STUK

STUK-YTO-TR 160 December 1999

Evaluation of incident analysis practices in the Finnish nuclear power industry

Jari Kettunen, Kari Laakso
VTT Automation

In STUK this study was supervised by **Pentti Rannila**

STUK • SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

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

ISBN 951-712-352-2
ISSN 0785-9325

Oy Edita Ab, Helsinki 1999

KETTUNEN Jari, LAAKSO Kari (VTT Automation). Evaluation of incident analysis practices in the Finnish nuclear power industry. STUK-YTO-TR 160. Helsinki 1999. 89 pp. + Appendices 12 pp.

ISBN 951-712-352-2
ISSN 0785-9325

Keywords: cause, corrective action, direct cause, event, event investigation, operational experience feedback, root cause, root cause analysis

ABSTRACT

This report provides an analysis and evaluation of incident analysis methods and practices applied by the Finnish regulator *Radiation and Nuclear Safety Authority (STUK)* and the two Finnish nuclear power plant operators *Teollisuuden Voima Oy (TVO)* and *Fortum Power and Heat Oy (Fortum)*. The study was conducted in 1998–99. The research material was based on tape-recorded interviews as well as internal directions and event investigation reports provided by the three participating organisations. A framework for analysis and evaluation was developed as part of the study on the basis of referenced root cause analysis and operating experience review methods, selected (foreign) inspection reports, scientific papers and research literature. Well-known inspection methods and principles, such as ASSET and MTO/HPES, provided important guidance to this work.

This study shows that although all the evaluated organisations had rather comprehensive incident analysis arrangements, more focus and priorisation is needed. Deficiencies were identified mostly in the areas of recording, assessment and classification of new events and observations, use of existing operating experience data, utilisation of information technology based tools, and allocation of work and resources. In general, the direct causes of identified events can be detected and removed, but more emphasis should be given to the prevention of recurrence. This requires a more efficient feedback loop that can be created and maintained by focusing on the root causes of significant events, tasks and activities in which the originating errors occurred, and weaknesses of defensive barriers, and by implementing periodic operational experience reviews. A strategy document for the operating experience feedback process, and firm procedures for the initial assessment of new events and the carrying-out of data analyses would help.

CONTENTS

1 INTRODUCTION

1.1 Background

This study has been initiated due to an assignment from the Finnish regulator, Radiation and Nuclear Safety Authority (STUK), to the Technical Research Centre of Finland (VTT). The study relates to the IAEA Coordinated Research Programme "Investigation of Methodologies for Incident Analysis". The IAEA programme aims at investigating what kind of methods and practices are being used for analysing operational events in nuclear power plants today, how do they work, and how to improve in the future. Special attention is paid to root cause analysis methods and their application in the IAEA member countries.

Today there is a great number of different methods and approaches for investigating operational events. Methods like HPES, MTO and ASSET—together with dozens of other more or less widely known techniques—are being used within the nuclear industry. It is generally recognised that different techniques are necessary for different applications e.g. depending on the characteristics of the events to be investigated. For instance, the significance of the event or the amount of available information may have a major effect on how the investigation ought to (or can) be carried out. As a result, it is important to know the strengths and limitations of existing methods in relation to different investigation needs.

In addition, also the characteristics of the investigation process itself as well as prevailing operational preconditions do have an impact on the outcome of the process. For instance, personnel workloads, management support or inspectors' acquaintance with the method to be used may significantly influence the overall reliability of achieved results. This is why the IAEA programme emphasizes i.a. investigation team issues such as team composition, resources and training, and on-site investigation practices.

The IAEA programme was initiated in 1997 and is envisaged to continue until the year 2001. The overall objectives of the IAEA programme are as follows:

1. to explore feedback of operating experience, especially on event investigation (root cause) methodologies and techniques in current use,
2. to review and analyse existing root cause methodologies and techniques, and determine their applicability areas and evaluate their strengths and limitations,
3. to develop "tool boxes" of root cause methodologies/techniques for particular application areas emphasizing the multiple cause determination concept with corresponding definitions and the classification of direct and root causes.

1.2 Objectives

The main objective of this study is to provide STUK with an evaluation report on the adequacy and reliability of incident analysis methodologies and practices currently applied by STUK itself and the two Finnish utilities Teollisuuden Voima Oy (TVO) and Fortum Power and Heat Oy (Fortum) at their nuclear power plants. The study will focus on the investigation of safety significant operational events. In addition, the study aims at providing a broad overview of the whole organisational framework to support event investigation practices in the three participating organisations.

1.3 A systems approach to incident analysis practices

1.3.1 Nuclear power and organisational reliability

Nuclear power plants are industrial facilities with an important societal function. In many countries they produce a significant part of the total electrical power supply around the year, 24 hours a day. Due to their societal role they have many obligations. First of all, they are supposed to maintain high levels of performance and service to meet public expectations. Secondly, they are also required to maintain high levels of operational safety and reliability to be allowed to continue their operation. As well, as commercial enterprises power companies will have to meet the business goals of their owners. In other words, they must cope with an ensemble of different kinds of, and sometimes conflicting, requirements and expectations.

Many organisations i.a. in the fields of civil aviation, chemical industry and armed forces are also dealing with similar challenges. One of them is their need to manage demanding safety critical operations on day-to-day basis. Such organisations have been called *high reliability organisations* (HROs) in the sense that instead of relying on good fortune or the vagaries of probability they have assumed a pro-active risk management approach to pursuing safety and operational reliability (Rochlin, 1993).

In the field of nuclear power safety is paramount. One could claim, however, that the ever increasing stature of safety issues within the nuclear community partly stems from the fact that people have become more risk conscious. Media pays a lot of attention to all nuclear power related incidents and hazards, and the notion of risk or an impending danger is nowadays the driving force behind most media stories (e.g. Hawkes, 1999). Risk sells, and that is something the Nuclear Managers will have to cope with. It is obvious, therefore, that one just cannot run a nuclear power plant without assuring the public, the media, and the regulator that safety will always come first.

Needless to say, this is just another side of the coin. For most people working in nuclear facilities, as well as for the nuclear organisations themselves, safety is not just a trick to ensure public acceptance. Safety is an important value *per se* although there are different interpretations of what does it mean or require in practice to operate safely. Safety is also rational from the economic point of view. It is evident, for instance, that in the long run safety does correlate with plant reliability and utilisation rates. This means that sound safety investments are likely to result in good economic performance, too, whereas the outcomes of an indifferent safety policy may be quite reverse indeed (consider e.g. the case of Ontario Hydro, described by Andognini, 1998). In consequence, safety has undoubtedly become a matter of organisational survival and an operational imperative for all (commercial) nuclear facilities.

As part of the promotion of operational safety and reliability both utilities and regulatory bodies stress the importance of preventing nuclear safety significant incidents in operating nuclear power plants around the world. Pro-active safety related measures are of utmost importance to all HROs simply because most of them cannot really “afford” major failures. For this particular reason they cannot solely rely on the practice of learning by trial-and-error, either (Rochlin, 1993, p. 16). As a result, most HROs must mainly enhance their safety performance by other means, e.g. by the utilisation of sophisticated risk assessment methodologies, application of advanced design concepts and defence-in-depth principles, and by fostering personnel commitment to safety (e.g. Rasmussen, 1993). Eternal vigilance and the application of efficient pro-active analysis methods are thus prerequisites for successful operation for most HROs (Rochlin, 1993). Nevertheless, even the most reliable organisations tend to fail sometimes.

1.3.2 Improving through learning from experience

Many nuclear organisations have established event investigation practices to monitor and analyse operational events and incidents at their facilities. The very idea of the event investigation practice and the whole operational experience utilisation process is to learn from existing experience (e.g. incidents and failures) and to use that information for the promotion of plant safety and operational reliability. The primary objective of

the practice is the prevention of the occurrence or recurrence of operational events, process transients and latent failures of safety systems..

The operational experience utilisation process consists of several subprocesses or activity areas. Typically it includes procedures for the monitoring and recording of both internal and external operational events, assessment and classification to determine their safety significance and further inspection needs, and the actual inspections of (safety significant) incidents and accidents. Also the processing and implementation of proposed corrective actions can be mentioned in this context since sound investigation results alone do not lead to improvements in plant operations. In addition, the acquisition and storage of operational event data, and the carrying-out of comprehensive operating experience data analyses to identify important failure types, such as recurrent failures and common cause failure mechanisms in safety significant systems and equipment, can be regarded as important subprocesses of the operational experience utilisation process (Fig. 1).

Another question is, however, what are the best possible practices for carrying them out, and how do they depend on various contextual factors, e.g. the existing political and economic situation, or the type and history of the concerned organisation. These are difficult questions without certain and simple answers. The main point is, however, that organisations have to be able to learn from their experiences and transfer that knowledge into practical and effective enhancements. Such learning is largely based on a profound understanding of how and why the incidents really took (or are taking) place. That in turn calls for an identification of the actual *root causes* or the major contributing factors of those incidents and decisions on corrective actions and remedies. The identification of root causes ought to be done by means of a reliable and comprehensive root cause analysis method.

Root cause analyses are used for the in-depth assessment of selected operational events. A root cause analysis is generally (or shall be) conducted for operational events which have, or may have, specific safety significance and whose causes are not obvious. In addition to safety, also economic reasons, e.g. the possibility to avoid production losses, equipment damages and personnel injuries, will initiate the inspection process.

There are dozens of different kinds of root cause analysis methods. Their techniques and concepts may significantly differ from each other partly because they have been designed to tackle different problems, and partly because they are

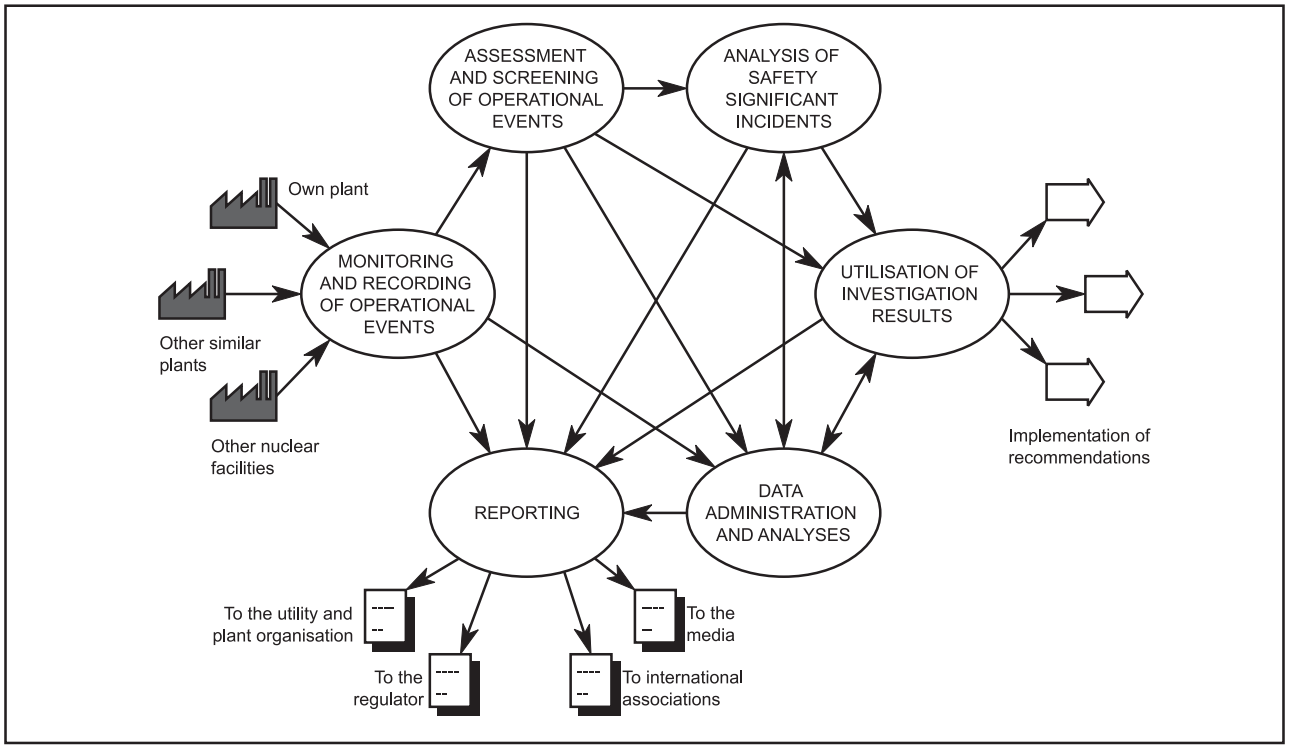


Figure 1. *An overview of an operational experience utilisation process: major subprocesses and their mutual interconnections.*

based on different thinking and theories. Many methods have a lot in common, however. The following list itemises some general *objectives* that are typical of many root cause analysis methods:

- to explain what happened and to illustrate the course of events from the very beginning of the incident to the consequential failure at the end of the event chain,
- to provide a better understanding of how different causal factors actually contributed, or may have contributed, to the incident initiation and propagation,
- to explain why the incident was not prevented from happening i.a. by evaluating the adequacy and effectiveness of existing technical and administrative barriers,
- to shed light on what else might have happened under different conditions, and to assess the general reliability and adequacy of plant systems and control procedures,
- and to issue recommendation for further actions to prevent the recurrence of similar and corresponding events in the future.

