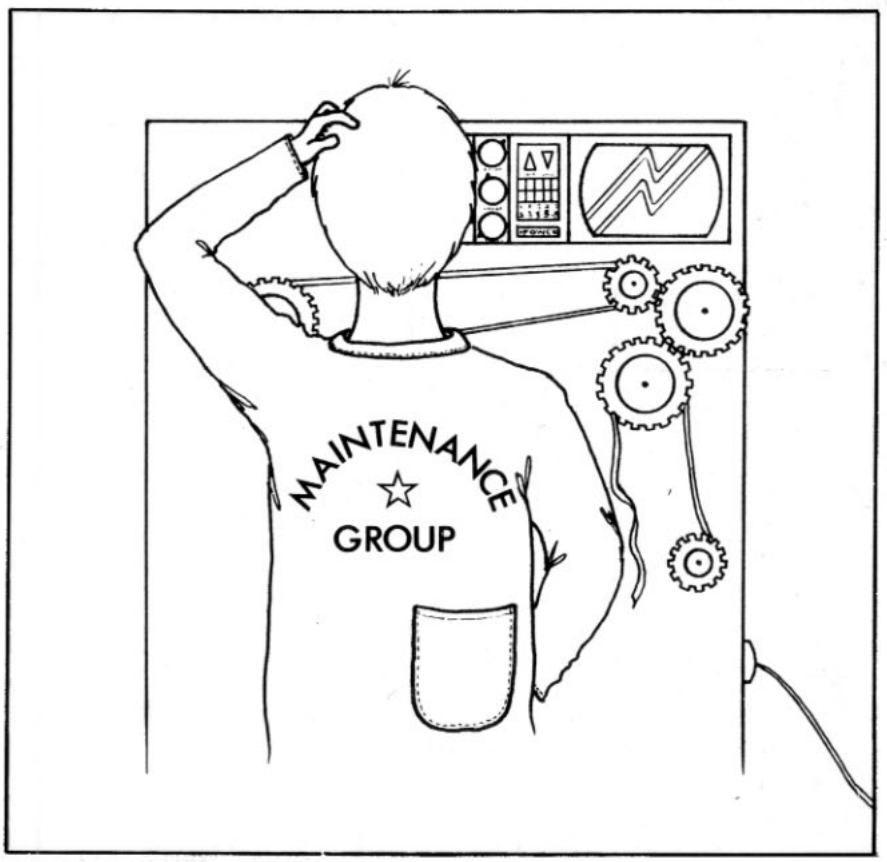
August 85

HUMAN ERRORS IN TEST AND MAINTENANCE IN NUCLEAR POWER PLANTS

NORDIC PROJECT WORK



nka

Nordic
liaison committee for
atomic energy

nka

Nordisk kontaktorgan for atomenergispørgsmål | Nordiska kontaktorganet för atomenergifrågor | Pohjoismainen atomienergia-yhdyselin | Nordic liaison committee for atomic energy

NKA/LIT(85)2

HUMAN ERRORS IN TEST AND MAINTENANCE OF NUCLEAR POWER PLANTS

NORDIC PROJECT WORK

Final report of the NKA project LIT-1

Edited by

Håkan Andersson
Studsvik Energiteknik AB

and

Bo Liwång
Swedish Nuclear Power Inspectorate

Sweden

August 1985

THE LIT STEERING COMMITTEE

B Wahlström*	Technical Research Centre of Finland (VTT)
L Goodstein	Risø National Laboratory
M Øvreeide	Institute for Energy Technology, Norway (IFE)
J Lindqvist	The Swedish State Power Board (SV)
F Marcus	Nordic Liason Committee for Atomic Energy (NKA)
B Liwång	Swedish Nuclear Power Inspectorate (SKI)

LIST OF PARTICIPANTS IN THE LIT-1 PROJECT

Swedish Nuclar Power Inspectorate (SKI)	Bo Liwång **	
	Roger Hagafors	(-June 1983)
	Else Pettersson	(-May 1982)
Risø National Laboratory	Jens Rasmussen	
	Ove M Pedersen	
Technical Research Centre of Finland (VTT)	Björn Wahlström	
	Lena Norros	
Aktiebolaget Asea-Atom	Kerstin Alm	
	Staffan Björe	
	Paul van Gemst	
Chalmers Institute of Technology	Eva Blinge	
Studsvik Energiteknik AB	Håkan Andersson	
	Per-Gunnar Sjölin	

* Chairman
** Project Leader

ABSTRACT

The present report is a summary of the NKA/LIT-1 project performed for the period 1981-1985. The report summarizes work on human error influence in test and calibration activities in nuclear power plants, reviews problems regarding optimization of test intervals, organization of test and maintenance activities, and the analysis of human error contribution to the overall risk in test and maintenance tasks.

Key words

Human Error - Test - Maintenance - Nuclear Power - Sweden - Finland - Denmark - Test Intervals - Databases - Calibration - Documentation - Probabilistic Risk Assessment - Risk Management - Search Strategies - Work Analysis - Incident Analysis - Diesel Generators

This report is part of the safety programme sponsored by NKA, the Nordic Liason Committee for Atomic Energy, 1981-85. The project has been financed by the Nordic Council of Ministers and the participating national institutions and regulatory bodies.

PREFACE

The safety of nuclear power, as for other complicated industrial processes, depends on an accurate and timely execution of tasks during the operation. There is, however, always the possibility that human errors either directly or indirectly initiate an unwanted course of events. The general aim is then to decrease the probability of human errors and to increase the probability of their detection. This is in principle made possible by a careful task design and by giving the human operator an appropriate training. This means in practice that one should consider the tools of the operator, the organization he is working in, and the training he is given. All these aspects have been addressed in the Nordic LIT-research programme over the period 1981 to 1985.

The Nordic LIT-research programme has concentrated on:

- human errors in test and maintenance (LIT-1)
- safety oriented organizations and human reliability (LIT-2)
- computer aided design of control rooms and plant automation (LIT-3.1)
- computer aided operation and experimental validation (LIT-3.2 and LIT-3.3)
- planning and evaluation of operator training (LIT-4)

These fields of research were selected from the experience of an earlier phase of the Nordic cooperation (cf. the reference Wahlström, Rasmussen, 1983).

The Nordic LIT-research programme involved a total effort of about 40 personyears of qualified researchers in Denmark, Finland, Norway and Sweden. The research programme has been financed partly by project funds from the Nordic Council of Ministers and partly by funds from the different participating organizations. The LIT-research programme was initiated by the Nordic Liaison Committee for Atomic Energy (NKA) as a part of the Nordic cooperation in the field of safety in the energy production field. The following organizations have been financing and have also been directly involved in the LIT-research programme:

Risø National Laboratory, Roskilde, Denmark

Technical Research Centre of Finland (VTT), Espoo, Finland

Institute for Energy Technology (IFE), Halden, Norway

Swedish Nuclear Power Inspectorate (SKI), Stockholm, Sweden

Swedish State Power Board, Vällingby, Sweden

The LIT programme is reported in the following final reports:

- The human component in the safety of complex Systems; LIT programme summary report, NKA/LIT(85)1
- Human errors in test and maintenance of nuclear power plants - Nordic Project work; LIT-1 final report, NKA/LIT(85)2
- Organizations for safety; LIT-2 final report, NKA/LIT(85)3
- The design process and the use of computerized tools in control room design; LIT-3.1 final report, NKA/LIT(85)4

- Computer Aided Operation of Complex Systems; LIT-3.2 & 3.3 final report, NKA/LIT(85)5

- Training in diagnostic skills for nuclear power plants; LIT-4 final report, NKA/LIT(85)6

Reference

Wahlström, B. and Rasmussen, J. (1983): Nordic Cooperation in the Field of Human Factors in Nuclear Power Plants. Conf. on Nuclear Power Experience, IAEA Vienna, 1983, IAEA-CN-42/247, pp 281-290.

Summary

The development and operation of advanced large scale energy production systems raise high demands for plant reliability, to ensure human safety and to protect the environment. In addition loss of production from plant failure can cause heavy economic penalties.

To reduce these risks, parallel and mutually independent (redundant) technical systems are used where malfunctions would be especially hazardous.

The protection offered by redundant systems can be threatened by so-called common cause failures, CCF, whereby a single class of fault may cause malfunctions in several redundant systems which may for instance contain components with similar weakness. A common error in test and maintenance procedures of several redundant systems could also affect the overall safety.

The NKA/LIT-1 project has focussed om human errors during test and maintenance of redundant safety systems in nuclear power plants. Such work is carried out at regular intervals, and the optimum time between tests can be calculated with a balance being struck between risks and costs. One factor is that the testing itself may increase the risk, both because the tested system will be inoperable during the test, and because the test itself may introduce errors. Models for the calculation of optimum test intervals therefore have to include assumptions on the way in which the tests are carried out.

