen 2003]. This combined strategy is thus applied to eliminate or reduce functionally critical failures and damages on very important equipment.

Condition based maintenance strives to prevent the functional failure of equipment by utilising condition monitoring information, information systems and personnel expertise for identification of deviations and maintenance steering of necessary preventive maintenance actions instead of performing the predetermined maintenance tasks at predetermined time points. An increased use and analysis of existing condition monitoring information have a great potential in increasing condition based preventive maintenance [Laakso, Rosqvist & Paulsen 2003]. The analysis of condition monitoring information would increase the certainty about equipment condition. One way to reduce the number of errors and unavailability of equipment is to avoid unnecessary maintenance which has the potential to cause unnecessary failures. Using condition monitoring information to steer the preventive maintenance to correspond better the real needs [Laakso, Hänninen, & Hallin 1995] could thus also reduce the number of error prone predetermined intrusive and disassembling maintenance actions performed. In early life failures caused by errors in installations or disassembling maintenance, the use of planned condition monitoring can also help to discover pre-existing defects prior to their development into functional failures by environmental or operational loads such as vibration, heat, temperature transients, activations etc.

A more situation specific steering of preventive maintenance actions to restore the degraded equipment condition to standard condition before development of functional failures would also contribute to a better utilisation of the personnel expertise and equipment responsibility. The use of process monitoring information and control room better for condition monitoring of equipment would also contribute as a help. An effective use of process information for analysis of the condition of equipment requires a good access of the maintenance personnel to this information. Thus the condition based preventive maintenance strategy puts new demands on flexibility and knowledge based approach of working instead of the rule based approach of the predetermined periodic maintenance.

It is recommended to integrate the condition monitoring into the functional testing phase of the modifications or intrusive maintenance for important equipment. Increased use of effective condition monitoring for operative identification of deviations and steering of maintenance actions instead of predetermined and intrusive maintenance tasks is recommended. Examples of good working practises at the both plant sites are such co-operation where the control room personnel performs the testing and the maintenance personnel the condition monitoring simultaneously in certain periodic testing of rotating standby safety equipment.

This identification, planning, decision and work

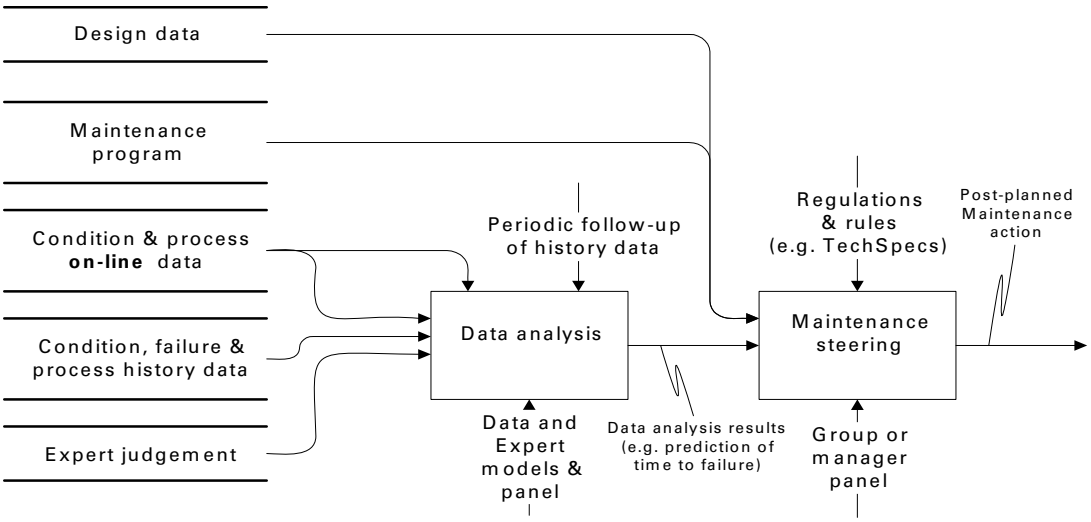


Figure 13. A diagram showing the information sources and decision context related to operative maintenance steering based on condition monitoring.

task of condition based maintenance seems to be most difficult because it is subjected to the all critical demands Monitoring, Reacting, and Anticipation. And it requires the conflicting instruments Felixibility and Methodicalness as well as Learning and specialist knowledge as instruments for quality results.