In practice, operational event reports contain a lot of plant specific information (e.g. log files, graphs, process computer recordings, specifications etc.) needed in evaluating the safety importance of the case in question. Moreover, their content is being regulated by the national reporting directions which usually comprise extensive requirements for reports' coverage and thoroughness (see ch. 4.2.1). General requirements for event investigation and reporting practices formulated as part of this study are given in full detail in Chapter 2.3.

1.3.3 The anatomy of an incident

Although the concept of "root cause" is quite well-established and commonly used throughout the nuclear community, its precise meaning is by no means clear. For instance, it is not quite obvious whether it stands for the "initial occurence" that launched the course of events, or for the "major factor" that (most) significantly contributed to the outcome of the process. The same applies to the vast majority of the professional jargon used in this field, including such terms as direct causes, contributing factors, event sequences and missing barriers, just to mention some of them. In the absence of clear definitions it is sometimes rather difficult to convey as well as catch the very essence of the message. However, the problem does not solely relate to those linguistic considerations. It is the inherent complexity of the organisation and its influence mechanisms that makes it so difficult to describe what, how and why had happened, and consequently, to find applicable and unambiguous concept for that purpose.

On the one hand, many operational events or incidents result from a combination of several contributing factors at *different stages of operation*. For example, human errors committed during the processes of systems specification or design may remain undetected and progress through the stages of inspection and commissioning and finally result in a major systems failure several years later. Detection failures are possible because single errors do not necessarily have any immediate deteriorating impact on the work in progress. The outcome of an erroneous action at one stage may also lead to another (human or technical) failure at the next one.

In consequence, it might be very difficult to differentiate between the underlying causes of the event, the event itself and its outcome (Hollnagel, 1998). Therefore, the outcome of one specific event may be the "root cause" of the next one in a long chain of subsequent events and failures. This is called a *horizontal influence mechanism* (Fig. 2).

On the other hand, an incident may also result from a combination of several contributing factors at *different levels of the organisation*. According to Reason's (1995) model of organisational accident causation most event chains are actually initiated at the highest level of the organisation by inadequate policies and inefficient or unreliable administrative processes. They lay the foundations of error and violation-producing conditions at the workplace which increase the likelihood of individual errors and violations at the "sharp end" of operation. Inadequate safety management practices and insufficient understanding of the safety implications of operation are also likely to result in missing or unreliable barriers.

This *vertical influence mechanism* from the upper echelons of the whole operating environment to the sharp end of the system is rather hard to tackle since the upper you go the weaker the connections come. In consequence, the identifica-

tion of root causes is very much dependent on the scope and thoroughness of the analysis.

Contributing factors may be either active or passive, and stem from individual, organisational, environmental as well as purely technical origins. According to OECD/NEA coding and reporting propositions they can be divided into two categories: causal factors and actual root causes (NEA/CSNI/R(97)15/PART1 1998), of which the latter refer to the initiating events, measures or deficiencies that significantly contributed to the occurrence of the incident.

According to the official position of STUK a root cause is "such a common or systematic (not random) failure, deficiency or drawback that has significantly contributed to the occurrence of the analysed event". It is also characteristics of a root cause that "the licence-holder can influence it by appropriate measures. A root cause thus cannot be a law of nature or actions, or modes of action, of an individual who is not a member of the component manufacturer's or licence-holder's staff". STUK also emphasizes incidents' and organisations' systemic nature by stating that "a root cause is not a single human error or the failure or breaking of a component". This is also the view of the authors of this study. (YVL 1.11, p. 5.).

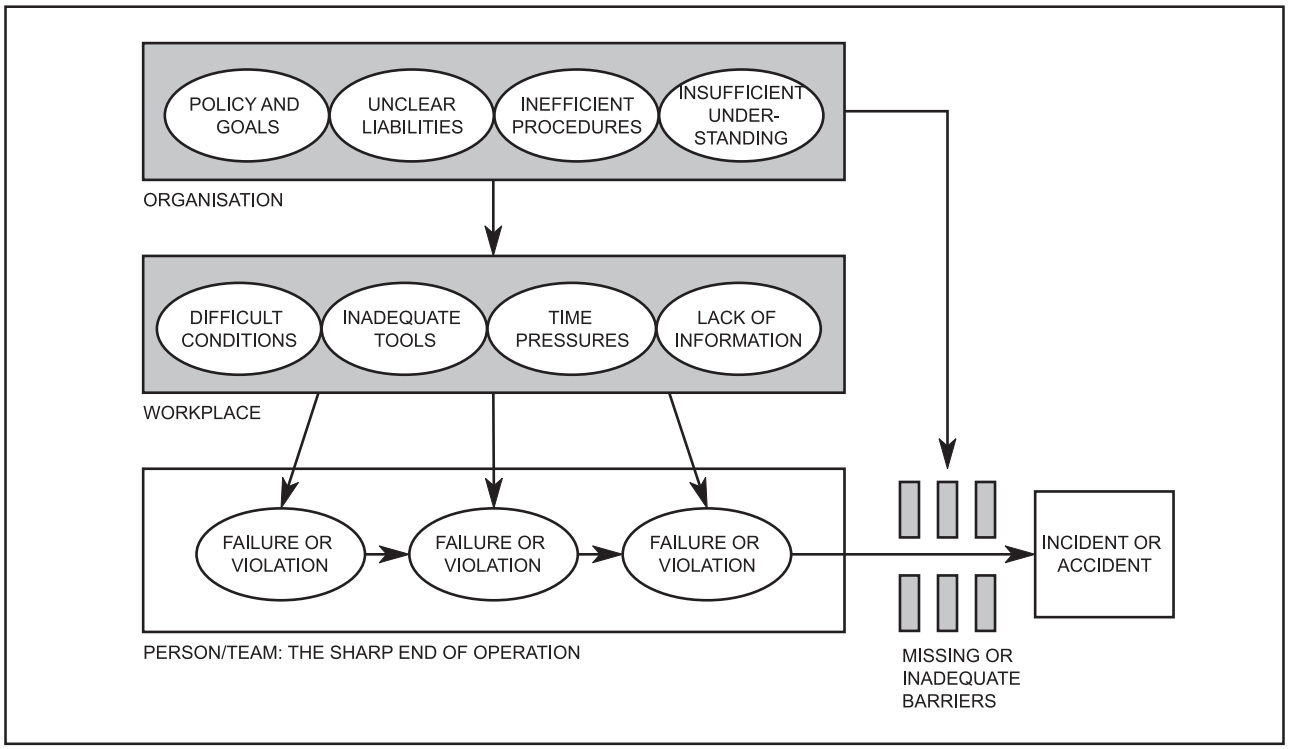


Figure 2. *Horizontal and vertical influence mechanisms contributing to event initiation and propagation (modified from Reason, 1995, p. 1710).*

2 METHODS

2.1 Research procedure

This study was carried out as a joint research project of VTT Industrial Automation (Espoo) and VTT Risk Management (Tampere). Altogether six researchers with different areas of expertise participated in the project. VTT Industrial Automation was responsible for the project management and assumed the main responsibility for the work. The project was started in November 1998 and completed at the end of July 1999.

2.1.1 The framework for analysis and evaluation

The project was carried out in five major stages (Fig. 3). At the first stage a framework for analysis and evaluation was compiled on grounds of selected scientific papers and expert task group reports, selected reference methods and examples of their use for event inspections and existing subject matter expertise at VTT. The framework specified the scope of the analysis and issued require-

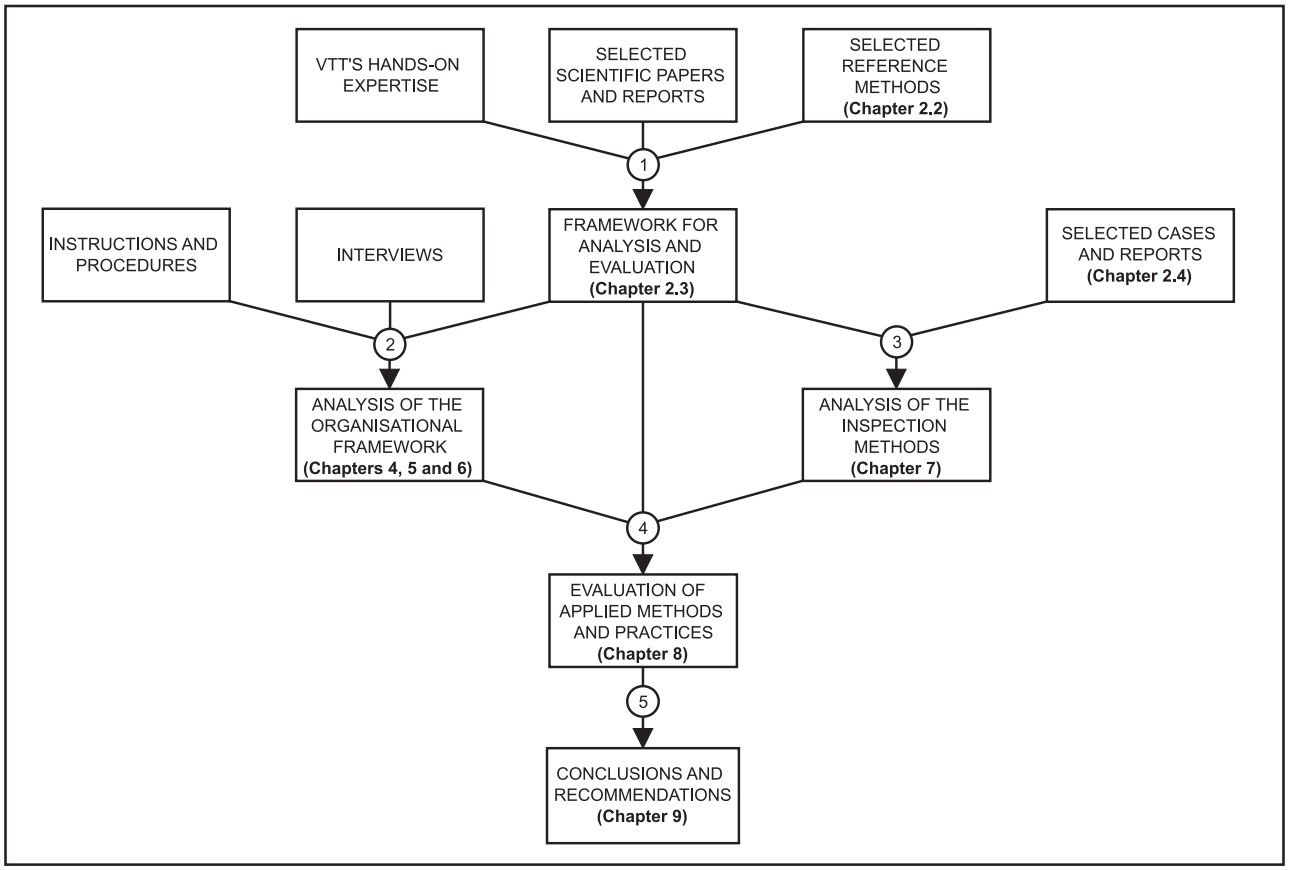


Figure 3. *The research procedure.*

ments for event investigation practices and methods. The framework is described in Chapter 2.3. Referenced inspection methods as well as other important information sources that have been used for drafting the framework are specified and justified in Chapter 2.2.

2.1.2 Organisational framework and investigation practices

The second stage resulted in an analysis and general description of the organisational framework of the event investigation practices in the three participating organisations. The analysis was conducted from the organisational reliability point of view and focused on the managerial framework, investigation procedures, and operational preconditions. The analysis was mainly based on available instructions and procedures, semi-structured interviews as well as information system demonstrations on site. The formal documentation was selected and the interviewees were nominated by the concerned organisations.

Altogether six people were interviewed at Olkiluoto NPP, two at Loviisa NPP and two at STUK, the Finnish regulator. All the interviewees had substantial experience in the field of nuclear safety and their current tasks related to event investigation activities. More than half of the interviewees held a position of a section head or equivalent in their organisations. The interviews took usually from 90 to 120 minutes. Interviews were tape-recorded and transcribed.

Preliminary versions of the analyses of the interviews were submitted to the representatives of the three organisations for commentation. In connection with redrafting the analyses the representatives of Olkiluoto and Loviisa NPPs were interviewed over the phone. According to the authors comprehension a consensus was achieved on most of the remaining open questions. The analyses are reported in Chapters 4, 5 and 6.

2.1.3 Inspection methods and selected inspection reports

At the third stage applied inspection methods and their application were analysed on the basis of selected incident cases and related inspection reports. The cases were selected from the bulk of recent inspection reports provided by the object organisations for evaluation. They as well as their selection criteria are itemised and justified in Chapter 2.4. In the nuclear power plants special attention was paid to the special and root cause analysis reports, and at STUK to the so called TAPREK incident reports. The evaluation focused on the contents, structure and coverage of the inspection reports, characteristics of applied inspection methods and treatment of the particular cases (operational events and a bulk of them) in question. The particular cases were subjected for a new follow-up analysis of the information in inspection reports supplied by the utilities and regulatory body. The results of the analysis and evaluation are presented in Chapter 7.