In the project these assumptions were compared with actual experience of such tests in some nuclear power stations. This found that the assumptions in the models often do not correspond to actual test practice. The present models are then inadequate for a proper optimization of the frequency of tests. The project also identified a number of other factors to be taken into consideration.

To calculate test intervals information is needed on the expected frequency of malfunction of components. An existing database (the ATV database) contains data on detected malfunctions from Swedish nuclear stations and the TVO plants in Finland. Most of this data comes from the maintenance records at the plants, but more complete information is necessary before it can be used. For instance information on how the tests were performed and the ways in which malfunctions were detected is required; improvements in collecting this data are considered and informa-

tion on human errors that were committed in carrying out the tests should also be included.

Since human errors are liable to occur during maintenance activities, an analytical attempt was made to identify those parts of the process in which the risk for human error is highest. Reported errors in Nordic and American nuclear power plants were used to develop a search strategy for finding error-prone maintenance tasks. This search strategy was found to be useful both for evaluating existing procedures for test and calibration activities, and for designing new ones.

Using this method test procedures could be improved either by removing causes of human error, or by increasing their probability of detection at an later stage of the test procedure. In cases where modification of test procedures turns out to be impracticable the introduction of independent checking routines could be a solution. Such an approach would be part of the overall risk management concept of the entire plant, to be performed at the organizational level.

The use of the search strategy is rather laborious and time consuming. Its application should therefore be limited to activities of vital importance to safety. Safety analysis reports could be a basis for defining such vital activities. The general principles of the search strategy are, however, applicable to the evaluation of all kinds of test and maintenance activities.

As a part in a larger project on diesel generators, the LIT-1 project studied human errors in test and maintenance. An important result was that the origin of human errors can be found at three different levels: the organizational, the task, and the performance level. In the project it was demonstrated that many errors that appeared at the performance level could be attributed to human errors committed in course of the planning phase at the organizational level. Efficient systems for information exchange and feed-back of operation experiences could be valuable tools for the gradual elimination of such errors.

Although the LIT-1 project was directed to a study of nuclear power plants, the results have a wider application to all advanced technical systems with high demands for safe operation, or where economy is closely dependent on plant availability.

Sammanfattning

Utvecklandet och driften av avancerade energiproduktionssystem ställer stora krav på säkerheten av hänsyn till personal och omgivningen. Härtill kommer den ekonomiska risken vid oönskade stillestånd.

För att reducera riskerna har man infört olika typer av parallella men ömsesidigt oavhängiga (redundanta) system, framför allt på de ställen som har betydelse för säkerheten.

Ett hot mot att redundansen fungerar på avsett sätt är så kallade "fel med gemensam orsak" (common cause failure, CCF), dvs. att ett och samma fel inverkar på de olika redundanta kretsarna. Orsaken till CCF kan vara att tillverkningsbrister finns i likartade komponenter. En annan orsak kan vara mänskligt felhandlande i samband med service och underhåll.

Inom detta projekt NKA/LIT-1 har frågor rörande mänskligt felhandlande i samband med service och underhåll studerats.

Teoretiskt bör det vara möjligt att optimera tidsperioden mellan två tester. Vid bestämning av testintervallet måste man emellertid göra avvägning mellan säkerhet och kostnader. Genomförandet av testen innebär i sig en ökad risk genom att det testade systemet ofta blir otillgängligt under testet. Dessutom kan själva testet introducera fel i systemet.

För beräkning av testintervall används modeller och inom projektet studerades dessa modeller och jämfördes med det praktiska genomförandet av testerna. Det visar sig att de idag existerande modellerna inte alltid stämmer överens med det sätt som testerna i verkligheten utförs på. Därför är dessa modeller ofta otillräckliga som basis för optimering,men de faktorer som har betydelse och bör inkluderas har identifierats inom projektet.

För att bestämma testintervall behövs även erfarenhetsdata rörande komponentens förväntade feluppträdande. Den idag existerande feldatabasen för svenska kärnkraftverk och TVO-reaktorerna i Finland (ATV-databasen) innehåller uppgifter om upptäckta fel hos olika typer av komponenter, i regel hämtade från verkens underhållsdatabaser. Emellertid behövs ytterligare uppgifter för att databasen skall vara användbar för optimering av testintervaller, t.ex. använd testmetod och på vilket sätt fel upptäcks. I projektet redogörs för hur man i framtiden bör insamla erfarenhetsdata mer anpassade för denna målsättning. Denna insamling bör också omfatta uppgifter om de mänskliga fel som konstateras i samband med testerna.

Mänskliga fel förekommer givetvis även vid underhåll. Genom att analysera underhållsaktiviteten försöker man identifiera var i processen risken för felhandlande är störst. En analys av verkliga fel som uppkommit vid underhåll i nordiska och amerikanska kärnkraftverk har använts som underlag för en inom projektet utvecklad strategi för hur sådana felkällor skall sökas (sökstrategi). Denna strategi kan användas för existerande men också för uppläggning av nya test- och kalibreringsaktiviteter. Eliminering av vissa felkällor kan ske genom modifiering av testrutinen så att fel som ändå introduceras kommer att upptäckas genom att en efterföljande åtgärd avslöjar felet. Om en sådan omläggning av testrutinerna inte kan leda till detta resultat, kan man istället ta hand om möjliga uppkommande fel genom att införa ytterligare oavhängiga kontroller. Sådana åtgärder utgör då en del av hela anläggningens riskbegränsande administration (''risk management'').

Användning av den beskrivna sökstrategin fordrar relativt stora arbetsinsatser. Arbetet bör därför koncentreras till sådana aktiviteter som har vital betydelse för säkerheten. Som underlag för prioriteringar bör resultaten från genomförda säkerhetsanalyser kunna användas. Den allmänna kvalitativa grundfilosofin i sökstrategin kan dock utnyttjas för att analysera alla typer av test- och underhållsaktiviteter.

LIT-1 projektet var även involverat i ett större projekt, rörande dieselgeneratorer, för att studera mänskligt felhandlande i samband med service och underhåll. Vid genomförandet av undersökningen antogs att orsaken till mänskligt felhandlande kan sökas på tre olika nivåer: Organisationsnivå, Uppgiftsnivå samt Utförandenivå. Inom projektet konstaterades att många fel som manifesterar sig vid utförandet av underhållsverksamheter ursprungligen härrör från misstag gjorda i planeringsfasen på en annan nivå inom organisationen. System för informationsförmedling och erfarenhetsåterföring är värdefulla hjälpmedel för att stegvis eliminera sådana fel.

Även om den tekniska bakgrunden för LIT-1 projektet har varit kärnkraftverk så är det utförda arbetet användbart vid andra typer av avancerade tekniska system med säkerhetskrav eller där ekonomiska risker är av betydelse.

LIST OF CONTENTS

1 INTRODUCTION

Within the previous NKA project NKA/KRU (1977-80) (NKA/KRU-(81)11), human relability was identified as an important factor contributing to the overall level of risk in nuclear power operation. The domain of test and maintenance was found to be particularly vulnerable because the plant designers primarily had designed the safety system to cope with human errors in normal plant operation and not for human errors in the test and maintenance of the safety systems themselves. This was the reason to devote one NKA project, NKA/LIT-1, entirely to human reliability in the test and maintenance of nuclear power plants.

Within the NKA/LIT-1 project two topics have been studied by the participating organizations. These are

- the possibilities to optimize the length of test intervals on the basis of existing systems for collecting information about operation experience and present models for calculating optimal intervals

- the possibilities of coping with human errors:

  1. by developing and applying new search strategies for their pre-identification and elimination, to be applied during the design of a human task and in a pre-construction risk analysis

2. by controlling their effects when they occur in pracice, by risk management employing post-incident analysis as a means of feedback from operational experience.

2 ACTIVITIES

The focus of the first part of the project period was on developing principles for data collection and on preparing descriptions for subsequent use in the project. Studies in the later part was mainly aiming for test and analysis of principles for human error analysis and control.

The following studies have been performed and the results reported separately:

Actitivites providing common basic information on the performance of test and calibration:

- description of ten sample cases of human errors during test and calibration (NKA/LIT-1(83)406).

- description of the organization and performance of test and calibration activities in some nuclear power plants (NKA/LIT-1(82)404).

- a comparative analysis of the organisation and performance of test and calibration activities in boiling water reactors in Sweden and Finland (Wahlström B, 1983).

- an analysis of human errors during test and maintenance on dieselgenerators (NKA/LIT-1(83)212, Mankamo, T & Pulkinnen U, 1982).

Activities involved in test-interval optimization.