Adjustment needs of the pre-planned work orders. At planned maintenance or installation of equipment such as e.g. electric motors, valves or piping, it has proven necessary to disconnect extra cables or actuators to facilitate the planned work locally in the plant. Sometimes these unplanned work objects have not been reconnected or reconnected poorly during the work. But the corresponding increased needs of installation inspections or functional testing after the work of this additionally fixed equipment have remained unnoticed leading to common cause failure cases during operation.

A more agile initiation of necessary adjustments to the pre-planned work orders to correspond the specific local or new conditions identified at work by maintenance personnel would have helped. The question is also whether it is acceptable to make a personal judgement and perform the work needed, or should the work be interrupted until the new work order is planned and permitted.

This planning and work task is subjected to the critical demands of Reflecting and Reacting and requires both Flexibility and Learning as well as adhering to work permit procedures and the knowledge of the technical function as instruments for quality results.

Understanding the maintenance and operability verification process. Modelling of the maintenance and operability verification process including the organisational interfaces, covering both maintenance and small modifications, is recommended. The errors, their progress, missed detection and occurrence of the common cause failures could also be compared with the process models and be made visible in them. The modelling would help to increase the understanding of the planning practises and work order procedures and identify and visualize the possible weaknesses requiring remedies in the process of maintenance and operability.

This planning task is subjected to the critical demands of Anticipation and Reflecting and it requires both Methodicalness and Learning as well as an overall knowledge of maintenance and operation as instruments for quality results.

Identification, reporting, event analysis and operative prevention of common cause failures. A new solution has been implemented in the new power plant information systems at the both Finnish NPP sites for identification and reporting of common cause failures. This enhancement will complement the earlier failure and repair work order feedback data. The information is given on the screen of the power plant information system by a question and relevant text description of a suspected common cause failure.

This routine will help to operatively identify CCFs better in the future from the plant information system and to start continuous human and technical CCF event investigations for their prevention. Already today, the “operation event reports” at one of the sites cover rather well that part of the CCF cases which are timely identified. Also a promising reporting and treatment system of deviations and near misses at the other site was recently implemented. However the “maintenance event related” CCF cases have remained more undetected and thus have not been adequately reported.

A fault repair process model, including inspections of the prospect of a CCF, for one of the Finnish sites has been prepared to support the above operative investigation and prevention task. The following process flow model shows, how you proceed from the failure detection through the activities of work planning, safety actions of the work, repair work, restoration of the safety actions, testing and start-up of the work object up to the acceptance of the work and closing the activities in the history part of the plant information system. A part of the activities will include checkpoints for the own or independent inspections to be performed by the actors from maintenance or operation. The checkpoints are given in Fig. 14 with *-marks.

In the above process model the activities are supervised by controls or rules which are coming as arrows from top and and resourced by organisational branches which are given down in the activity boxes. For instance, in connection to the safety actions of the work, the shift supervisor performs an inspection of the possible train crossing effects in order to identify and prevent possible common cause failures in safety related systems controlled by Limiting Conditions for Operation (LCO).

As the reporting activity of final feedback information is finishing the maintenance work in the information system, a suspected CCF can be confirmed, analysed and reported or alternatively struck off as a common cause failure. This can be performed in a further investigation in co-operation between maintenance, operation and safety branches.

In the operating plants, it is easiest to implement new routines such as above for identification, reporting and prevention of human and technical common cause failures and errors when the plant information system is renewed or upgraded and the ways of acting are simultaneously defined, modified and trained. This opportunity was used for implementation of the classification of direct errors of this report (see Table IV) when defining lately the new failure classification and reporting for the new plant information system of one of the Finnish NPP sites.

A further developent of maintenance and technical personnels' responsibilities of the function and dependability of specific equipment and systems are also expected to improve the use of feedback reporting of failures and maintenance in the plant information systems for follow-up, analysis and planning for prevention or reduction of multiple and recurrent errors in future.

Training. The event analyses of maintenance and operability related multiple and single errors would provide a good plant-specific material for training of the maintenance, operation and technical personnel. This improves understanding of the error mechanisms for learning, and error identification and prevention purposes, as well as for maintenance quality assurance. The training should also include the definitions of common cause failures and types of direct errors on equipment supported by examples from the event and error descriptions.

Maintenance and operability planning activity. The review of the results of the root causes of the analysed human common cause failure events indicate that planning of maintenance work phases and operability verification tasks is a very demanding task due to the complex planning environment of different objectives, safety requirements and instructions, and needs of multifunctional plant technical, maintenance and functional knowledge. The planning task demands both Anticipation and Reflecting and balancing between the Methodicalness and Flexibility as well as Learning which bring it to a knowledge work.