2.1.4 Evaluation of applied methods and practices

At the fourth stage a comprehensive and summarising evaluation of applied investigation practices and methods in the three participating organisations was produced. The evaluation was conducted on grounds of the two analyses and the evaluation criteria (i.e. requirements and ideal models) specified in the framework paper (Chapter 2.3). Equal attention was paid to the identification and reporting of good practices as well as weaknesses. However, due to the extent of the problem area and possible limitations of the selected analysis cases, many important and interesting issues may remain uncovered and remained beyond systematic assessment. The results of the evaluation are presented in Chapter 8. The main conclusions and recommendations are given in Chapter 9.

2.2 References for analysis and evaluation

2.2.1 Organisational framework

There are numerous studies to show that in addition to strictly technological issues the reliability of any complex and demanding process is also dependent on an ensemble of individual, organisational and environmental performance shaping factors. With respect to nuclear power, comprehensive lists can be found e.g. from Jacobs & Ha-

ber (1994), NUREG/CR-6093 (1994) and NEA/CSNI/R(98)17, Vol. 1 (1999). Especially management issues have been shown to be of great importance to reliability and efficiency in nuclear power plants, as indicated e.g. by the studies of Andognini (1998), Reason (1995) and Dahlgren & Skånberg (1993). There are similar findings also in the areas of civil aviation (Reason, 1995), and chemical industry (Shrivastava, 1992).

It can be assumed that a NPP event investigation practice is no exception of this rule. It is a complex, demanding and time-consuming process, and its outcome is dependent on individual and organisational contributions over a long period of time. Therefore, the question is not just about the theoretical competence of applied methodologies and procedures but also the availability of adequate control and support functions that provide those activities and individuals with necessary direction and resources. As a result, also the prevailing organisational framework needs to be analysed and evaluated in a way that reflects its relative importance to the reliability and effectiveness of the whole process. That is why this study has been conducted from an organisational reliability point of view.

Organisational reliability, as we would like to define it, refers to the degree to which organisations have managed to define, acquire and/or adhere to such policies, structures, processes, resources and knowledge that are necessary to guarantee an acceptable level of performance. On the basis of existing empirical evidence it is argued that they can be created and maintained by deliberate management decisions and procedures only, and that reliability has a systems nature in the sense that it cannot be reduced to, or solely explained by the attributes of a single employee or a particular function or device. This is what we call *a systems approach* to organisational reliability. A good description of its utilisation in the area of safety assessment can be found (in Swedish) from Wahlström and Gunsell (1998, pp. 89-112).

This analysis is divided into two parts of which the first one (covering Chapters 4, 5 and 6) provides an overall description of the organisational framework of the three participating organisations in relation to their operational experience utilisation processes. It has been further divided into three themes called *managerial framework*, *investigation practices* and *operational preconditions* as shown in Figure 4. The second part (Chapter 7) focuses on the analysis of applied *inspection methods* on the basis of their use on selected cases and related (e.g. special and root cause analysis) reports.

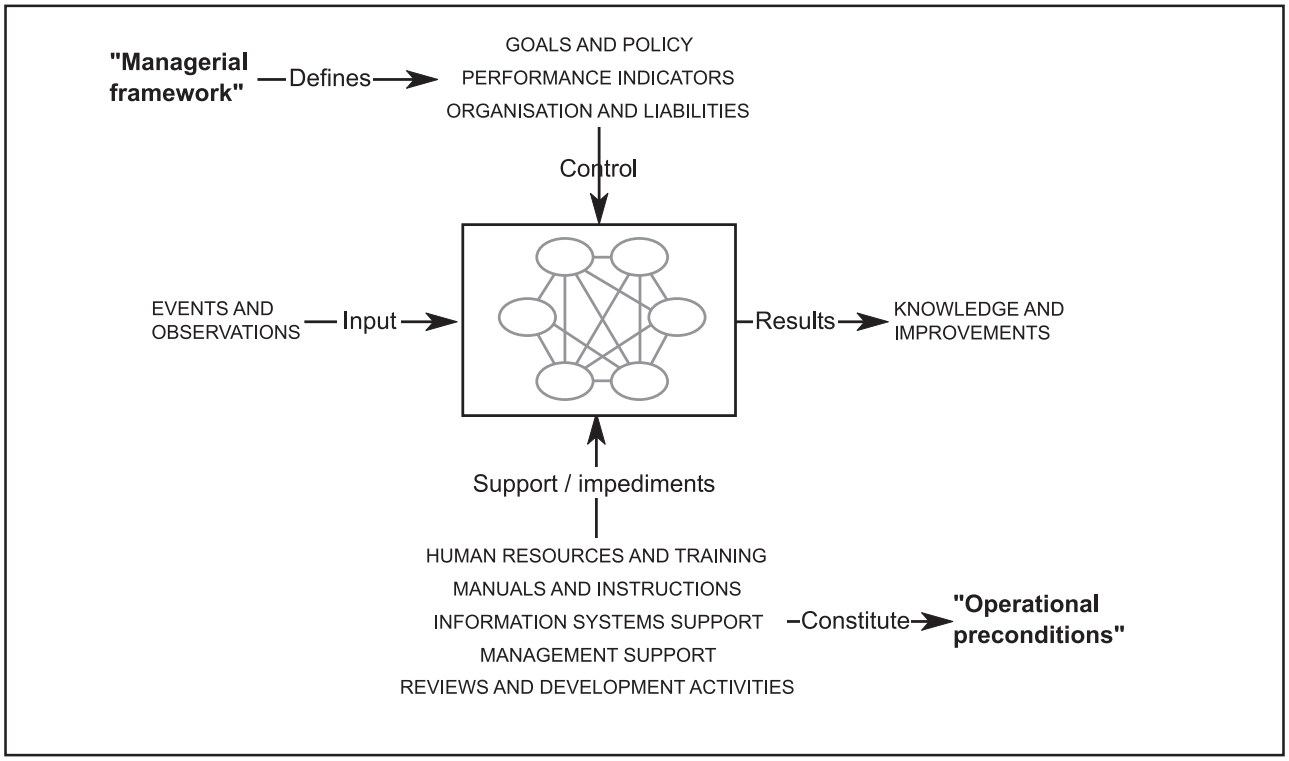


Figure 4. *The organisational framework of the operational experience utilisation process.*

The major reference for the analysis and evaluation of the organisational framework is "Successful health and safety management" (HSG65, 1998), a guide produced by the UK Health and Safety Executive (HSE). It is mainly aimed at health and safety directors, managers and professional to provide practical guidance to managing safety related activities. In general, the guide describes the principles and management practices which provide the basis of effective health and safety management, sets out the issues which need to be addressed, and provides guidance to the development of improvement and self-assessment programmes. In this study, those principles and practices have been used to produce a list of topics (i.e. practices, procedures, instructions etc.) to be addressed in the analysis of the organisational framework, and to provide guidance to drafting the general evaluation criteria for the concerned areas. The key elements of successful health and safety management, as presented in HSG65, can be found from Appendices. A detailed, but concise, description of the UK approach is given in (NEA/CSNI/R(98)17, Vol. 2, 1999, pp. 28-31). However, the scope of the analysis and evaluation framework formulated as part of this study is *not* limited to HSG65 or any other single study, guide or source of information.

2.2.2 Inspection methods

Two internationally recognised event inspections methods were selected as reference methods. The first of the methods MTO (Man-Technology-Organisation) analysis is a root cause analysis method developed in Sweden and used by most Nordic utilities. The second is ASSET (Assessment of Safety Significant Events Team) which includes both an assessment method of single incidents and a periodic operating experience review of the bulk of incidents. ASSET is launched by the IAEA (International Atomic Energy Agency) serving here as the world's intergovernmental forum for scientific and technical co-operation for the nuclear safety and power branch.

The MTO method is based on the HPES method (Human Performance Enhancement System) which was developed for the U.S. NASA space programs. Later on, INPO (Institute of Nuclear Power Operators) started to apply HPES for root cause analysis in nuclear power plants. Today a large number of U.S. utilities use the HPES method. Also the large Canadian Ontario Hydro and French EDF utilities use the HPES method. One benefit of the MTO root cause analysis method in Finland is that its use can be benchmarked and trained with Swedish utilities (Bento 1990, Rollenhagen 1998). The most important aim of the MTO method for analysis of events is to search weaknesses in performance of a utility to prevent *recurrence* (0-S-O-23/1).

The parts of the MTO method are event and cause analysis, deviation analysis, barrier analysis and consequence analysis. In Figure 5, a principal extraction of a block diagram combines and represents in a structured way the *event sequence, deviations from normal conditions, causes* and the broken or failing *defensive barriers.*

Although the MTO analysis is rather resource consuming, it is also suitable for root cause analysis of technical incidents that have significance potential although they not exhibit directly human errors or organisational weaknesses. The graphical presentation of the events and causal factors in an informative chart is particularly useful for complex and complicated situations, and is much more meaningful than long narrative descriptions. In addition, the probable causal factors become evident as the chart is developed (HPES 1992).

The objective of ASSET self assessment is to answer thoroughly seven basic questions with a view to enhance event prevention. The questions are numbered and summarised in Figure 6.

The starting point of ASSET is detailed screening and follow-up analysis of the past operating experience. The bulk of the operational incidents that have occurred during past five years (during operation and plus all failures during periodic testing/inspections). A standard follow-up event analysis report is prepared for each incident including safety impact assessment, the logic tree of failures, the root causes of each failure, the safety culture assessment and the action plan.

In addition the aim of the periodic review of the operating experience is trending of good events (identified by surveillance) versus bad events (failures), trending of safety relevant events versus the whole population, trending of recurrent failures, trending of the ten indicators

of safety impact and trending of three indicators of safety culture according to the IAEA definition (ASSET 1998).

The starting point of the ASSET peer review is the plant self assessment report. This requires from the plant clear and thorough answers to the above seven basic questions in the self assessment report on plant safety performance, safety problems and safety culture.

The final result of the periodic operating experience review is a conceptual ranking of the pending safety problems and specification of the remaining corrective actions (equipment, personnel, procedures) still to be implemented at the plant. The ASSET peer review report has also the task to present an evaluation of the management capabilities to prevent occurrence and recurrence of failures by either repairs or remedies during operation.

Although the standard event analysis reports of ASSET are aimed at conducting a follow-up analysis at both single incident and past incident population, the ASSET format and tools seem also to be practical for analysis of new single events and incidents.

However, the evaluation of the inspection methods and reports used in Finland is not limited to the comparison of the method guides of MTO and ASSET with the actual outcome at the plants and regulatory body. The insights acquired and contributions done in the forums for scientific and technical co-operation such as the Task Forces of the OECD/NEA/CSNI/PWG 1 (The Principal Working Group for operating experience and human factors), independent NKS (Nordic Nuclear Safety Research) and KTM (Ministry of Trade and Industry) research programs on operational and reactor safety, and the IAEA co-ordinated research programmes were also used as an input and references contributing to the evaluation and comparison (NEA/CSNI/R(98)17, Vol 1, 1999), (NEA/CSNI/R(97)15/PART1, 1998), (NEA/SEN/SIN/WG1 (98)17, 1998), (NEA/CSNI/R (97)5, PARTS 1 & 2, 1997), (SKIFS 1998:1), Laakso, Pyy & Reiman (1998), Bento (1997), (NKS/SIK-1, 1994), and Laakso (1984). The international, Nordic and Finnish case and task force studies and their selected examples of well analysed and clearly documented inspection and operating experience reports have provided references and valuable