- a trial development of a database for the optimization of test intervals
- an assessment of the basis for the choice of test intervals in some nuclear power plants.

Activities involved in coping with human errors by predictive and retrospective analysis.

- preconditions were established for the treatment of human errors, particularly for the development of search strategies, and typical search strategies were proposed
- ten sample cases were studied in order to evaluate the preconditions and in order to get indications of the applicability of the search strategies proposed
- a trial application of one search strategy was performed
- guides for a search strategy and for post-incident analysis were written.

3 PRESENTATION OF RESULTS

3.1 Optimizing test intervals in nuclear power plants

3.1.1 Background

In nuclear power operation there are high demands on safety. For that reason the plants have a large number of standby safety systems which are not used in normal operation but should be ready to operate on demand in case of disturbancies or emergencies.

Because most of these systems are never used in normal operation their function have to be tested with regular intervals. Malfunctions in the standby systems can develop both as a function of time and be caused be human errors during preventive maintenance.

Frequency of testing

There is a number of drawbacks from the testing itself which makes it neccessary to optimize the test intervals against the achievements in terms of lower risks. The most obvious drawbacks are that

- some tests can not be carried out without a loss of production

- frequent testing requires more man-hours to be spent

The attitude towards these drawbacks has been to keep the risk as low as has been considered affordable. If there has been any sign of

decreased reliability in the system functions there has always been room for an increase in the frequency of testing. The question of the optimum test interval is however not only a matter of risks and costs. There are a number of other factors which indicate that test intervals may not be reduced at random:

- The standby safety systems sometimes become unavailable during the tests. Too frequent tests may for that reason lead to an increased level of risk.

- The tests could accidently be carried out on redundant systems and make them unavailable at the same time.

- The tests may cause damage on systems and components and in that way increase both risks and costs.

- The tests may introduce common mode failures in redundant safety systems.

- Unreliable tests may lead to unnecessary repairs which in turn increase both risks and costs.

- Some tests involve physical risks for the personnel.

- Frequent tests and subsequent repairs increase the possibility for introducing human errors.

Taken together all the factors mentioned above have made it reasonable to seriously reevaluate

the belief that frequent tests and shorter test intervals lead to a decrease in the total level of risk.

Principles for choosing test intervals

Test intervals are today determined by a combination of judgements from experienced people and simple reliability models. Recent studies and the accumulating experiences from present practice have led to the conclusion that the present practice will not automatically lead to optimum test intervals.

This situation has been the starting point for some LIT-1 studies. The objectives have been to assess the usefulness of present databasis for the faulty components, the validity of models for test interval optimization, and in addition to study the possibilities for improving present databases and to use more sophisticated models for optimizing test intervals.

3.1.2 Comparing assumptions and models with actual test practice

The most important requirements on models for calculating optimal test-intervals are that

1 the models are sufficiently sophisticated to incorporate all the important aspects that determine the relation between the length of the test interval and the total level of risk, and that

2 the fundamental assumptions comply with the reality that is modelled.

A study was therefore made where the presently used model and a few more sophisticated models were reviewed and evaluated in these respects (NKA/LIT-1(83)405).

In the study a classification of factors contributing to system unavailability was made. The following important factors were identified:

- the distribution of faults among components
- wear and tear on the components due to many cold starts
- faults on redundant systems due to a common cause
- faults caused by repair
- omission to reset isolated systems after repair
- systematic faults caused by human errors like
  a) using incorrect instructions
  b) using incorrect test standards
- the delay from the detection of a fault to the start of repair
- the duration of tests
- the rate of detection of actual faults during tests
- the range of error modes that is covered by the test methods

Three models were compared with the presently used method for optimizing test intervals: Vaurio´s model, Apostolakis´ model and the data code Frantic II. In the study the optimization of test intervals for residual heat cooling system, the emergency core (spray) cooling system and the containment cooling system were analyzed with the different methods and the assumptions were all compared to actual test practice.

The major conclusions from the study were

- For a given system different tests are used for testing different system functions. In the present practice sometimes only one kind of test is performed on each system and only one system function is therefore tested. This practice differs from the assumptions in all models which assume that all system functions are tested.

- It is not sufficient to use time for repair as a measure of unavailability such as assumed in the models. A more adequate measure would be the time from the detection of a fault to the completion of the repairs. The delay from the time when a fault is detected to the start of repairs should be known. Because there was a large variation in this delay the variation in unavailability was quite large too, which is inconcistent with the assumptions in the models.

- The models assume that the test is the only possibility to detect faults and that all faults are detected during the test. An analysis of fault reports show that only 20% of the faults in the studied systems were detected during scheduled tests (Mankamo, T & Pulkkinen U, 1982).

An overall conclusion seems to be that the assumptions made in models for optimizing test intervals have some severe inconsistencies with test practices and thus must be reconciled before valid calculations can be made.

A study (Mankamo T & Pulkinnen U, 1982) of the reliability of diesel generators in Finnish and Swedish nuclear power plants illustrates the problem of test-methods and the optimal test interval.

Simple start-up tests and full load tests were compared. It is shown that frequent start-up tests had negative effects because of the building up of soot in the engine. Full load tests with longer intervals were therefore preferable. Longer test intervals with no starts did however cause drying off of the oilfilm in the engine. The latter effect could however be compensated for by simply rotating the engine in shorter intervals.

The combination of a long test interval and a simple preventive maintenance action on a shorter interval was a way to optimize the availability of the system functions.

Thus a combination of test methods and preventive maintenance with the focus on system functions may eventually lead to a (more) optimal test practice, where the length of the test interval only is one aspect among many others to be considered.

3.1.3 Assessing the usefulness of the present data basis for the calculation of optimal test intervals

The ATV-system

The ATV-system is a centralized system for reporting faults in the nuclear power plants. The system is administrated by the Swedish Nuclear Power Inspectorate and all Swedish nuclear power plants as well as the TVO owned plants in Finland are reporting to the system.

For reported faults the following information is recorded in the database:

- nuclear power unit
- functional parts of the plant
- type of system
- time for detection
- time for start of repair
- time until the component is available again
- number of man hours used for the repair
- how the fault was detected
- type of function that was affected
- consequences of the fault
- type of fault
- actions taken as response to the fault cause

- description of the fault and actions taken

The reliability and completeness of the system have been assessed in two earlier studies. In 1980 coverage was between 60-80% and the reliability of the coding system was about 50% correct codings.

In the NKA/LIT project a comparison was made (NKA/LIT-1(83)405) between the reported faults for the main steam valves on the residual heat cooling system, the emergency core cooling (spray) system and the containment cooling system.

Data from the ATV-system were collected from the BWR-plants

- Ringhals 1
- Barsebäck 1 and 2
- Oskarshamn 1 and 2

Because of the similarity between the plants the effects of different test intervals could be studied for fairly comparable conditions.

The number of reports were 387 in all. The results showed some interesting but unfortunately not clear-cut results.

One result was that the coding of faults caused problems. Malfunctions in valves can for example be that the valve is leaking, that it is stuck open or stuck closed or that it can not be closed or opened completely.

This means that the definition of malfunctions and their effects on safe functioning was difficult. This result is important since it has significance for the use of ATV-data in reliability analysis.

Another important result was that only 20% of all faults were detected during tests. This was because the tests were made as valve manoeuvres and therefore only could lead to the detection of stuck valves. Leakages on the other hand were detected during tests performed during the revision period.

A third result was the great variation found in the duration of malfunctions, ranging from 2 days to 2 weeks even for faults hindering normal system function.

Unfortunately the ATV-database was not adequate for a comparative statistical analysis. Too many factors influencing the statistical results made it difficult to draw proper conclusions.

The results therefore supports the general conclusion that optimal test intervals hardly can be based on statistical analysis of data in the present ATV-system. An improved database must take into account the relationship between the test method and the system function tested, how the test practice effects the probability of detecting faults and how that in turn affects the duration of the unavailiability time.

3.1.4 Development of a data base optimization intervals

Because an adequate database is a neccessary condition for the calculation of optimal test intervals, an attempt was made to develop an improved classification system based on ATV-reports, incident reports and work permits (NKA/LIT-1(83)407).

In this study a form was developed where the following information could be found

- the test method
- the normal mode of operation (valves)
- the description of the fault
- the way the fault was detected
- the classification of the fault
- the number of tests required in the Technical Safety Requirements (STF)
- the number of activations initiated by trip conditions
- the total number of activations

An attempt was then made to analyze the reported data according the this scheme. The results from this posteriori analysis showed that it was difficult to make reliable posteriori analyses of reported faults.

An estimation of the test effectivness is for exampel dependent on how an internal leakage is coded in the test report.