Thus the results of this analysis show that maintenance and operability planning should not be regarded as separate functions at the plants but

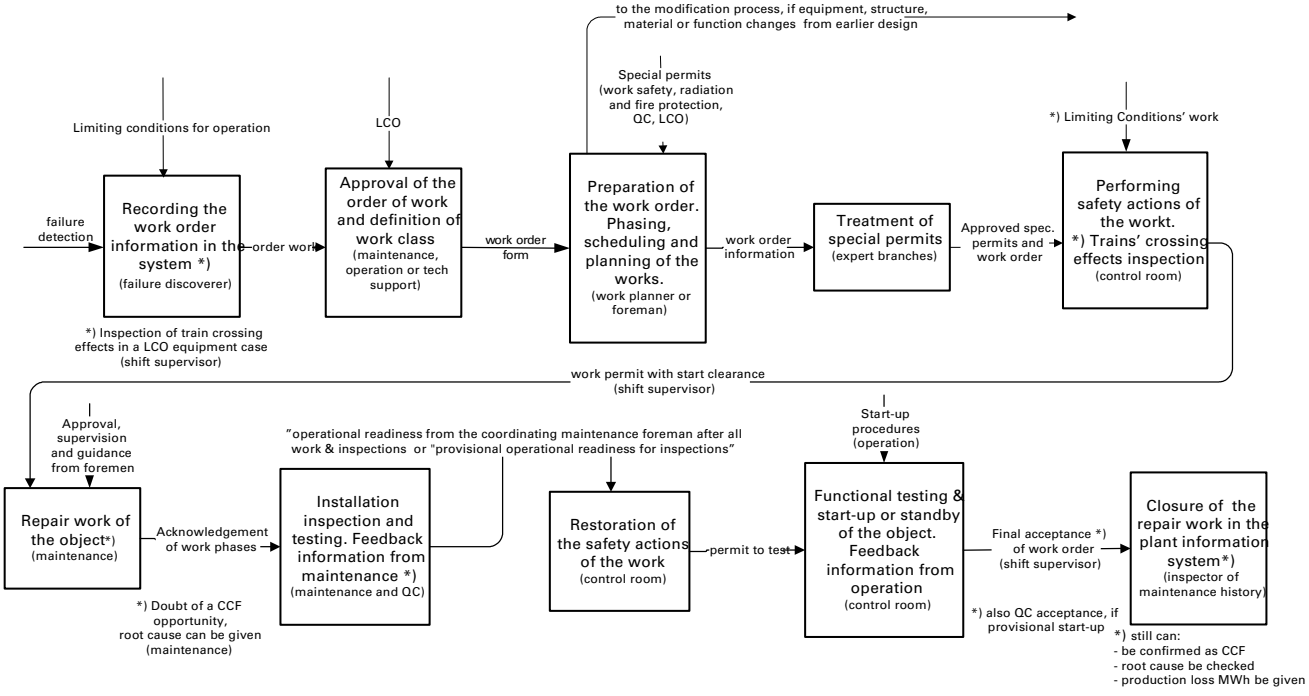


Figure 14. A fault repair process with a view to operative identification and prevention of CCFs. (check points *- marked).

performed better as an integrated planning requiring the joint knowledge of both the maintenance and operation branches. This conclusion is also confirmed by the findings from the studies of operational readiness verification in Swedish nuclear plants [Hollnagel, E., Gauthereau, V., Persson, B. 2004].

Good examples of recent co-operative developments at the Finnish nuclear power plants are the maintenance planner on duty in the control room during the maintenance outages at one of the sites, and maintenance supervisors for daily coordination of plant maintenance and condition monitoring at the operation organisation at the other site.

Concluding remarks. Although a large part of the studied error events may be suggested as negative experience, the experts and managers in the nuclear power plants and regulatory body view these studies as extremely valuable for experience feedback. They regard this improved knowledge of errors as useful for the development of safety, operability and control of maintenance as well as for prevention of costly maintenance rework or forced plant shutdowns. The feedback from discussions of the analysis results with plant experts and professionals has been crucial in developing the final conclusions and recommendations that meet the specific development needs of remedial actions and practises at the plants.

After these studies, analyses of the recent maintenance history have continued at one of the plants where the error analyses have been performed by the plant maintenance development personnel and reported in interaction with VTT [Leino & Laakso, 2005] and are planned for continuation in 2006 at the other plant, too.