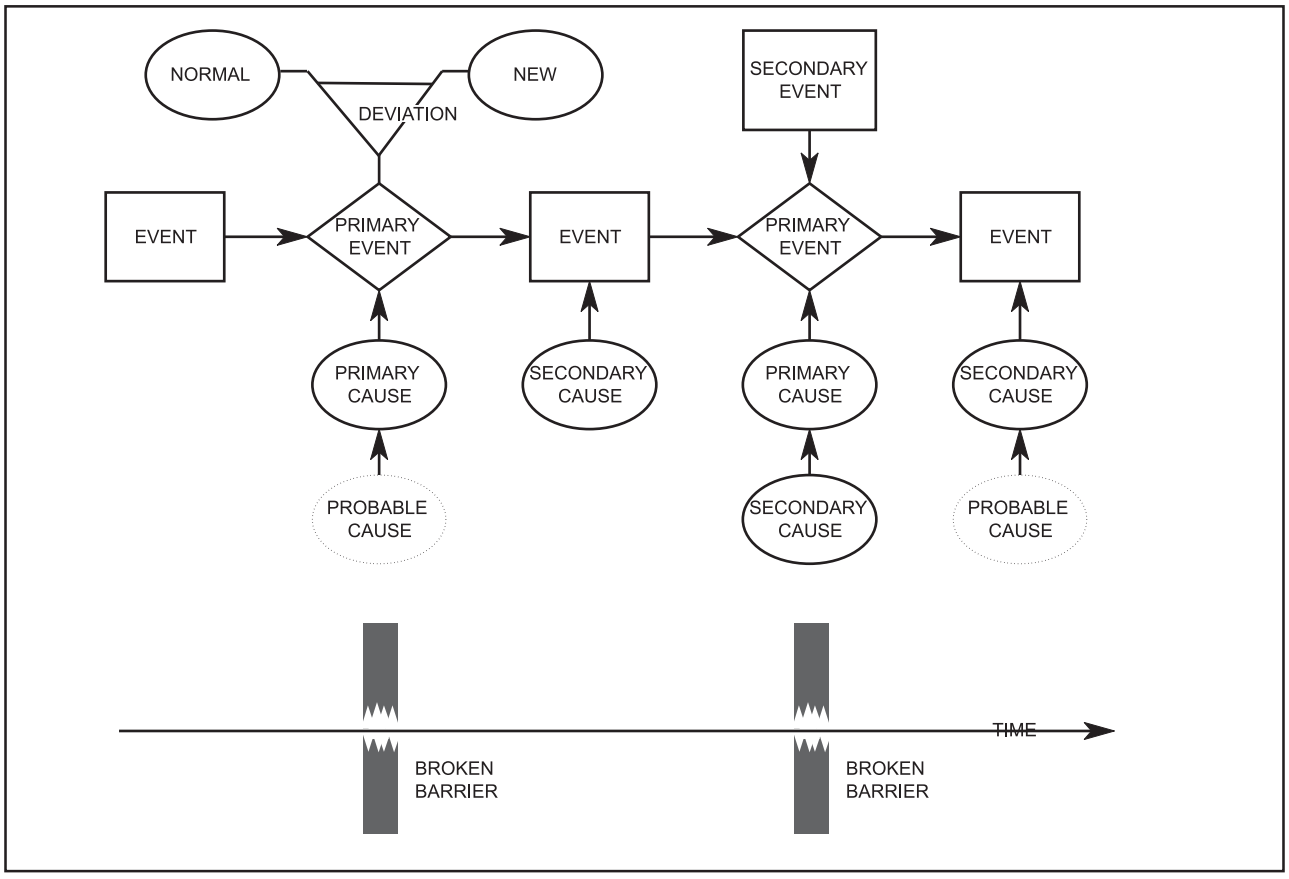


Figure 5. *A MTO event and cause diagram (0-S-O-23/1).*

insights on specific inputs and requirements for the ideal model construction for the following framework of the analysis and evaluation.

2.3 The framework for analysis and evaluation

The framework comprises four analysis areas and five ideal models. The analysis areas are managerial framework (ch. 2.3.1), investigation practices (ch. 2.3.2), operational preconditions (ch. 2.3.3), and inspection reports (ch. 2.3.4). The ideal models present good practices and requirements for the structure and phasing of the event investigation procedure (ch. 2.3.5) and the operating experience feedback loop (ch. 2.3.6), and for the scope and characteristics of event inspection methods (ch. 2.3.7), follow-up analyses (ch. 2.3.8), and periodic operating experience reviews (ch. 2.3.9). In connection with the analysis areas both the scope of the analysis and the area specific requirements have been defined under corresponding subtitles. The ideal models are "ideal" in the sense that they present target states against which licensees' and STUK's methods and practices are compared. The framework description has intentionally been left concise to enhance readability and to allow flexibility in identifying successful and effective practices and methods for event investigation and the operating experience feedback loop.

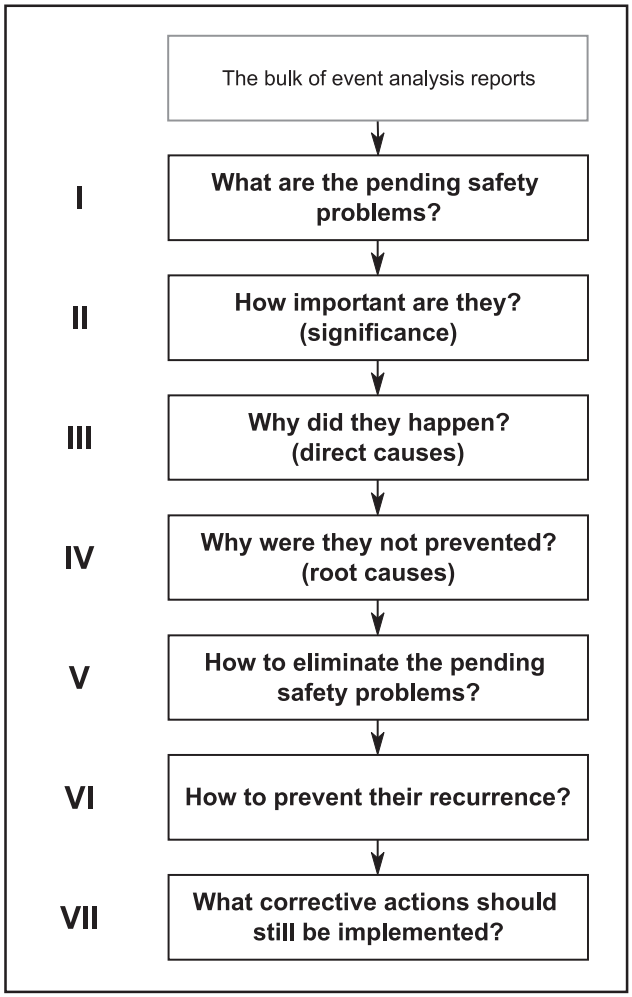


Figure 6. *The ASSET procedure for plant self assessment of safety performance.*

2.3.1 Managerial framework

Scope of the analysis

- Goals and policy
- Performance indicators
- Organisation and liabilities

General requirements

- Goals have been defined and documented
- Goals are explicit and unambiguous
- Goals are generally known and understood
- A pro-active approach towards safety is being emphasised
- Prevention of the occurrence and recurrence of events is of top priority
- Indicators for effectiveness have been defined and are in use
- The plant management knows what is going on at the plant
- Liabilities have been clearly defined
- Each key process or activity has an owner
- The event investigation practice has enough integrity and independence

2.3.2 Investigation practices

Scope of the analysis

- Monitoring and recording of operational events
- Assessment and screening of operational events
- Analysis of safety significant incidents
  - Initiation
  - Team composition
  - Inspection procedures and methods
  - Experiences
- Utilisation of investigation results
  - Safety assessment
  - Processing and implementation of recommendations

- Data administration and analysis of the bulk of investigation data
- Reporting
- Self-assessment on strengths and weaknesses

General requirements
- There is a procedure for each key process and activity
- Practices comply with approved procedures
- Current monitoring practice has potential for detecting all safety significant events
- Current monitoring practice has potential for detecting recurrence
- Operational experience from other plants is being monitored and assessed
- All events and observations that have, or may have, safety significance are recorded
- All such events and observations are assessed and classified in a systematic way
- There are clear criteria for determining what kind of further inspections are needed
- All safety significant events are thoroughly inspected
- Inspections are carried out by competent and knowledgeable personnel
- Remedial actions are recommended for the prevention of recurrence
- Inspection results are assessed in a systematic way from the safety point of view
- The processing and implementation of recommended actions is under supervision..
- ...and achieved results are identified and compared with acceptance criteria
- Operational event data is stored in a systematic way and made easily available
- Operational event data is subject to systematic reviews (or periodic data analyses)
- Reporting to the regulator is conducted in accordance with the reporting requirements

Specific requirements
- The event investigation practice comprises the main components of ideal model A (ch. 2.3.5)
- Operational experience is being systematically utilised as shown in ideal model B (ch. 2.3.6)
- Applied event inspection methods fulfil the requirements given in ideal model C (ch. 2.3.7)
- Each significant event is subject to a follow-up analysis according to ideal model D (ch. 2.3.8)
- Operational event data is subject to periodic reviews according to ideal model E (ch. 2.3.9)

2.3.3 Operational preconditions

Scope of the analysis
- Human resources and training
- Manuals and instructions
- Information systems support
- Management support
- Reviews and development activities

General requirements
- Adequate resources have been assigned to each key process and activity
- There are competent personnel who can concentrate on event investigations
- A good understanding of the functional features of the plant is available
- Human and organisational factors expertise is available and being used
- Technical expertise is available and being used
- Attention is paid to personnel training and succession planning
- Instructions are available, clear, useful and up-to-date
- The potential of information technology is being utilised to the extent it is practical
- Existing information systems are generally considered usable and useful
- Upper management provides concrete support for the event investigation practice
- The event investigation practice is subject to regular performance reviews
- External and independent evaluators have regularly participated in/conducted reviews
- Major deficiencies have been recognised and are subject to development activities

2.3.4 Inspection reports

Scope of the analysis

An in-depth analysis of selected cases (i.e. operational events) and related inspection reports from the three participating organisations was carried out as part of this study. Selected cases and reports as well as criteria for their selection are itemised in Chapter 2.4.

General reporting requirements
- Reports are clear, illustrative and unambiguous
- They focus on systemic deficiencies and causes, individual anonymity is maintained

- There is a clear distinction between fact and speculation
- Information sources are identified, conclusions are justified
- Reference to applied methods is given, selection of the method is justified

Specific reporting requirements

- According to ideal model C

2.3.5 Ideal model A: General framework for the event investigation practice

- All events and observations that have, or may have, safety significance are identified and recorded (see Fig. 7).
- All such events and observations are assessed, described and classified in a systematic way. The initial classification and screening is based on significance and further inspection, action and reporting needs.

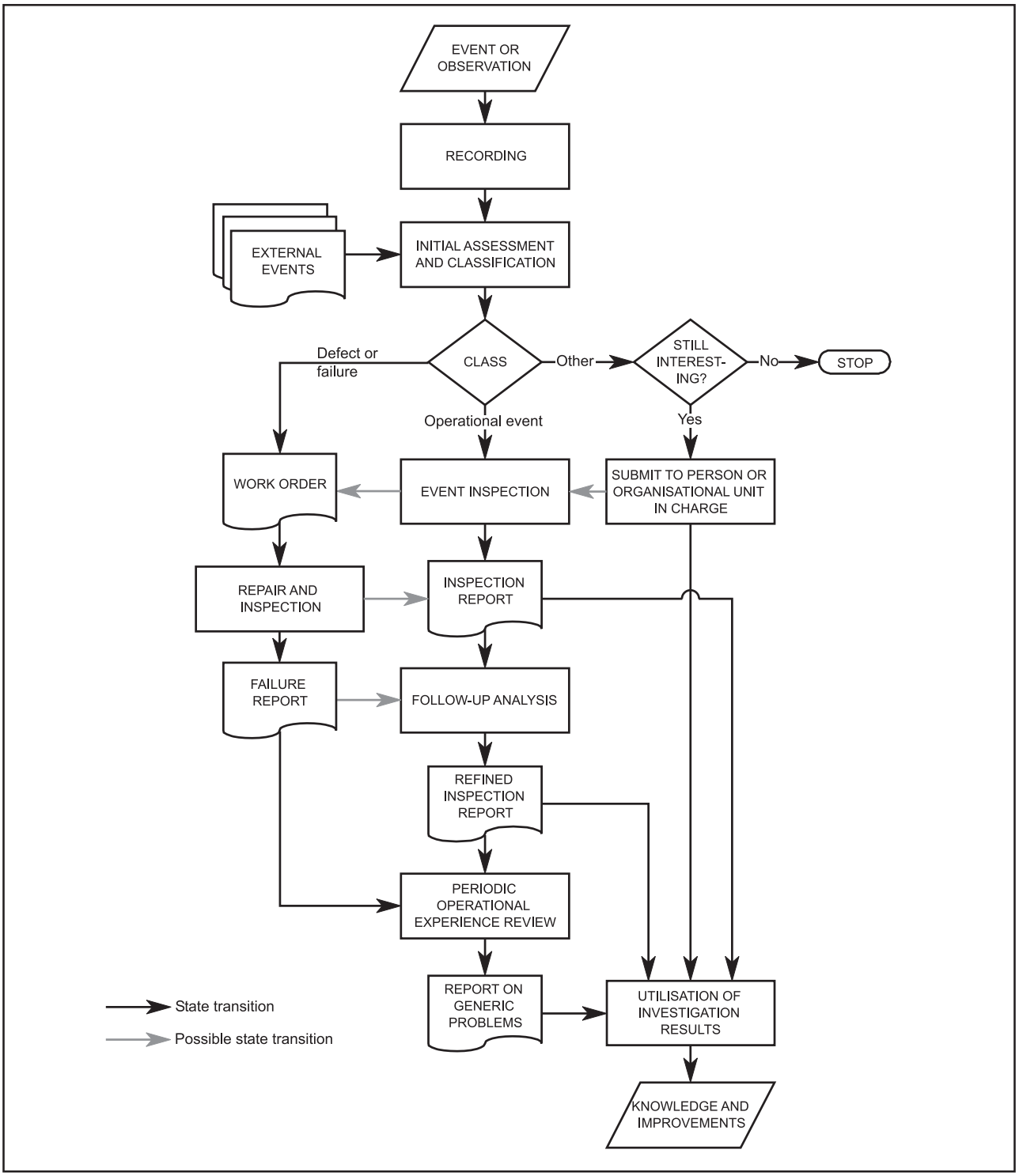


Figure 7. *Ideal model A. General framework for the event investigation practice.*

- Each significant event is analysed by an appropriate method. Minor (technical) defects and failures are passed through the work order (and data collection and analysis) procedure. Other interesting events are submitted for consideration to the persons, teams or organisational units that are responsible for the concerned matter and/or could benefit from the information. Events and observations classified as non-significant are filed.
- Each significant event is reanalysed after a certain period of time. The original inspection report is updated to reflect the latest knowledge, actions and understanding.
- Operational event and failure data are subject to regular and comprehensive reviews. The recurrent failures, and pending plant level safety and operability problems are identified and an action plan for improvement is compiled.
- Investigation results are always taken into account in an appropriate way. They result in learning and decisions on corrective and remedial actions.