A conclusion from the study was that systems and components should be treated separately. In addition it is necessary to consider

the demand for perfect functioning of the system, to which a faulty component belongs.

3.1.5 Recommendations

Although many of the studies mentioned were limited in scope and despite the limited statistical basis which was available some fairly well founded conclusions and recommendations can be made.

The first and perhaps most important is that the present practice for calculating optimal test intervals can be seriously questioned, mostly because the assumptions behind the models for calculating test intervals do not comply with actual test practices. Since the present Technical Safety Requirements (STF) is based on these assumptions it seems to be an issue of immediate concern.

The second conclusion is that the system for reported faults does not contain sufficient and reliable data for a valid reliability analysis.

It is recommended that a database is developed that treats components and systems differently so that the choice of test methods, and the definition of test effectivness are related to the demands on the system functions.

The third conclusion is that data on human errors are difficult to find in the present data basis. It is thus recommended that reported faults are checked by interviews of the test-personnel in order to reveal "hidden" human errors in the reports on technical malfunctions.

3.2 The organization of test and calibration

3.2.1 Background

Human errors take place not only in a technical but also in an organizational environment. Causes of human errors could therefore be attributed to an inadequate organisation of test and calibration activities, to characteristics of the maintenance personnel, or to the design of equipment.

For a better understanding of the overall context of test and calibration a study was made where a description of test and calibration activities were made and where possible organizational causes for human errors was discussed (NKA/LIT-1(82)404).

In the report it is pointed out that the most important organizational factors are:

- the organization of work
- the degree of training and motivation
- the quality of manuals and documentation
- routines
- the technical design
- feedback from previous tests

In the study test and calibration activities are analysed for two Swedish nuclear power plants with reference to these factors.

Periodic tests performed on safety related systems are regulated by the Technical Safety Requirements (STF). Normally the tests are made

on components only and not on entire systems. Before a test is carried out work permits are required. In order to make a test possible the component must be taken out of operation or be isolated during the test.

For some tests specific test equipment for measuring and calibrating are used. During the tests the results from the tests and the calibrations are noted, in protocols.

These protocols are checked afterwards by persons specially assigned for this task and the results are reported to the Nuclear Power Inspectorate. After a test is finished the component must be put back in to operation or put back to the stand-by state. The report shows that most test and calibration tasks follow this general scheme and that many different persons and responsible groups participate in the overall test and calibration activity.

Division of responsibility

One often neglected source of human errors is the structure of responsibilities for different parts of a test and calibration task. The study shows that the following kinds of responsibilities must be properly met.

- the responsibility that test and calibration are initiated and organized

- the responsibility for carrying out the task

- the responsibility for the technical systems (system and function)

- the responsibility for the components

- the responsibility for personnel safety e.g. radiation, chemistry

- the responsibility of a nuclear power unit or a part of a unit(e.g. Turbines)

- the responsibility for reporting to the Nuclear Power Inspectorate and/or other authorities

In the report examples are given of how the division of responsibilities is made for a few test and calibration tasks.

3.2.2 Test and calibration

Standards

Of vital importance for the test and calibration is the primary standards against which the portable calibration equipment is calibrated.

This is an important part of the test and calibration chain where human errors could cause common mode failures in the safety systems.

Missions

The test and calibration task comprises the following missions

1 Preparation
2 Coordination with the control room
3 Isolation of components and application of test equipment
4 Test and calibration
5 Removal of test equipment and resetting tested systems
6 Reporting the results

In the study it is discussed where human errors could affect the different stages in this sequence.

3.2.3 Documentation

Every permanently installed measuring channel has an individual record. This system of individual records is used irrespectivly of which unit in the organization has the responsibility.

This record keeps all information of relevance for a particular measuring chain and for components that are part of that chain.

The records follow the individual components even when they are repaired or put back in some other part of the plant.

3.2.4 A comparison of the test and calibration practices in Swedish and Finnish nuclear power plants

The recognition of the importance of organizational aspects of test and calibration activities was the basis for a comparative study of current practice in Sweden and Finland.

The results show more similarities than differences. This is explained by the close cooperation between the particular Finnish utility and Swedish utilities.

The role of the safety authorities seems to be some what different in Finland and in Sweden. In Sweden the responsibility for test and calibration is delegated to the utility and regulated by the Technical Safety Requirements. The authority then checks that this responsibility is properly met by the utility.

In Finland the authority exercises a more direct supervision and personnel from the Finnish Centre for Radiation and Nuclear Safety is often present during test and calibration.

3.2.5 Recommendations

From the studies of the organization of test and calibration practices it is possible to make the following recommendations with a certain degree of confidence.

Since human errors can not be avoided altogether it is recommended that a higher degree of redundacy is built in to the test and calibration procedure. This means in particular that the practice for calibration of standards and the dubbelchecking of the corresponding test protocols should be verified so that human errors would not pass undetected.

The use of manuals and instructions should also be encouraged. At present many tasks are performed with no instructions at all.

It is thus necessary to improve the present instructions. Care must then be taken to use a level of detail which is relevant for the particular tasks.

3.3 The coverage of human errors by Probabilistic Risk Assessment PRA and Risk Management (RM)

3.3.1 An integrated concept of PRA and RM

Two principal methods exist for the control of human as well as other kinds of risk contributions:

1. their pre-identification and elimination, as far as possible, during the design of a human task and in a pre-construction risk analysis

2. to reduce their probability improve or counteract them when they occur in practice.

Obviously, the two principles should be brought to support and supplement each other, resulting, particularly for a nuclear power plant, in the following approach:

The information provided by performing a Probabilistic Risk Assessment (PRA) or an As-operated Safety Analysis Report (ASAR) should be used as reference for a closed-loop risk control or Risk Management (RM) utilizing post-incident analysis as means of feedback of operational experience, see figure 1.

This in theory provides a way of securing completeness of a total risk control. The underlying

assumption, however, is that accidents not covered by the risk analysis are due to the coincidence of several sub-events each of which can be identified and controlled individually by means of post-incident analysis. This assumption which must be studied carefully appeąrs to be realistic owing to the "defense in depth" plant design philosophy.

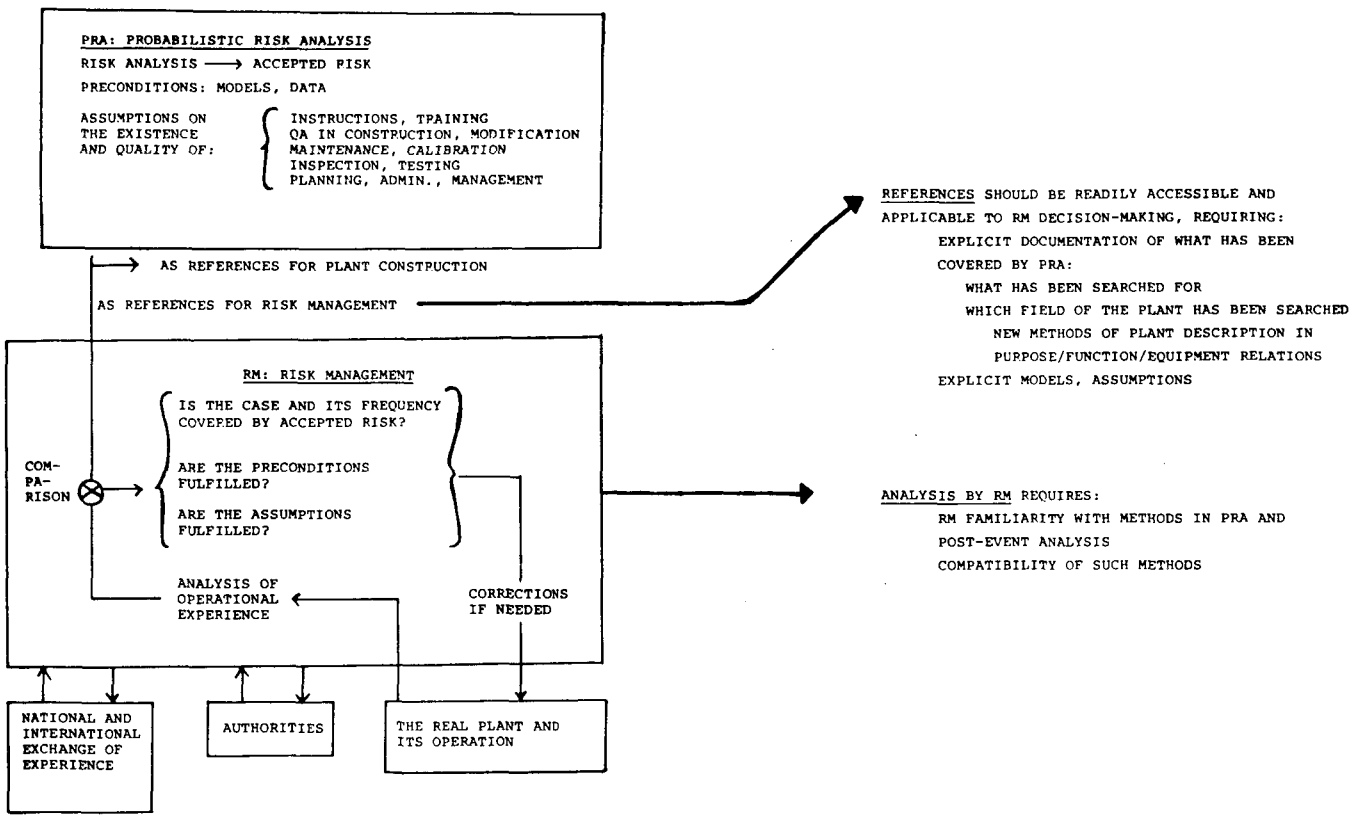


Figure 1 The information provided by performing a probabilistic risk assessment should be used as reference for a closed-loop risk control or risk management utilizing post-incident analysis as means of feedback of operational experience.