It must however be admitted that human errors are inevitable and cannot be totally eliminated. The aim has been to turn negative experiences of "undetected common cause failure events" and recurrent errors into so uneventful maintenance and operation as reasonably practicable. Learning from one's and others' occurred errors and experiences is the best way for the real actors to learn and develop.

References

EN 13306 1999. Maintenance Terminology. European Standard prEN 13306. Final draft. April 1999. Brussels. 53 p.

ICDE 1999. ICDE project report on collection and analysis of common-cause failures of centrifugal pumps. OECD/NEA(CSNI/R(99)2. September 1999. 30 p.

Hollnagel, E., Gauthereau,V., Persson, B. 2004. Operational readiness verification, Phase 3. A field study at a Swedish NPP during a productive outage (safety-train outage), SKI Report 2004-10. January 2004. 34 p.

IEC 50(191) 1990. International Electrotechnical Vocabulary. IEC Chapter 50 (191). First edition 1990-12. International Electrotechnical Commission. 112 p.

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. pp. 103–107. ISBN 87 7303 422 3.

Laakso, K, Hänninen, S, Hallin, S. 1995. How to evaluate the effectiveness of a maintenance programme. Paper presented in Baltica III Conference 1995, Condition and life management for power plants. Helsinki–Stockholm, 6–9 June 1995.10 p.

Laakso, K., Pyy, P., Reiman, L. 1998. Human errors related to maintenance and modifications. Finnish Centre for Radiation and Nuclear Safety STUK, Helsinki. 42 p. STUK-YTO-TR 139. ISBN 951-712-242-X.

Laakso, K., Simola, K. and Hänninen, S. 2002. Maintenance Analysis of Technical Systems. In Kunnossapito 5/2002. Maintenance Research in Finland. pp. 49–51.

Laakso, K., Saarelainen, P. 2003. Inhimillisperäiset yhteisviat kunnossapitotoiminnan yhteydessä. Kunnossapitohistorian järjestelmällinen tutkinta ja analyysi Loviisan voimalaitokselle. (Human originated common cause failures in relation to maintenance activities at Loviisa NPP). VTT report BTU062-041220 in Finnish. 107 p. + app 26 p. Espoo 2003.

Laakso, K. 2004. Inhimillisperäisten yhteisvikojen esteiden jatkoanalyysi kohteena Loviisan voimalaitos. (Follow-up analysis of the barriers of human originated common cause failures applied to Loviisa NPP.) VTT Research Report BTU062-031211. Espoo. 33 p + app. 17 p. In Finnish. 10.8.2004.

Laakso, K., Rosqvist, T., Paulsen L. J. 2003. The Use of Condition Monitoring Information for Maintenance Planning and Decision-Making. Report NKS-80(2003), Nordisk kernesikkerhedsforskining NKS, Roskilde. 33 p.

Leino, M. Laakso, K. 2005. Inhimillisperäisten vikaantumisten tutkinta Loviisan voimalaitoksen vuoden 2003 kunnossapitohistorian avulla. (Analysis of human failure events from the Loviisa power plant maintenance history of the year 2003). Report in Finnish. 30 p. + app. A_B.xls.1.6.2005.

LOTI. Loviisa power plant information system. Brochure 4 p. For further information contact Fortum Power & Heat Oy. Loviisa nuclear power plant. FIN-07900 Loviisa, Finland.

NEA/CSNI/R(2004)17. 2004. Modifications at Nuclear Power Plants – Operating Experience , Safety Significance and the Role of Human Factors and Organistation. WGOE Workshop Proceedings. Paris. France. 6–8 October 2003. 272 p.

NEA/CSNI/R(27.4.2005). 2005. Safety of modifications at nuclear power plants - The role of minor modifications and human & organisational factors. Version 2.2. 27.4.2005. CSNI/WGOE. Paris. France. 78 p.

Oedewald, P., Reiman, T. 2003. Core Task in Cultural Assessment: A Case Study in Nuclear Power Plant Maintenance. In Cognition, Technology & Work 5 (4) pp 283–293.

Reiman, T.,Oedewald, P., Rollenhagen, C. 2004. Characteristics of Organizational Culture at the Maintenance Units of Two Nordic Nuclear Power Plants. Maintenance. To be published in Reliability Engineering and System Safety in 2005. Draft 36 p.

Pyy, P. 2000. Human reliability analysis methods for probabilistic safety assessment. VTT Publications 422. Dissertation for the degree of Doctor of Technology. Espoo. 63 p. + app 64 p.

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.