2.3.6 Ideal model B: Operating experience feedback loop

- Operating experience is gathered, recorded and administrated in a systematic way (see Fig. 8).
- Records of events and failures are easily available and widely utilised.
- Classifications and decisions are based on existing knowledge and approved objectives.
- The effectiveness of applied policies and result of implemented remedial actions is being followed.
- Inefficient or inappropriate policies and measures are detected and corrected.

2.3.7 Ideal model C: Requirements for event inspection methods

General requirements

- The inspection procedure is initiated as soon as possible
- Inspections are carried out in a no-blame atmosphere
- The concepts of “direct cause” and “root cause” have been explicitly defined

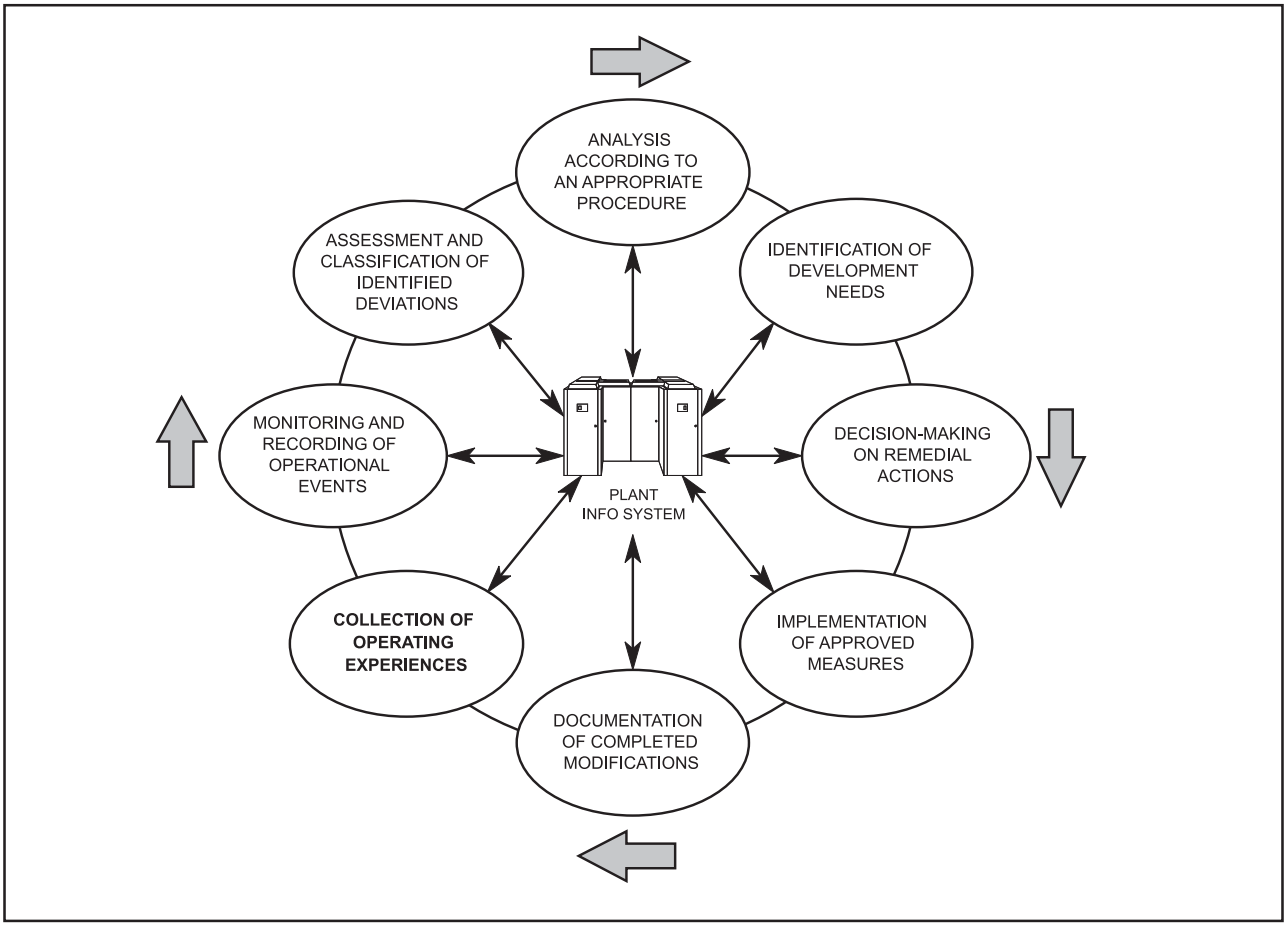


Figure 8. *Ideal model B. Operating experience feedback loop.*

- Both initiating events (transients, defects) and latent failures are addressed
- The method has potential to reveal all major failure modes and safety significant issues
- The stopping criteria have been defined
- The inspection report has a clear structure, format and contents
- The report suits for utilisation of information technology and periodic operating experience review.

Specific requirements concerning the issues to be covered

The following list comprises specific requirements for inspections that have been initiated due to an initiating event (e.g. process transient) or a latent failure (e.g. unavailable standby safety system):

- ID information: unit, date, time, descriptive title, inspectors etc.
- Immediate consequences of the incident
- Affected systems, equipment and structures
- Operational conditions and major process parameters prior to the incident...
- ...and explanatory process and computer recordings to illustrate its progression
- Means of detection and the situation in which the incident was discovered
- The course of events (event sequence from the origin up to and including recovery actions in a chronological order)
- Problems encountered in managing and controlling the situation
- Use and adequacy of approved procedures and instructions
- Direct and root causes of the incident (the cause-effect chains explaining the case)
- In case of a human failure, the work task in which the error occurred (the failure origin)
- Common cause failure (CCF) mechanisms, origins and interconnections to other systems
- Efficiency and adequacy of both technical and administrative barriers...
- ...and in case of a technical failure, the adequacy of operability verification activities
- Evaluation of historical recurrence (both local repair actions and root causes)
- Availability of important safety systems
- Incident's significance in terms of nuclear, personnel and radiation safety
- Necessary immediate and long term corrective actions and their expected effects
- Event recording and classification system (the event report is completed with classification for searches and periodic operating experience review purposes)
- Reference to other related investigations, such as work orders and failure reports

Although the above list of specific requirement issues for incident inspection that have been initiated due to an initiating event or a latent failure is the same, differences in the thoroughness of the analysis and reporting of the issues depend on event classification and significance.

2.3.8 Ideal model D: Requirements for the follow-up analysis

- Important operational events shall be reanalysed within a certain period of time
- Certain period = after the causes and failure mechanisms have been substantiated and the remedial measures have been identified and decided
- The follow-up analysis shall be based on the utilisation of the plant information system
- Signs of historical recurrence, CCF mechanisms and latent failures are checked
- Status of proposed corrective measures is checked
- Effects of already completed enhancements are evaluated
- Evaluation of the event's safety significance is substantiated (or changed)
- If necessary, new action proposals are issued
- Findings of the original inspection report shall be updated to reflect the latest knowledge
- The updated report and new findings shall be brought to a responsible person's notice
- In general, the follow-up analysis should result in a report that supports periodic operational experience reviews and trend analyses as well as possible.

Examples of different follow-up analysis reports or their features can be found e.g. in the Swedish final reports of safety related occurrences (Ericsson, 1999), in TVO's analysis summaries of single events (TVO ASSET, 1998), in detailed TAPREK event reports of STUK, in the PSALO human fai-

lure reports (see Appendices), in the description of regulatory body uses of trend analysis of incident data (NKS/SIK-1, 1994) and in the plant disturbance follow-up analyses carried out by Laakso (1984).

An example of a follow up analysis of a human common cause failure studied at root cause level can found in Appendices.

2.3.9 Ideal model E: Requirements for periodic operational experience reviews

The bulk of event investigation data shall be reviewed on a regular basis. One way of doing that is a comprehensive review carried out once every five (ASSET assessment period) or ten (IAEA's recommendation) years to cover all the operational events and significant failures that have been recorded and analysed since the previous corresponding assessment.

However, it is proposed that instead of such "non-recurring" exercises reviews should be based on an annual sliding assessment of the past five (or more) years' operating experience reports. Such a review could be carried out in two phases as follows:

1. A follow-up analysis of operational events identified and inspected during the preceding (calendar) year in accordance with ideal model D.
2. Classification of the new event data resulting from the follow-up analysis, updating of statistics, review of the event inspection and failure/ maintenance data acquired during at least the past five (1 + 4) years period, and compilation of a review summary report.

The main objective of the review is to identify and rank the pending safety problems and to come up with concrete and well justified recommendations for enhancing the effectiveness of incident prevention. The review shall thus address / take into account following issues:

- All relevant operating experiences and failure history data (including those that remained below the *official* reporting threshold)
- Dominant event and failure types, related systems, equipment and structures
- Recurrent events and failures, trend analyses
- CCF mechanisms
- Direct and root causes of those events and failures
- Status of proposed and approved corrective and remedial actions
- Effects of completed enhancements and modifications
- Systematic comparison and benchmarking between the plant units and with other plants
- Identification and ranking of the pending safety (and other) problems
- Prioritisation of necessary corrective and remedial actions based on their expected effects
- The review report and new findings shall be brought to responsible persons' notice.

Other proposals:

- Take full advantage of existing follow-up analysis reports
- Aim at developing a clear and useful classification system for events and their causes
- Address specific themes such as particular systems, activities and procedures, too
- Try to identify operational events from the maintenance history data (e.g. CCF mechanisms).

Examples of periodic operating experience reviews or their features can be found in e.g. the TVO self assessment report of safety performance, safety problems and safety culture on the basis of operational events (TVO ASSET, 1998), in the report on systematic identification and analysis human common cause failures (Laakso, Pyy & Reiman, 1998), in the analysis of MTO related events in Swedish nuclear power plants 1994-1996 (Bento, 1997), in the description of regulatory body uses of trend analysis of incident data (NKS/SIK-1 1994), in the ageing study of the Loviisa power plant plant protection automation (Simola & Maskuniitty, 1995), in the report of Experience Based Reliability Centered Maintenance of MOV drives (Hänninen & Laakso, 1993), in the CCF analysis of high redundancy systems (Mankamo *et al.*, 1992), in the trend analyses of LERs and reactor trips at the Forsmark 2 nuclear power plant (Brolin, 1988 & 1987) and in the report of systematic feedback of plant disturbance experience in nuclear power plants (Laakso, 1984).

2.4 Selected cases and reports

The needs of the operating experience feedback of the two Finnish nuclear power plants and their four operating units have resulted in a large amount of incident inspection reports during their present life of about 20 calendar years. Due to the vast extent of available information and rather limited evaluation resources, the assessment had to be focused on a smaller number of suitable cases that could be more thoroughly investigated. In addition, the sample had to be a representative one to provide a sound basis for further evaluations. Therefore, an adequate criteria for selection was needed.

The criteria for the selection of cases for a detailed review are given below together with related justifications:

- information on the incident is available, because the reviews were conducted as follow-up analyses of selected cases and were not limited to the structural characteristics of related reports
- in addition to technical problems, also human and/or organisational factors were involved, because this study was based on the presumption that the treatment of human and organisational factors is of significant importance to the quality of investigations
- the event has been investigated according to valid procedures, because one important objective of this study was to pay attention to the strengths and weaknesses of different event investigation methods and techniques
- the procedures represent "mainstream" investigation activities in evaluated organisations, because the main objective of this study was to evaluate those incident analysis methods and practices that were actually being applied by the participating organisations
- the regulatory body has performed an own investigation of the event, because this was considered to most feasible way evaluate the regulator's methods and practices and to make comparisons between the utilities and the regulator.

As a result of an initial screening the following cases and reports were selected to be thoroughly assessed:

2.4.1 Olkiluoto NPP cases and reports

- TVO 1. *Neutron flux trip limits left too low after isolation valve capacity test*. Dates of detection: 24.05.1994 and 05.06.1994. Related documents: Root cause analysis 1-TR-R1-2/94, Special report 1-TR-R7-1/94, Reactor trip report 1-KK-R6-1/94, ASSET Event Analysis Nos. 27 + 28, STUK TAPREK report 111/ 28.11.1996.
- The ASSET self-assessment and peer review for operational events occurred during the five year period of 1993-1997 at Olkiluoto power plant. Related document: TVO ASSET 1998.
- TVO 2. *Oil leakage and fire initiation*. Date of detection 29.1.1998. Related documents: Plant disturbance report 2-KK-R4-1/98, STUK TAPREK report 149/25.9.1998.