The above approach and its consequences particularly for the PRA and its search strategies are discussed and analysed in (NKA/LIT-1(82)101). Important consequences for the PRA documentation and for the post-incident analysis are indicated in Figure 1 and will be discussed subsequently.

3.3.2 Formalized search strategies

The use of the PRA, including its preconditions, as a reference for RM, requires explicit and user-oriented documentation of the PRA, including preconditions, models and data sources. A particular part of this formalization is documentation of the coverage of the analysis and search methods, i.e., what has been searched for and which fields of the plant have been searched must be known in order to evaluate operational experience as a basis for RM decisions in the feedback control. A well documented model and description of the risk identification strategies of the PRA are necessary to decide whether or not an individual occurrence falls within the accepted risk and, thereby, it will be possible to identify oversights or operational problems which call for special precautions. In this respect, documentation of what has been covered is considered more important than attempts to reach high theoretical degrees of completeness that will depend upon the individual creativity of an analyst and, therefore, will be susceptible to problems with undefined boundaries.

For the identification of human risk contributions and its integration into a total plant PRA, the following procedure is assumed:

First a basic PRA is performed of the plant technical systems. In this analysis are included only those human activities which are formalized in written work instructions and consequently are considered analyzable by formal analysis.

Next, as an augmentation of the basic PRA, an analysis is performed in order to identify the possible modifications of the content of the basic PRA owing to errors during human activities in general. This analysis includes less structured activities, and with the possibility of affecting event propagation in the following ways:

- by significantly increasing the frequency of event chains
- by altering the propagation structure
- by introducing causal couplings between otherwise independent events.

The above analyses are assumed to provide explicit documentation of the search strategies and of the fields of search so as to form the reference for a systematic risk management through feedback from event report analysis.

A detailed discussion of this above proposed formalized procedure including its possibilities

of covering different types of human errors is presented in (NKA/LIT-1(82)101) where also proposals are made for different types of search strategies for identifying human risk contributions. One strategy: Work Analysis, for well-structured formalized activities, is described subsequently.

3.3.3 Work Analysis: A method for well-structured human activities

Work Analysis is developed for well-defined activities, e.g. test and calibration, and is a formalized procedure for the pre-identification of relevant human errors leading to a lack of task result and/or to immediate effects not covered by the lack of task result itself. The method makes possible a systematic documentation of analysis results such as the risk-related intentions of reasons for the task design and/or its modifications. Quantification of results can be attempted if needed and if meaningful data can be provided.

In the following the four main phases of WA will be expounded, a detailed procedure is given in (NKA/LIT-1(84)106).

a) Analysis of Task Sequence is made in order to provide a description of the task as a basis for subsequent error analysis. For the sake of realistic coverage, acceptable alternative acts such as short-cuts and "tricks of the trade" should be identified for inclusion into the subsequent analysis, and accordingly non-acceptable acts should at this stage be eliminated by design or precautions against them should be stated.

b) Analysis of Task Reliability is concerned only with the identification of error possibilities affecting the task result. Criteria for the task result to be acceptable should carefully be defined and error recovery possibilities should be identified.

For acts not covered by recovery and for acts in relevant recovery activities, "error modes" are postulated and evaluated for their significance. The error modes can be in terms of external acts only or by also including postulated psychological error mechansisms of the kinds given in the description system for human malfunctions shown in figure 2.

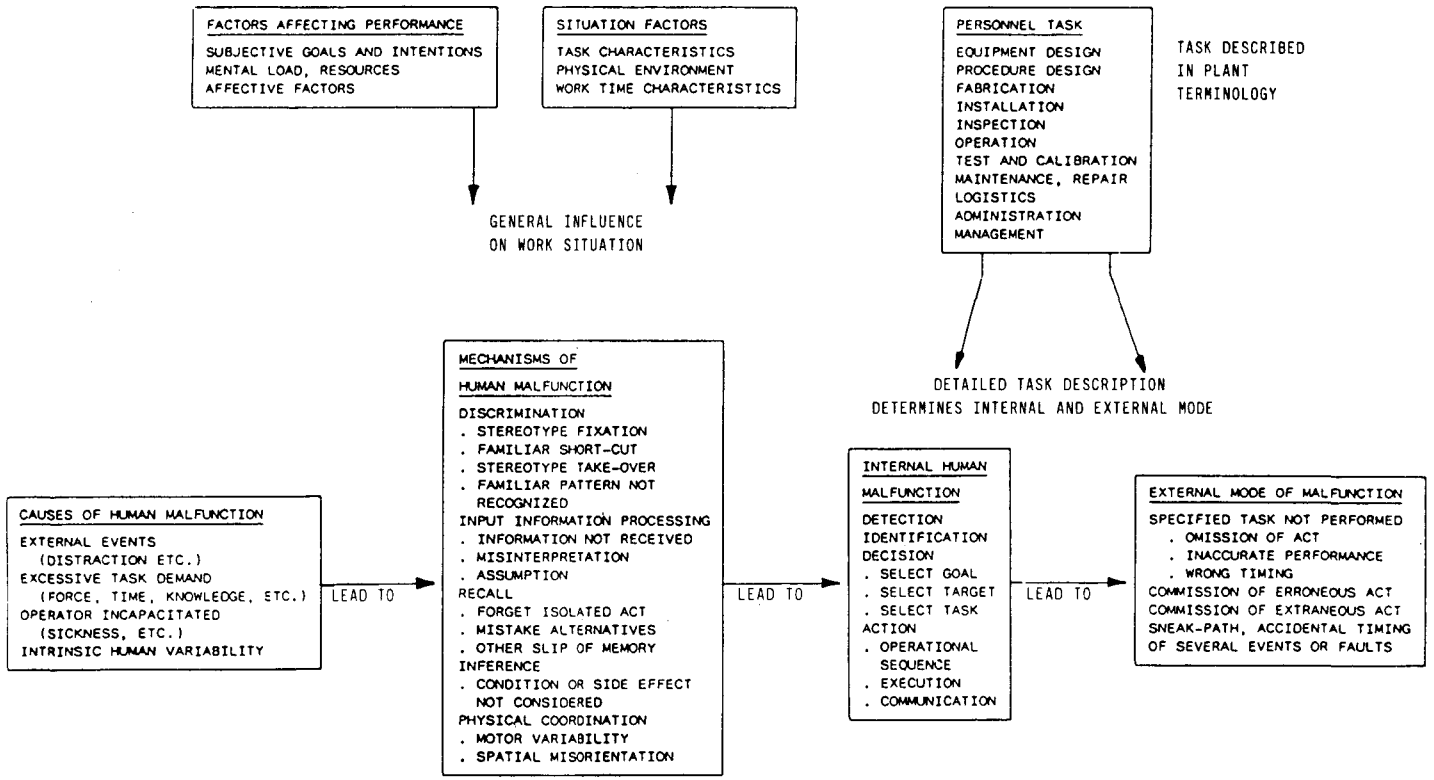


Figure 2 Description system for human malfunctions

The descriptiors in the four boxes in the bottom of the figure enable the analyst

- to have the chain of descriptors connected with a conventional task description given in equipment-oriented terms

- to postulate a causally ordered chain of descriptors connecting an external cause of the human malfunction with an external manifestation of the effect of the malfunction through two human-oriented descriptors of a general, not task-specific kind, and based upon such chains, to generate relevant scenaria.

c) Analysis of Immediate Effects is a search for error effects not related to the lack of task result e.g. an effect in a different system owing to mistaking a valve for a different valve belonging to a different system. First, systems or functions are identified which can be affected by errors in the task under analysis by applying search criteria such as closeness or similarity. Error modes and possibly related mechanisms are postulated for each act of the task and error effects found are analyzed for recovery and for risk significance.

d) Analysis of Task Disturbances, such as lack of tools or spare parts, aims at identifying risky consequences of improvized activities e.g. in order to accomplish the task in spite of the disturbance. Disturbance sources are selected and applied to acts without recovery and to relevant recovery acts and the analyst looks for probable alternatives or improvizations.

3.3.4 Preliminary evaluation of coverage afforded by PRA, RM and WA

In order to get a preliminary indication of the applicability of the concepts, including Work Analysis, presented in the previous subsections, cases from nuclear power plants were studied: 10 cases related to test and calibration (T&C) in Swedish plants and described in detail (NKA/LIT-1(83)406), 70 cases from American Licensee Event Reports representing a wider spectrum of task types and, therefore, expected to contribute supplementary information.

The study aimed at the following:

a) To get an indication of which typical human errors could be expected to be covered by established PRA methods and which could not and, consequently, should be controlled by RM.

b) To get an indication of the applicability of two typical search strategies: Work Analysis (WA), seeking for significant human error effects, internal or external to the task, and Risk Analysis, which is typically applied in a PRA when seeking for significant causes of critical events, in our case particularly human causes.

The study was reported in (NKA/LIT-1(84)104) and a summary presented in (NKA/LIT-1(84)107).

For the 10 Swedish cases the main results are summarized in the following. It should be noticed that the number of cases is too small for rendering any statistical evidence and any qualitative indication is valid only for the particular cases analysed.

A significant number of errors and deficiencies was found in activities not directly related to the actual T&C such as planning and administrative activities: These are not analyzable by present predictive methods, but are, covered in a pre-construction PRA by assumption, not by explicit analysis. Therefore they are available, for application of RM control and post-incident analyses. A proposal (NKA/LIT-1(83)102) was made for studying the structure and contents of such less-structured activities.

For activities directly related to T&C it was found that they were or could be well-structured and, consequently, could be subject to WA, leading to the coverage of most of the simple error effects including "immediate effects", these being the dominating type of effect, although they were not covered by conventional predictive methods.

The analysis of the Swedish cases also served for a useful trial application of the kind of analysis needed in RM. It also demonstrated how the analysis of even simple cases with low potential risk can identify factors that could be important ingredients in complex situations with higher risk potential.

The results for the American cases did not provide significant contributions.

Conclusions

An integrated use of Probabilistic Risk Assessment and Risk Management could contribute to improved coverage of risk.

Well documented search strategies are a necessary requirements in RM in order to make a systematic use of event reports possible.

For the cases analyzed a significant number of errors and deficiencies were found in planning and administrative activities that is tasks which cannot be covered by PRA and, therefore, have to be covered by RM. Most T&C activities are or could be made well-structured and consequently could be subject to Work Analysis: If this is done the results were judged to render a promising predictive coverage.

For the cases analyzed it was felt that a systematic post-incident analysis of human errors would to be very useful in RM activities.

3.3.5 Trial application of Work Analysis

In order to get a more realistic evaluation of WA in predictive analysis the method was applied to an actual T&C activity. This trial application is reported in detail in (NKA/LIT-(84)408) and summarized in the following.

The objectives of the assessment were:

- To demonstrate the method by analysing a selected test and calibration task.

- If possible, to identify classes of human errors which cannot be identified with the aid of the actual method.

- To express opinions on the usefulness of the method as a tool for risk analysis in nuclear power plants.

The application and assessment of the search strategy was, limited to cover only the main execution part of the selected task.

Bases for analysis:

The activity selected for analysis was test and calibration of differential pressure cells for measuring the water level in the pressure vessel of a nuclear power plant. A written instruction described the main parts of the work procedure. The detailed manual actions, however, were performed by the maintenance technicians. They were reconstructed by the analyst based on interviews and observations of the actual task execution. For the resulting task description a computer-oriented language was adopted.

The WA procedure, including the use of error mechanism descriptors, was applied as reported in (NKA/LIT-1(84)408) and summarized in subsection 3.3.3

Result and conclusions:

The general impression from the analysis of the selected activity is that the procedure was well established and thoroughly worked out. The analysis indicated, however, that a large effort may have to be spent on the reconstruction of

procedures that are not well-documented in written instructions.

The Work Analysis search strategy as far as it has been tested works well. However, the manual effort for performing the analysis is quite large, even for a rather small task.

Therefore, in order to keep the volume of the analysis effort within reasonable bounds, the analysis had to be restricted to the most urgent tasks, i.e. those which were judged to contribute the highest risk.

If information can be provided, it is in principle possible to perform a more detailed analysis for every step or subsequence in the task in order to identify possible mechanisms and causes of the human malfunction. However, this must be done selectively, otherwise the effort will be gargantuan.

Accordingly, it is felt that the search strategy should be limited to support the identification of primary errors. In principle it would be possible to expand the prediction of human errors also of secondary faults. As mentioned above this type of expansion, when applied generally, would involve large amounts of work.

In the general case a recovery point in a procedure for the detection and correction of errors, is related to one or a few error modes. This implies that even if there are "smaller" recovery points within a "recovery loop", there is a possibility for an error of a certain mode to pass unnoticed through a set of recovery points.

These error modes must therefore be identified and the consequences should be considered in the risk analysis.

Recommendations:

It may be adviceable, once a written guide for the use of the strategy is available, to perform a systematic analysis of the existing procedures for test and calibration of measurement and alarm channels which are parts of the protective systems. With regard to the required effort the analysis should start with those procedures that contribute the highest risk.

Since work procedures, particularly those which are not documented, sometimes have a tendency to change as time goes by, the survey of the procedures should be performed periodically.

Obviously, the strategy is not limited to procedures related to protective systems but can also be applied to other procedures which may be interesting in relation to availability or because of economic reasons.

The strategy can also be used as a tool when designing work procedures. Particular isolated acts can be identified and entered into some sort of recovery loop for reduction of the risk contribution.

3.3.6 Guides for the application of Work Analysis and post-incident analysis

The accumulated experience and results from the previous project phases were collected in a single report (NKA/LIT-1(84)106) for the purpose of serving practical application.

The report should be considered a guide for the treating of human errors: for identifying possibilities of occurrence when designing well-structured human tasks and for improving the situation when the tasks are performed in reality.

For these purposes a strong coupling between predictive and retrospective analysis is emphasized: In order to control human errors, post-incident analysis of cases with human errors in a given industrial plant should be performed as means of feedback from reality in order to get verification of the results of predictive analysis and also as a general means of identifying and improving such human errors which cannot be expected covered by predictive analysis.

Primarily, the report addresses people with a knowledge of the technical plant in question and involved in the safety-oriented design and improvement of human activities and without a particular human factors background.

The report describes the procedures for post-incident analysis and for Work Analysis, these being based on a common description system for human malfunctions. This system is explained and so are its underlying models and way of reasoning.

Also a word index is provided for supporting the reader.

Conclusions

For the purpose of promoting immediate practical application guides were written for the predic-

tive and also retrospective analysis of human risk contributions.

3.3.7 Summary of conclusions and recommendations

Summary conclusions:

The information provided by performing a Probabilistic Risk Assessment (PRA) or an As-operated Safety Analysis Report (ASAR) is assumed to be used as reference for a closed-loop risk control or Risk Management (RM) utilizing post-incident analysis as means of feedback of operational experience.

Based on this concept a search strategy: Work Analysis was proposed, developed, tested and described in a guide. Work Analysis was developed for well-defined activities, e.g. test and calibration. It is a formalized procedure for the pre-identification of relevant human errors that would lead to a lack of task result and/or to immediate effects not covered by the lack of task result itself. The method makes possible a systematic documentation of analysis results including the risk-related intentions of/reasons for the task design and/or its modifications.

Also in the guide is described a post-incident analysis procedure which will provide a systematic description and documentation of incidents involving human malfunctions, also in activities not covered by PRA and, therefore, to be controlled by RM. Thus, the post-incident analysis makes possible the systematic feedback for monitoring the quality of task performance.

WA and the post-incident analysis procedure are based on a common description system which enables the analyst

- in post-incident analysis to identify a causally ordered chain of descriptors connecting an external cause of the human malfunction with an external manifestation of the effect of the malfunction through two human-oriented descriptors of a general, not task specific, kind

- in predictive analysis to postulate relevant causally-ordered chains of the same kind as above and to generate relevant scenaria.

- to connect the chain of descriptors with a conventional task description given in equipment-oriented terms.