The ASSET report was selected to avoid bias in an evaluation in which only a very limited sample of single event inspection and refined inspection reports were thoroughly assessed. Due to the extent of the ASSET periodic operating experience review report it was however less thoroughly analysed than any specific event case according to the requirements of Chapter 2.3. In addition, the researchers got acquainted with a large number other operational and failure events as well as annual operating experience utilisation reports that were compiled during the period of 1993-1998 at Olkiluoto NPP. This was done to establish a good overview of TVO's investigation and reporting practices and to avoid the risk of losing an integrated perspective. That ensemble of reports was however not subjected to a rigorous follow-up analysis and assessment according to the requirements of Chapter 2.3.

During the course of this study it was observed that the follow-up analysis of selected cases and related inspection reports took more time and resources than originally anticipated. In consequence, TVO's third case (oil leakage and fire initiation) was deliberately excluded from the analysis and cannot therefore be found in Chapter 7.1.

2.4.2 Loviisa NPP cases and reports

- LO 1. Common cause failure of TL 22 air fans to start due to incorrect connection diagram. Date 23.09.1997. Related documents: Operational Event Report KT 47/97.
- LO 2,1. Unallowed disconnection of back-up emergency feed-water pump for preventive maintenance during power operation: Date of detection: 14.01.1997. Related documents: Root cause analysis LO1-K863-6, LO2 special report 1/97, KT report 01/97, STUK TAPREK report 134/ 11.06.97.

In addition, the researchers got acquainted with a large number other operational event, failure, QA theme inspection as well as annual operating experience utilisation reports that were compiled during the period of 1995-1998 at Loviisa NPP. This was done to establish a good overview of Fortum's investigation and reporting practices and to avoid the risk of losing an integrated perspective. That ensemble of reports was however not subjected to a rigorous follow-up analysis and assessment according to the requirements of Chapter 2.3.

2.4.3 General

Before case evaluations were started the utility representatives were asked to comment on the selection criteria and proposed cases. To the reviewers' question "*Do these cases and connected inspection reports provide a true and comprehensive conception of the inspection of operating events at your plant*?" both utility representatives answered "*yes*".

The selected approach facilitated also a comparison of the contents of the inspection reports prepared by the utilities and the regulatory body on the same incident cases and commenting on advantages and weaknesses of all parties' inspection reports and incident analysis practises. Results of the analysis and evaluation of the selected cases are presented in Chapter 7.

3 USE OF NUCLEAR POWER IN FINLAND

3.1 Finnish nuclear power plants

Finland's nuclear power plants are located on the south and west coast of Finland. The state-owned Fortum Power and Heat Oy, founded in 1998 as a merger of two Finnish power companies Imatran Voima Oy and Neste Corporation, operates two 488 MWe VVER-440 type pressurised water reactor units, Loviisa 1 and Loviisa 2, near the city of Loviisa. On the west coast of Finland Teollisuuden Voima Oy (TVO) operates two 840 MWe ASEA-ATOM type boiling water reactor units, Olkiluoto 1 and Olkiluoto 2, in Eurajoki. Both utilities have been involved in the process of increasing the electrical output of their stations over a period of last four to five years, and the plant modifications related to the power increase were mainly completed at the time of this study. The first unit, Loviisa 1, was connected to the national grid in 1977, and the fourth, Olkiluoto 2, in 1980. These four reactors generate about 30 % of Finland's annual electricity output.

3.2 Finnish nuclear regulation

Regulation of the use of nuclear energy and radiation in Finland is based on the Nuclear Energy Act (990/87) and the Radiation Act (592/91). Further requirements are given in Nuclear Energy Decree (161/88) and the Decision of the Council of State "General Regulations for the Safety of Nuclear Power Plants" (395/91). According to the legislation Radiation and Nuclear Safety Authority (STUK) sets safety requirements and verifies compliance with them. STUK has in this respect developed a comprehensive set of safety guides, the so called YVL-guides, to cover all the major areas of nuclear power plant operation.

The regulation of nuclear power plants covers the entire life cycle of each facility, from design to decommissioning. The primary objective of regulation is to ensure that the reactor remains under control in all conditions.

The operating organisations have the full and undivided responsibility for the safety of nuclear power plants. In accordance with defined inspection programmes, STUK verifies that their operations and related support activities are appropriate and in compliance with safety requirements. STUK emphasises the significance of the users' voluntary work in ensuring the safety of their practices. According to STUK's official position it would mean failure if shortcomings had to be rectified by enacting compulsory measures by the regulator.

4 RADIATION AND NUCLEAR SAFETY AUTHORITY

4.1 Managerial framework

4.1.1 Goals, policies and performance indicators

As part of its supervisory duty the Finnish regulator, Radiation and Nuclear Safety Authority (STUK), follows operational events and event investigation practices in Finnish nuclear power plants and conducts its own investigations for selected cases. The general directions regarding the utilisation of nuclear power plant operational experience are given in Section 27 of the Decision of the Council of State (395/91), according to which operational experience and safety research results shall be systematically followed and assessed, and actions to enhance safety on grounds of operational experience, safety research and advances in science and technology shall be implemented. The decision pertains to the utilities as well as to the regulator itself. Detailed regulations concerning the utilisation of operational experiences in Finnish nuclear power plants are given in YVL 1.11 "Nuclear power plant operational experience feedback" and YVL 1.5 "Reporting nuclear power plant operation to the Finnish Centre for Radiation and Nuclear Safety"[1].

The general objective of STUK's investigation practice is to support nuclear power plant operational safety surveillance (YTO 7.4). What does it mean in practice remained, however, somewhat vague to the authors of this study. YTO 7.4 did not contain any additional, more detailed or concrete definitions, and the representatives of STUK were not able to give them either during the interview. In this respect they referred to the content of the aforesaid Decision of the Council of State as a basis of their operation.

However, in response to this finding STUK later provided the authors with the following list of objectives:

- To maintain guides in relation to event investigation and operating experience utilisation activities, and by means of them to support and direct licensees' operations in this area without limiting their own development initiative.
- To ascertain that licensees have adequate practices for investigating operational events and utilising operating experiences. This is to be achieved by inspecting licensees' event reports and by comparing their results with the results of STUK's own investigations.
- In accordance with licensees' own objectives, to identify sufficient corrective measures and to ensure that events do not recur.
- To find out whether STUK's activities or their deficiencies have contributed to the initiation of occurred events, and to use that information to improve STUK's operations.
- To inform the public on occurred events both in Finland and internationally.

Those goal were not included in YTO 7.4 or any public document at the authors' disposal. This was also admitted by one inspector who also reckoned that it should be corrected.

The interviewees were also unable to provide a clear and concise description of STUK's policy or approach to pursuing its objectives. On the one hand, they stressed that instead of "over-regulating" licensees' daily activities they would rather concentrate on setting standards of operation and identifying major deficiencies to be corrected. On the other hand, they did not quite seem to rely on the licensees' willingness or capacity to take care of their duties in a proper manner without exten-

1 *Finnish Centre for Radiation and Nuclear Safety* is the previous name of the Finnish regulator, STUK, today known as *Radiation and Nuclear Safety Authority*. The acronym STUK comes from *Säteilyturvakeskus*, the Finnish name.

sive guidance from the regulatory body. These contradictory findings can be partly explained by the fact that STUK has got very encouraging as well as discouraging experiences concerning the way operational events are investigated and acknowledged in Finnish nuclear power plants. It can be concluded that this diversity may make it rather difficult to adhere to any kind of predefined regulation policy in practice. Nevertheless, STUK's investigation activities are based on the reporting system defined in YVL 1.5, and especially on the inspection of licensees' event reports. The interviewees stressed that the power companies have the main responsibility for investigations and the utilisation of investigation results, and that it is STUK's duty to make sure that power companies' activities comply with the law and the YVL guides. They also said that STUK and power companies aim at the same target although their stake in the investigation process is different.

STUK does not have any explicit indicators for assessing the adequacy of its own event investigation activities. It was reckoned that such indicators could in principle be based on the impact of STUK's activities on plant operations but the task of developing explicit performance indicators was considered very demanding and difficult by the interviewees. According to the authors' conclusion this difficulty may in part be related to the lack of specific goals of operation. When this impression was later presented to the representatives of STUK they replied that the problem had more to do with the difficulty of assessing effectiveness by means of quantitative tools in general rather than lack of goals. They also claimed that they *do* have specific goals of operation although they were not documented in YTO 7.4.

The interviewees pointed out that in spite of the absence of explicit performance indicators STUK is actually paying attention to the influence of its activities on a more qualitative basis. For instance, they said that in many cases STUK's intervention has resulted in significant and sustainable improvements at plants, and that one clear sign of such improvements is the degree to which the utilities engage in new self-initiated development activities. It was generally agreed that in the future the indicator system could possibly be built to measure such enhancements on site. Another quantitative indicator proposed in the interviews was the amount of various clearance requests submitted to the utilities where a low number of requests would indicate good performance. Those proposals were, however, not operational at the time of this study. Nevertheless, STUK did monitor the efficiency of its administrative processes, e.g. handling times for operational transient reports received from nuclear power plant.

4.1.2 Organisation and liabilities

STUK's regulatory activities are organised around four major departments: Nuclear Waste and Materials Regulation, Nuclear Reactor Regulation, Radiation Practices Regulation, and Research and Environmental Surveillance. The Nuclear Reactor Regulation Department is responsible for monitoring the safety of Finnish nuclear power plant operations (Fig. 9).

The Nuclear Reactor Regulation department consists of six branches the special areas of which are reactor and systems engineering, radiation protection, risk assessment, mechanical engineering, electrical and I&C systems, and operational safety. The Operational Safety Branch (KÄY) has the responsibility for the day-to-day supervision of plant operations and the investigation of safety significant operational events.

4.2 Investigation practices

4.2.1 Monitoring and recording of operational events

STUK monitors operational events at nuclear power plants by means of resident site inspectors and a formal reporting system described in YVL 1.5. In general terms, all operational events shall be reported to STUK on a regular basis in daily, monthly, quarterly and annual reports. In addition, every six months the licensees shall submit a summary report to STUK on the activities taken to utilise the operating experience gained at own and other nuclear facilities. The inspection of daily reports in on KÄY's responsibility (YTO 7.4).

On the other hand, the licensees are obliged to report on all special situations or incidents that have, or may have, importance to the nuclear,

personnel or radiation safety. This is done on event basis by means of special, reactor and turbine scram as well as operational transient reports.

A special report shall provide a comprehensive description of the incident containing information e.g. on the operational condition of the plant at the beginning of the incident, course of events and their consequences, safety implications, direct and root causes, and proposed measures to avoid the recurrence of similar incidents in the future. The reporting requirements given YVL 1.5 itemise the following situations as examples of incidents that necessitate the compilation of a special report:

- plant or general emergency situation,
- violation of the technical specifications or a shutdown imposed by a requirement in them,
- actuation of the emergency core cooling system or containment isolation, or unsuccessful launching of a protective function,
- defect of a system or component characterised e.g. by increased radioactivity of the reactor coolant, an exceptional leakage in the primary circuit, decreased availability of a safety function, or a repeatedly observed error in an important instrument related to a safety function,
- deficiency in safety assessment concerning the estimated value of the reactor multiplication factor, the possibility of an unplanned criticality inside or outside the reactor, or an observation in an accident analysis which may affect the safety of operation in some situations,
- radiation incident relating to an uncontrolled leakage of radioactive substances inside the plant, individual radiation doses exceeding the dose limit, or radioactive releases to the environment that necessitate corrective measures,
- external incident, e.g. an exceptional natural phenomenon or other external threat, fire or explosion on site, or loss of off-site power,
- other incident relating e.g. to a damage of a fuel bundle, an intentional safety threat to cause damage to the plant, a significant defect in the physical protection arrangements, or defects in the nuclear material accounting, transportation, storage or disposal.