Recommendations:

As a means of improving completeness in plant risk control, post-incident analysis of human error cases should be applied consistently. In a long-time perspective, this could provide a systematic collection and classification of information on human performance including data for improving the quantitative assessment of human risk contributions.

In order to facilitate (RM) decisions where to apply RM to cover the risks of real occurences, PRAs and ASARs should provide explicit documentation of what has been covered by predictive analysis and what is assumed to be covered by RM.

Possibilities of human errors should be counteracted by methods like Work Analysis already during the design of such activities which, have a sufficiently well-defined structure, to permit the use of such methods.

Recommended future R&D

For WA:

Investigation of the possibilities of interactive computer aided support for the analyst. Development of more detailed and precise criteria for guiding the decision as to whether a given task design is accessible to formal analysis.

For less-structured activities:

Development of search strategies for the identification of such human interferences which can affect the content of a PRA and are not covered by WA.

Investigation of whether certain less-structured maintenance activities could, advantageously, be well-structured, i.e., the balancing of, on the one hand, higher degree of formalization leading to predictability and, on the other hand, the negative effects of such formalization.

Study of the contents and structure of administrative and planning activities in order to arrive at possible criteria for a reduced risk of such activities.

3.4 A case study of human errors influence on diesel generator failures

3.4.1 Background

The diesel generator (DG) study (Mankamo, T & Pulkkinen, U, 1982), where the authors found a high proportion of the critical failures to be affected by human errors, was the starting point for a specific study of human errors, in a case study of human errors at the Loviisa nuclear power plant in Finland (NKA/LIT-1(83)212). In the diesel generator study it was noted that the practice was to increase test frequency as a respons to an increased failure frequency. Increased test frequency did cause extra wear and tear on the components and had adverse effects on the motivation of the personnel. Since the additional test also increased opportunities for human errors it became evident that it was necessary to study failure mechanisms and possibilities to decrease the rate of testing. Therefore in this NKA/LIT study a qualitative analysis of human errors in test and maintenance of diesel generators was presented.

The methodological approach contained:

- an analysis of the test and maintenance activities
- descriptive analysis of error data
- a theoretical analysis of the particular test and maintenance case in the Loviisa nuclear power plant.

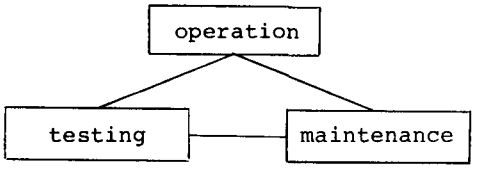
3.4.2 Problems at different analytical levels

In the study it was assumed that human errors can be found at different analytical levels.

a the organisational level
b the task level
c the activity level

In order to assess root causes for human errors it is necessary to consider all three levels.

At the organizational level the reliability of the system depends on the ease of the communication between the three functional units:



The problem is that errors often cannot be detected at the place of their origin. The communication between the three functions contain typically conditions that offer "blind spots" between the functions. To understand some of the possible human errors in test and maintenance it is necessary to start the analysis with the allocation of functions and check how this will affect the contents of particular test and maintenance tasks.

At the task level feedback is important and should be considered in relation to the task structure. If a task is defined by its goal it is possible to distinguish between primary and secondary sub-tasks at the task level.

Primary sub-tasks are directly related and controlled by the goal of the task and for that reason often also included in the work manuals. Secondary sub-tasks are necessary for a correct completion of the task but are not directly related to the task goal. Omissions and errors in secondary sub-tasks are thus not controlled by feedback at the task level. Secondary sub-tasks are sometimes also referred to as "functionally unrelated acts" and represent a high proportion of human errors in maintenance tasks (LER reports).

At the activity control level the focus is on the performance of sub-tasks which of course also are subject to errors. At this level the analysis should focus on "clumsiness" errors and mistakes in the activity regulation which are not due to the lack of goal related feed back control.

In the study the usefulness of a multilevel approach for human error analysis was demonstrated and some important suggestions for further studies were given.

3.4.3 Summary of result from the analysis

3.4.3.1 Method

The results in the diesel generator study (Mankamo, T & Pulkkinen, U, 1982) based on 40 diesel generators in Sweden and Finland have shown that 26% of critical failures

could be attributed to human errors in testing and maintenance. These human error data were further analysed in the present study.

A classification of errors was made where the errors were divided in the categories:

- faulty auxiliary activities
- carelessness
- faulty handling in testing
- faulty handling in calibration
- omissions of maintenance steps

An analysis of the consequences of the critical testing and maintenance errors was also carried out.

For the test and maintenance activities at the Loviisa nuclear power plant separate descriptions were prepared for the organizational level, the task level and for the activity level. Possible failure mechanisms for different levels were then studied.

3.4.3.2 Results

The results of the error analysis are shown in Table 1.

Table 1. Classification of errors in testing and maintenance by the type of inadequacy.

	Critical failures	Non-critical failures	All failures
Faulty auxiliary activites	1		1
Carelessness	4	8	12
Faulty handling in maintenance	4	10	14
Faulty handling in testing	4	2	6
Faulty handling in calibration	3	15	18
Omissions of maintenance steps	1	2	2
Total	17	37	54

The case study provided qualitative data and the findings were discussed separately for the assessment of the status of the dieselgenerators and performance of test procedure.

A Assessment of the status

The importance of the assessment task was clearly demonstrated. The essential task was not primarily to carry out the test procedure but to collect the information that was needed to evaluate the status of the diesel engine.

This conclusion is supported by some informal organizational changes that had occured at the nuclear power plant.

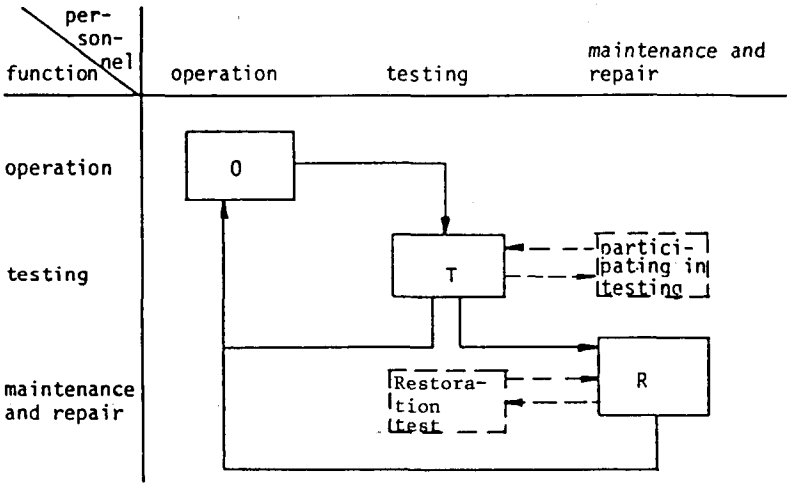


Figure 3. Illustration of the interactions between the functions and personnel involved in ensuring DG availability.

In fact an inofficial participation by maintenance personnel took place during the testing of the diesel generators, see Figure 3. This indicates that maintenance people want more information from the tests than a simple pass-fail statement. The test was seen as a diagnostic method rather than an end result. A diagnostic attitude towards the tests had developed based on the recognition that even a series of successful tests could step by step bring the diesel generator closer to a failure. Se figure 4. For the same reasons also "diesel diaries" were kept.

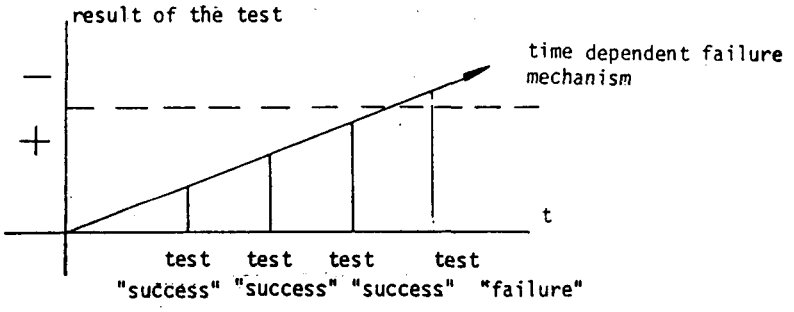


Figure 4. An illustration of the diagnostic orientation towards testing.

The classification of errors also supports the conclusion that a major part of failures have a latent and cumulative character. The category "carelessness" refers to a lack of interest in detecting symptoms that indicate a degraded status of the diesel engine.

B Performance ot the test procedure

Seeing the test as an information collecting activity makes the following mistakes possible:

1 Overlookings of necessary and adequate information

2 Failure to notice (e.q. in case of weak symptoms)

3 Incorrect conclusions from available (correct and effective) information

In the study it was argued that an increased orientation toward status assessment in the training and an improved test checklist would be the way to overcome these kinds of mistakes.