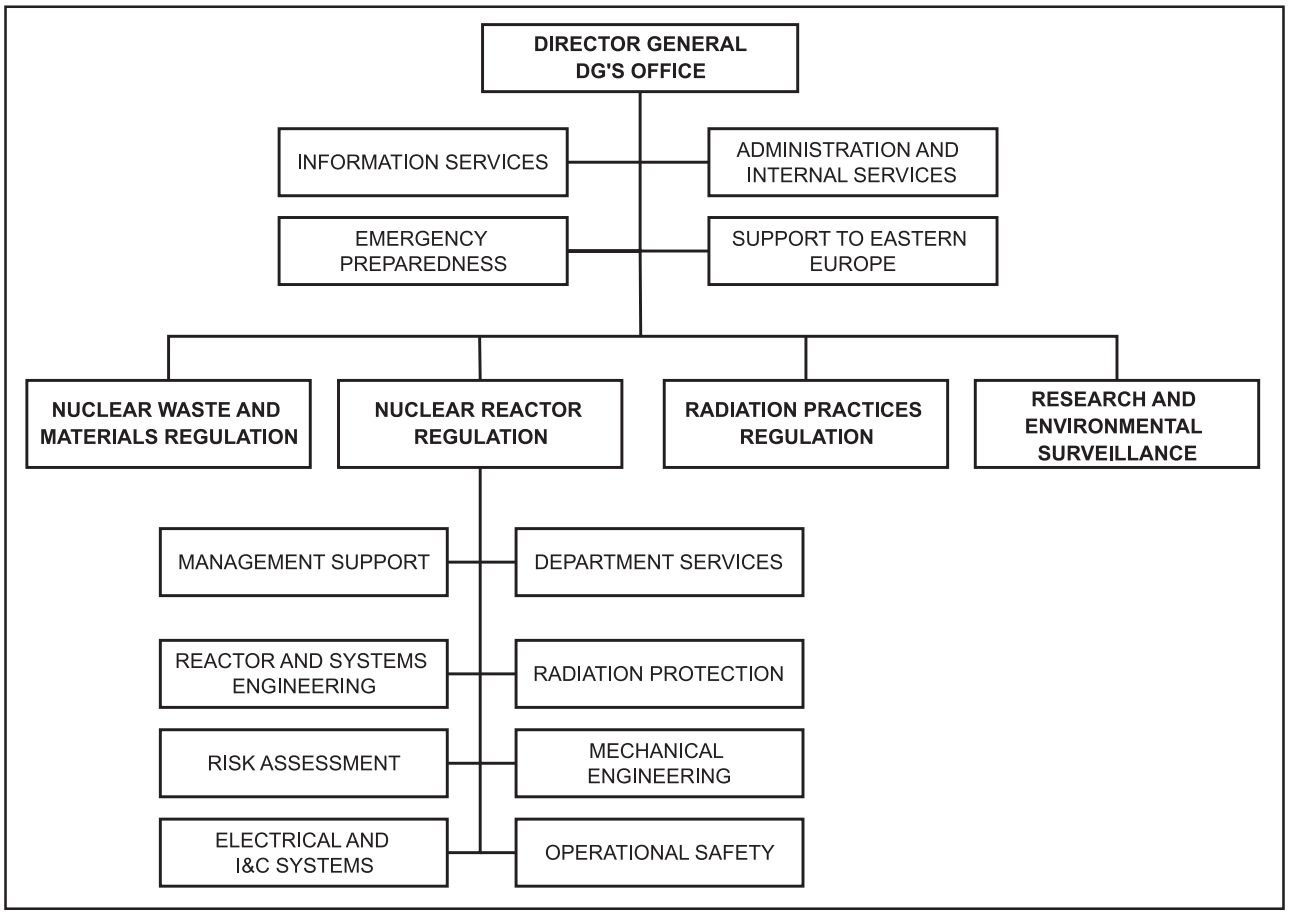


Figure 9. *The organisation of Radiation and Nuclear Safety Authority.*

In case of a significant operational event, e.g. an event classified at INES level 1 or higher, STUK shall be immediately informed by telephone or other feasible means (YVL 1.5). Contact persons at STUK and plants can be reached 24 hours a day. That information will be submitted to the head of the Nuclear Reactor Regulation Department, too.

In February 1999 STUK had two resident site inspectors at Loviisa nuclear power plant and one site inspector at TVO. An appointment of another site inspector at TVO took place in April 1999. Site inspectors spend most of their time on site which they come to know very well during their long appointments. The idea of having two inspectors at each plant is to increase their competence by allowing them to concentrate on different aspects of plant operation and equipment. Site inspectors have a free access to all plant data, and they have a key role of representing the regulator at plant during outages and other special situations. According to the interviewees site inspectors' role in ascertaining a steady flow of information is of great importance to STUK's supervisory practice.

Nevertheless, the monitoring of operational events is also very much based on plant personnel's own activity on site. Therefore, STUK encourages the personnel to pay attention to unusual phenomena and to openly report all safety significant observations, including errors made in own work. STUK also stresses the importance of recording the essential case specific data about operational events and the conditions during their occurrence (YVL 1.11).

4.2.2 Assessment and screening of operational events

KÄY is responsible for the assessment and screening of operational events in Finnish nuclear power plants. In principle, all regular reports as well as operational transient and reactor scram reports are submitted to STUK as a notice whereas special reports need STUK's approval. The head of KÄY will read all the reports. Reports are also distributed to selected offices on the basis of necessary specialist know-how.

Having received information on an unusual event KÄY will first assess, together with the management of the Nuclear Reactor Regulation Department, whether there is a need for an immediate intervention and/or other swift measures by STUK. The main purpose of the initial assessment of the event it to figure out its immediate safety implications, and to evaluate its impact on the possibilities to continue operation or to start-up the plant again (YTO 7.4). As part of the initial assessment process STUK may carry out inspections on site, too. The interviewees were convinced about the competency of the department management to make sound judgements on the safety implications of reported events and to decide on necessary measures in a timely manner.

All reported operational events are discussed once a week in the regular department meeting. The head of KÄY is responsible for preparing the presentations for the meeting, and they will be discussed in the presence of department and other branch managers. Depending on the characteristics of the event, experts from other branches and departments of STUK may be consulted (YTO 7.4). According to the normal procedure, a decision on additional investigations, i.a. the compilation of the so called TAPREK form, is to be made in each month's first department meeting.

YTO 7.4 does not contain any specific directions for the *initial* screening and assessment of operational events: there are no specific criteria for STUK's intervention, nor procedure for conducting the initial assessment. It seems, therefore, that the reliability of the process is very much based on the information received from the plant (provided by the plant organisation as well as resident site inspectors) and the adequacy of individual expert judgements at STUK. The reporting practices and connections between the representatives of STUK and the power companies appear to be well established and reliable.

There is a comprehensive procedure for the screening and assessment of IRS reports. A nominated IRS co-ordinator (during the time of the evaluation an IRS working group was implemented) reads all the reports and submits the interesting ones to a selected group of subject matter experts. These people in turn will read the reports and assess their relevance to the Finnish nuclear power industry. If the findings seem to have enough relevance, a memo will be prepared and submitted to the Finnish power companies together with the corresponding *IRS* reports *for consideration*.

4.2.3 Analysis of safety significant incidents

On the basis of a proposal prepared by the Operational Safety Branch the department management will decide on the initiation of investigation and nomination of an investigation team. The nomination may take place either immediately or later in the regular department meeting. Especially in such a case that the power company's own organisation has not responded to the event according to confirmed directions or in a proper manner, or when the event is likely to result in changes in the plant design (i.e. in systems, equipment or structures) or documentation (e.g. technical specifications, operating procedures or maintenance instructions), an investigation team will be assembled. In addition, the team shall be nominated whenever the event has been classified at INES level 1 or higher. (YTO 7.4.)

The main objective of STUK's inspection team is to find out the root causes of the incident and to define necessary corrective measures (YTO 7.4). The power company is also supposed to carry out its own studies e.g. to identify how and why the incident took place, to assess its safety significance and rate of occurrence, and to propose corrective actions. Those results together with all the necessary supporting documentation and event data shall be submitted to STUK (YVL 1.11). STUK's inspection team will scrutinise the report and conduct its own inspections on site. The team will pay special attention to:

- measures taken by the licensee to investigate the event,
- carrying out of root cause analyses and safety assessments,
- immediate and long term corrective measures,
- similar events in the past and corrective measures in relation to those events, and
- impact of the event on STUK's supervision (YTO 7.4).

STUK's incident analysis method is based on the use of a specific data collection form. The form was created in 1992 on grounds of "best possible knowledge, experience and references available at the time" and it was upgraded in connection with the introduction of a new computerised event register database system (TAPREK) in 1996. The form shall always be completed when the department staffing meeting considers the incident to have specific safety significance and when at least one of the following six registration principles has been fulfilled:

- INES level greater than or equal to 1,
- special report has been prepared of the incident,
- the incident relates to a significant organisational failure,
- the incident relates to a significant change or defect in a plant component,
- the incident relates to a significant change or failure in plant operation, or
- the incident relates to a common cause failure mechanism (YTO 7.4).

The inspection team will fill the form as part of the analysis process. The team usually consists of two or three principal inspectors and one case officer. Principal inspectors are selected on a case-by-case basis, taking into account their areas of expertise and the nature of the incident. The case officer usually comes from KÄY, and it is on his or her responsibility to provide the team with methodological support and to make sure that the case will be adequately completed. One of the main duties of the case officer is to help inspectors convey their findings in a clear and precise manner and to make the investigation report readable and understandable for other members of STUK's organisation.

In most event cases there will be no inspection team but the TAPREK form will be nevertheless completed. This may be the case e.g. if the causes of the incident are obvious but there is a reason to pay special attention to the implementation of remedial actions and to enter the information into a computerised database.

The data collection form aims at directing inspectors' attention to the essentials of the concerned incident and providing them with a certain viewpoint to possible influence mechanisms and performance shaping factors behind the course of events. Therefore they are supposed to use the form from the very beginning of the analysis. The completion of the data collection form is to be done on the computer, and the system will automatical-

ly store the information in STUK's event register database, TAPREK. Once the form has been completed, it will be printed and the inspection team members will sign it. After this the original paper print will be filed. The results of the study ought to be brought up for discussion in the Operational Safety Branch. (YTO 7.4.)

The interviewees were very satisfied with its present contents and structure. A detailed description of the data collection form and its use is given Chapters 7.1 and 7.2 in connection with the analysis of selected cases and inspection reports. For an example of the treatment of organisational factors in the form, see Appendices.

In many cases the power company has already submitted its own investigation report to STUK before STUK decides to carry out further inspections. Therefore, those (operational transient, reactor scram, special and root cause analysis) reports are an important source of information for STUK's investigation practice. However, the interviewees pointed out that STUK does not take power companies' findings and conclusions for granted but strives for its own interpretation of the course of events. STUK may also end up with different conclusions "and often does" as one of the interviewees reckoned and continued that "a completed data collection form can by no means be considered as a copy of previous power company reports".

In addition to so called "ordinary" event inspections based on the use of the data collection form STUK occasionally conducts comprehensive in-depth investigations for selected cases. About 10-20 % of the cases stored in TAPREK have been subject to that kind of special investigation. The special investigation usually proceeds in parallel to the compilation of the data collection form with no standard method or procedure. According to the interviewees they present the best possible know-how available at STUK. In the 1990s STUK has completed around 20 special investigation reports.

4.2.4 Utilisation of investigation results

According to STUK's internal directions given in YTO 7.4 the incident analysis process shall itemise requirements for corrective measures to be implemented by the licensee. As part of the inspection those measures shall be listed in the data collection form. According to the interviewees the data file will be kept open while the planning and implementation of required improvements is in progress. However, the guide does not provide any kind of description of the follow-up process to support and supervise those activities, nor did the interviewees specify how does it happen in practice. The licensees themselves are nonetheless required to have written instructions for the processing and implementation of proposed recommendations (YVL 1.11).

4.2.5 Data administration and analyses

STUK's archive contains all the reports prepared by the two Finnish power companies and submitted to STUK since the beginning of the Finnish nuclear program. The computerised TAPREK system contains all special reports and operational events classified at INES 1 or above from the year 1977. In addition, all data collection form based reports prepared by STUK have been entered into the system since its introduction in 1992. Special investigation reports are not in TAPREK because they comprise drawings, calculations and different kind of original documentation that are not in electrical form.

In connection with the processing of a new operational event the inspection team should search for indications of corresponding events or failure mechanisms in the past. Such an indication should also result in a reassessment of the event's rate of occurrence and an evaluation of previously proposed corrective measures and their effectiveness. It was estimated that this objective is met at least to a certain degree, depending on the case officer's initiative and personal commitment. However, there is no regular procedure or practice for analysing the bulk of event investigation data to identify common case failure mechanisms in a more systematic way. STUK's internal directions do not contain any instructions on the compilation of statistics or the carrying out of further analyses for recorded failure data, either. The licensees themselves are, however, required to have written instructions and adequate arrangements for such procedures (YVL 1.11).

4.2.6 Reporting

The decision on informing the public and international organisations on operational events at Finnish nuclear power plants is made by the management of the Nuclear Reactor Regulation Department of STUK. According to STUK's directions INES level 0 events are to be reported on grounds of a special reason only. Operational events classified at INES level 1 or higher shall be reported to the radiation news. All operational events classified at INES level 2 or higher shall be reported to IAEA within 24 hours. Events that are to be classified later due to a need for additional information and research shall be addressed in STUK's Quarterly Report on the operation of Finnish nuclear power plants. A press release is usually issued in relation to all safety significant operational events, too. (YTO 7.4; YTO 7.5.)

4.2.7 Self-assessment on strengths and weaknesses

The interviewees told that STUK's investigation practice has developed a lot since the foundation of Operational Experience Branch, the predecessor of the Operational Safety Branch, in 1992. They were of the opinion that it had had a positive impact on power companies' investigation practices, too, because "the branch forced them to try harder". However, the most recent organisational change at STUK in 1997 may have been an adverse movement in this respect. The interviewees claimed, namely, that the number of their duties has increased which in turn seems to have resulted in a loss of focus and efficiency. Says a senior official: "It is another thing to have two fully competent man to solely concentrate on event investigation than to deal with one hundred different tasks of which event investigation is just one among others". They also estimated that the number of special investigation reports is about to decrease due to the current division of tasks and duties. The problem is, therefore, that the officials do not consider to have enough time or possibilities to conduct ordinary inspections in a proper way. This, in turn, is likely to decrease the quality of long-term research activities. On the other hand, the interviewees pointed out that once an inspection team is organised it will be granted all the necessary backing and focus. And they did *not* claim that the quality of completed inspection reports had been degraded **so far**, either.