3.4.4 Recommendations

The study demonstrated the need for information of a qualitative character to support the conventional statistical error analysis. It is therefore recommended that error analysis includes information about

1 functional organisation of test and maintenance activities

2 subjective descriptions of test and maintenance tasks by the test personal

3 features about the tasks that affect the possibilities to have feedback control of task performance

A qualitative case analysis should be performed in human error analysis studies because better understanding of failure mechanisms becomes possible that way.

The value of a qualitative analysis is however entirely dependent on a firm and consistent theoretical framework. More theoretical oriented studies should therefore be done to increase the explanatory power of data from future case studies.

4 GENERAL SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

Although many of the studies carried out in the present NKA/LIT-1 projects have been limited in scope some fairly wellfounded conclusions and recommendations can be made.

Regarding the optimization of test intervals the first and perhaps most important result is that the present practice for calculating optimal test intervals can be seriously questioned. The reason is that the assumptions behind the models for the calculations do not comply with the actual test practice.

Since the present Technical Safety Requirements (STF) for nuclear power plants are based on these calculations it is recommended that the implications for the validity of the present Technical Safety Requirements are looked upon in more detail.

The second result is that the present database for reported faults does not contain sufficient data for a reliability analysis. It is recommended that the database is improved in two principal ways:

The first is to treat systems and components separately so that test methods and test effectiveness can be related to the demands on the system functions. The second is to separate human errors from technical malfunctions. In order to achieve this it is recommended that the reported faults are checked by interviewing the test personnel for human errors "hidden" in the reports on technical malfunctions.

The way in which test and calibration activities are organized is one important risk factor that was identified in the NKA/LIT-1 projects. The probability of human errors being detected was shown to be a function of how the test and calibration activities were organized. Since *human errors can not be avoided altogether* it is recommended that a higher degree of redundancy is built into the test and calibration procedures.

The studies also show that the use of manuals should be encouraged. In order to achieve this present instructions often need improvement. Presently, in many cases instructions are either missing or are irrelevant for the particular tasks.

Another important result from the LIT-1 projects was a demonstration of how data from Probability Risk Assessment (PRA) or As-operated Safety Analysis Reports (ASAR) can be used as reference for a closed-loop risk control or Risk Management (RM) activity by using post-incident analysis as means of getting feedback from the operational experience. For well-structured activities a method; "Work-Analysis", was demonstrated as a possible way of improve present PRAs in handling the influence of human errors. These experiences have been summarized in a guide. It is recommended that a comprehensive conceptual framework for risk analysis and risk management is adopted if a high degree completness in plant risk control shall be achieved. A common description system is necessary in order to apply human error analysis techniques consistently. PRAs and ASARs should aim at an explicit documentation of

what has been covered by the predictive analysis and what is left for Risk Management activities to take care of. It is finally recommended that the assumptions underlying the PRAs should be documented in a way that makes it possible to relate post-incident analysis results to these assumptions.

The need for information of a qualitative character to support the conventional statistical error analysis was demonstrated in a case study of human errors in the test and maintenance of diesel generators. It is recommended that error analysis should include information about (NKA/LIT-1(82)101) the functional organization of test and maintenance activities by the test personnel and (NKA/LIT-1(83)102) features about the tasks that affect the possibilities to have feedback control of task performance. A qualitative analysis is felt to give a better understanding of the failure mechanisms.

Since the value of a qualitative analysis is dependent on a consistent theoretical framework future studies should be given a theoretical emphasis in order to increase the explanatory power of data from studies of human errors in maintenance tasks.

5 REFERENCES

These are main reports from the LIT-1 project, which in turn contain broader references to international reports.

NKA/KRU(81)11: NKA/KRU Project on Operator Training, Control Room Design and Human Reliability. Summary Report.

Denmark

NKA/LIT-1(82)101: Rasmussen, J and Pedersen, O M. Formalized Search Strategies For Human Risk Contributions: A Framework for Further Development. Juli 1982. (RISØ-M-2351).

NKA/LIT-1(83)102: Pedersen, O M. Risø. Studiet Af Planlaegningsfaser Før Test Og Kalibrering. Oplaeg.

NKA/LIT-1(84)104: Pedersen, O M. Risø. Interim rapport LIT-1: 10 Haendelser Med Menneskelige Fejl I Test Og Kalibrering. Analyse Af Haendelsebeskrivelser Og Vurdering Af Daekning Af Fejl Via Søgestrategier Og Risk Management.

NKA/LIT-1(84)106: Pedersen, O.M. Risø. Human Risk Contributions In Process Industry: Guides For Their Pre-identification In Well-structured Activities And For Post-incident Analysis.

NKA/LIT-1(84)107: Pedersen, O.M. Risø. Human Errors In Test And Calibration: Analysis Of Event Descriptions For The Evaluation Of Coverage And Applicability Of Search Strategies And Risk Management. Summary report.

Finland

NKA/LIT-1(83)212: Leena Norros, Björn Wahlström VTT. Human Errors In Ensuring The Operability Of Standby Systems. VTT Research Notes 461, May 1985.

NKA/LIT-1(83)215: Wahlström, B, VTT. Några synpunkter på testintervallets längd. Internal Project Memorandum.

Mankamo, T & Pulkkinen, U: Reliability Of Diesel Generators In The Finnish And Swedish Nuclear Power Plants. Technical Research Centre of Finland, Research Report. 1982.

Wahlström, B. VTT. Anteckningar från besök på TVO den 1983-04-22. Utkast. Internal Project Memorandum.

Sweden

NKA/LIT-1(83)405: Blinge, E. Chalmers Tekniska Högskola. Val av testintervall för tre olika kylsystem hos svenska kokarreaktorer - Granskning av bedömningsgrunden.

NKA/LIT-1(83)406: Alm, K. ASEA-ATOM. Mänskliga fel vid test och kalibrering.

NKA/LIT-1(83)407: Staffan Björe, ASEA-ATOM. Framtagning av databas för testintervallsoptimering.

NKA/LIT-1(84)408: Sjölin, P-G, Studsvik Energiteknik AB. Assessment Of A Search Strategy For Human Risk Contribution In Test And Calibration Work In Nuclear Power Plants. Studsvik Technical Report NR-85/26.

NKA/LIT-1(84)409: Andersson, H. Studsvik Energiteknik AB. Human Reliability in Complicated Energy Production. Paper presented at the NKA/LIT-1 Seminar On Human Reliability In Complicated Energy Production In Stavanger, March 13-14, 1984.

NKA/LIT-1(82)404: Van Gemst, P, ASEA-ATOM. Mänskliga fel vid test och kalibrering.

Blinge, E. Chalmers Tekniska Högskola. Sammanställning av ventilfel i tre av kylsystemen hos Ringhals 1, Oskarshamn 1 och 2 samt Barsebäck 1 och 2. CTH-rapport A 83-123.

6 PARTICIPATING ORGANISATIONS

The following organisations have been instrumental in carrying out research tasks and preparing the NKA/LIT-I reports:

Denmark
Risø National Laboratory (Risø)
P.O. Box 49
DK-4000 Roskilde, Denmark

Finland
Technical Research Centre of Finland (VTT)
Bergmansvägen 5
SD-02150 ESPO 15, Finland

Sweden
Chalmers Institute of Technology (Chalmers)
S-412 96 Gothenburg, Sweden

Studsvik Energiteknik AB (Studsvik)
S-611 82 Nyköping

ASEA-ATOM
Box 53
S-721 04 Västerås

Swedish Nuclear Power Inspectorate (SKI)
Box 27106
S-102 52 STOCKHOLM

Individual reports can be requested from the organisation of origin. The VTT reports can be obtained by mail order from:

Government Printing Centre
Marketing Department
P.O. Box 516
SF-00101 Helsinki FINLAND

Norstedts Tryckeri, Stockholm 1985

LIT final reports:

LIT(85)1	The human component in the safety of complex systems.
LIT(85)2	Human errors in test and maintenance of nuclear power plants - Nordic project work.
LIT(85)3	Organization for safety.
LIT(85)4	The design process and the use of computerized tools in control room design.
LIT(85)5	Computer aided operation of complex systems.
LIT(85)6	Training in diagnostic skills for nuclear power plants.

These reports are available at the following organizations:

Technical Research Center of Finland, VTT/INF Vuorimiehentie 5 SF-02150 Espoo 15	LIT(85)1 & 4
Studsvik Energiteknik AB S-611 82 Nyköping	LIT(85)2
Statens Vattenfallsverk Fack S-162 87 Vällingby	LIT(85)3
Risø National Laboratory Postbox 49 DK-4000 Roskilde	LIT(85)5 & 6

Handling charge USD 10,- per report to be forwarded with order.