Another problem reckoned during the interviews related to the use of the data collection form. It appeared that officials working at other branches than KÄY did not always utilise the form as efficiently as intended: "... they are filled out for the bureaucracy's sake, and supplemented later". This was in part attributed to deficiencies in STUK's culture and management.

According to the representatives of STUK they still have a lot to learn in the field of human factors. They stated that STUK as well as the power companies do not have enough competence to analyse human behaviour induced operational events and failures in a proper manner. A solution proposed during the interviews was the recruitment of human factors specialists who could fully concentrate on the issue. So far STUK itself had relied on engineers in this respect, although under the recent years a small number of behavioural scientists have been working on other assignments at STUK.

4.3 Operational preconditions

4.3.1 Human resources and training

Despite the problem of missing focus in the event investigation practice the interviewees were of the opinion that they have enough competent personnel to take care of their duties. As most nuclear organisations in the world they also had to cope with peaking workloads and unexpected assignments which call for an ability to prioritise tasks and duties.

Learning is mostly based on hands-on training on the job. New interested inspectors are encouraged to join in the investigation practice as team members. STUK's inspectors have also attended MTO and ASSET courses in Finland and abroad.

4.3.2 Manuals and instructions

STUK's internal directions on operational event investigation are given in YTO 7.4. At the moment of this study the guide was under revision, mainly

due to the previous organisational change. The guide as well as related YVL-guides were generally considered to be of high quality and adequacy. The major function of YTO 7.4 is to assist inspection team members in the compilation of the data collection. The form and the guide appear to correspond very well to each other.

4.3.3 Information systems support

The basic data concerning safety significant operational events at Finnish nuclear power plants together with the investigation results end up in a computerised event register database, TAPREK. The first computerised event registration system was introduced in 1992, and it ran on the famous VAX computer. The present PC based system was introduced at the beginning of the year 1996. The data is stored in a relational database that can be accessed by a menu-driven graphical user interface. The interface supports multiple criteria queries. At the time of this study the system was being upgraded to Windows NT operating system.

TAPREK runs on STUK's local area network and is accessible from ordinary desktop computers. All the officials have been authorised to make queries and read the inspection reports stored in the database. Inspection team members may change the contents of their own reports until the reports have been completed and the corresponding files have been closed. Both open and completed reports can be retrieved from the database.

In connection with the introduction of the new system all the officials had an opportunity to attend special courses. People were sitting in front of their computers and played with the program while the lecturer, the main programmer of the system, provided them with necessary support and background information. The representatives of STUK seemed to be rather satisfied with TAPREK in terms of its functional features and usability. The interface appeared to be clear and easy-to-use.

To a certain degree TAPREK does support data analyses due to its clear user interfaces and the sophisticated event classification scheme built in the data collection form. In practice, the search of common cause failure mechanisms calls for patience, numerous data retrieval operations and profound familiarity with the system. It is apparent, however, that instead of the system itself the absence of well defined investigation result utilisation procedures is the main impediment for better results in this field.

4.3.4 Reviews and development activities

The first quality manager was appointed to STUK in 1998. In relation to the emerging quality assurance function STUK has already evaluated its instruction maintenance procedures. However, STUK's event investigation practice has not been subject to any deliberate review or audit before this study.

It appeared that STUK has had some difficulties in its efforts to initiate and foster internal evaluation programmes. Those difficulties related e.g. to the functioning of the predecessor of the Operational Safety Branch, i.e. the Operating Experience Section, the main duty of which was to analyse incidents and to pay explicit attention to STUK's deficiencies in connection with investigated cases, too. In particular cases the identification of deficiencies in other offices' activities had raised resistance within the organisation. According to one interviewee this was one reason for the close-down of the *section* and for the introduction of the latest organisational change.

Criticism is still allowed e.g. by means of the TARPEK form overlay that has a specific field for "effects on STUK's activities" (item 16). However, in only one report (No. 108/21.11.93) of altogether 17 TAPREK reports reviewed as part of this study such effects had been identified.

5 TEOLLISUUDEN VOIMA OY

5.1 Managerial framework

5.1.1 Goals, policies and performance indicators

The main objectives of Olkiluoto power plant's (hereinafter referred to as TVO) event investigation practice are to produce information to support plant operations, to prevent the recurrence of identified events and failures, and to report to the regulator (STUK). According to TVO's internal directions, special attention is to be paid to reducing the number of operational transients and reactor trips. In relation to these objectives, TVO emphasises the importance of investigating prevailing practices and existing operating experience, conveying the lessons learned to the right persons in TVO's organisation, and processing feasible modification proposals swiftly. (0-S-O-16/2.)

According to the interviewees, TVO's investigation policy is based on the principle to carry out event inspections by subject matter experts in concerned organisational units to the degree it is reasonably practicable. This was regarded as a natural way to integrate the best possible specialist knowledge into the investigation practice. In connection with this objective, both the Operational Safety Branch and the Group for Operating Experience, i.e. the major stakeholders in the event investigation and follow-up processes, function as expert functions to co-ordinate and supervise related activities at TVO.

Identified problem areas are to be tackled by means of specific development campaigns. These campaigns were introduced as part of efforts to increase the efficiency of investigation result utilisation activities. Usually the question is about an intensified treatment of pending statement requests in selected offices and branches (see also ch. 5.2.4).

Because Olkiluoto power plant was designed and commissioned by ABB-ATOM, TVO works in close co-operation with Swedish utilities in general and especially with its sister plants Forsmark 1 and 2. In addition, TVO has been relatively active with international nuclear energy organisations such as WANO where TVO is a member. Many of these joint projects and exercises relate to the evaluation and development of TVO's event investigation methods and practices. An overall impression is therefore that TVO is in the process of strengthening its competence in this area.

According to the interviewees, the recurrence rate of identified failures and defects would probably be the best measure for the adequacy and effectiveness of the event investigation practice. They said that recurrence is an important performance indicator at TVO and that it is being explicitly followed, too. During the interviews it appeared, however, that in relation to recurrence current statistics covered only major plant level events (such as reactor trips and unplanned production losses) while more precise figures on recurrent failure types were said to be missing or incomplete.

KÄKRY has a specific indicator for its own operational efficiency. Its value is determined by the number of new events included into their follow-up list of open cases, as well as the number of cases completed (and removed from that list) during the same period of time, at present one calendar year. However, the interviewees claimed that this throughput capacity indicator did not necessarily tell the whole truth about KÄKRY's efficiency. They said that its value was largely determined by the degree to which the rest of the organisation was able to proceed with the enquiries and recommendations they had issued in connection with their investigation and follow-up activities.

It is probable that e.g. in the long run the reactor trip rate will be inversely proportionate to the effectiveness of the operational experience utilisation process. However, it is the whole organisation and all the activities together, not only the event investigation practice, that are responsible for such things as plant performance. Therefore, and especially from the inspectors point of view the feedback provided by high level plant performance indicators may be too general and impractical to support concrete improvements in event investigation related activities. This leads to the conclusion that there are no *particular* performance indicators for evaluating the adequacy and effectiveness of applied event investigation practices. TVO's representatives were of the opinion, however, that it may be very difficult or even impossible to define a single indicator for that purpose and that in practice evaluations will have to be based on several and different kinds of information sources. In general, both the interviewees and the authors of this study agreed that performance measurement is a very challenging topic without clear-cut answers.

5.1.2 Organisation and liabilities

The activities of Olkiluoto power plant have been organised in three major departments: Production, Engineering and Finance. Both the Production and Engineering Departments comprise eight offices (Power Plant Engineering being a kind of administrative unit to co-ordinate the activities of four engineering offices in the Engineering Department). The Nuclear Safety Office belongs to the Engineering Department, too. Some offices in both departments are still divided into smaller branches. For instance, the Nuclear Safety Office has specific branches for Operational Safety, Reactor Safety, Reliability, and Radiation Safety. TVO's organisation is outlined in Figures 10 and 11.

The major responsibilities in connection with the operational experience utilisation process at TVO are held by the Nuclear Safety Office (TR) and its branches in the Engineering Department, the Operations Office (KK) and its branches in the Production Department, and the Group for Operating Experience (KÄKRY), an inter-departmental task force involving six members from three different offices in the Production as well as Engineering Departments. The Head of the Nuclear Safety Office reports to the Engineering Manager, i.e. his immediate line manager, and also to the TVO Safety Committee. The Head of the Operations Office reports to the Production Manager. Production and Engineering Managers report directly to the Managing Director of TVO. KÄKRY reports to the Plant Meeting and the Safety Com-

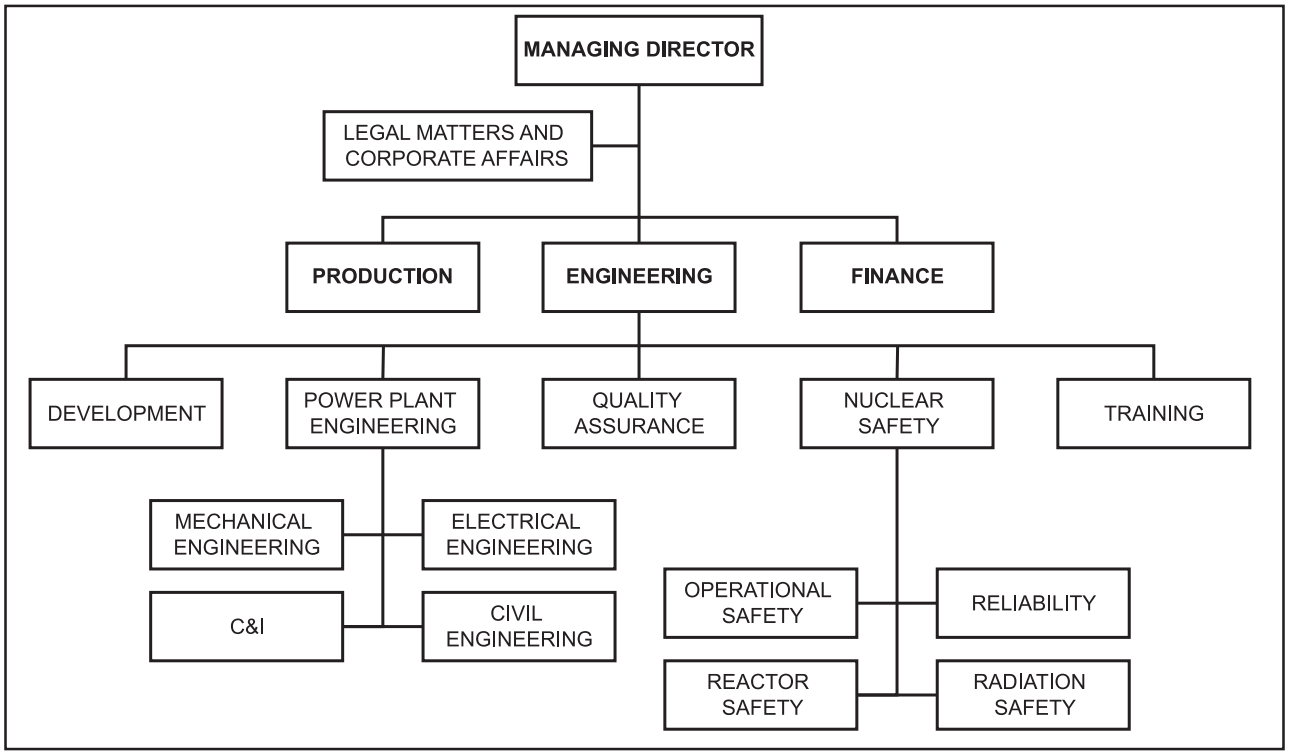


Figure 10. *TVO organisation chart. The Engineering Department.*

mittee (0-S-O-16/2). KÄKRY does not have a formal position in the line organisation.

TR has broad responsibilities relating to the assessment and inspection of operational events including the examination of identified operational transients and damages, inspection of completed operational transient, reactor and turbine trip reports, compilation of special reports, arrangements for the circulation and handling of special reports at TVO as well as for their submission to the regulator, co-ordination of root cause analyses, co-ordination of investigation activities in relation to external incidents, and introduction of measures to enhance operational experience utilisation. Most of these duties are carried out by the Operational Safety Branch (TRK) of TR. In general, TR is liable for the safety review of all the reports that relate to operational transients or other special situations. (TVO Ordinance, ch. 5.)

The Operations Planning Branch (KKK) of KK has the general responsibility for the planning and monitoring of plant operations, supervision of testing and operability activities in systems and equipment, identification of LCO related deviations from the Technical Specifications, and supervising the implementation of approved modifications, enhancements and changes in operating procedures. In addition, KKK co-ordinates investigation activities that relate to TVO's internal operational events (TVO Ordinance, ch. 5).

KÄKRY has three representatives from TR (KÄKRY's chairman is also the Head of TRK), two from KKK and one from the Training Office. KÄKRY is responsible for the handling of significant operational events, both internal and external, that have been reported and brought to its consideration. KÄKRY's main objective is to collect and assess existing operating experiences and to help transform that information into organisational learning and practical enhancements by recommending further actions and following their implementation. The actual operative responsibility for the implementation of approved measures lies in the concerned organisational units. In this respect KÄKRY has no formal authority. Nevertheless, if they are not satisfied with the progres-

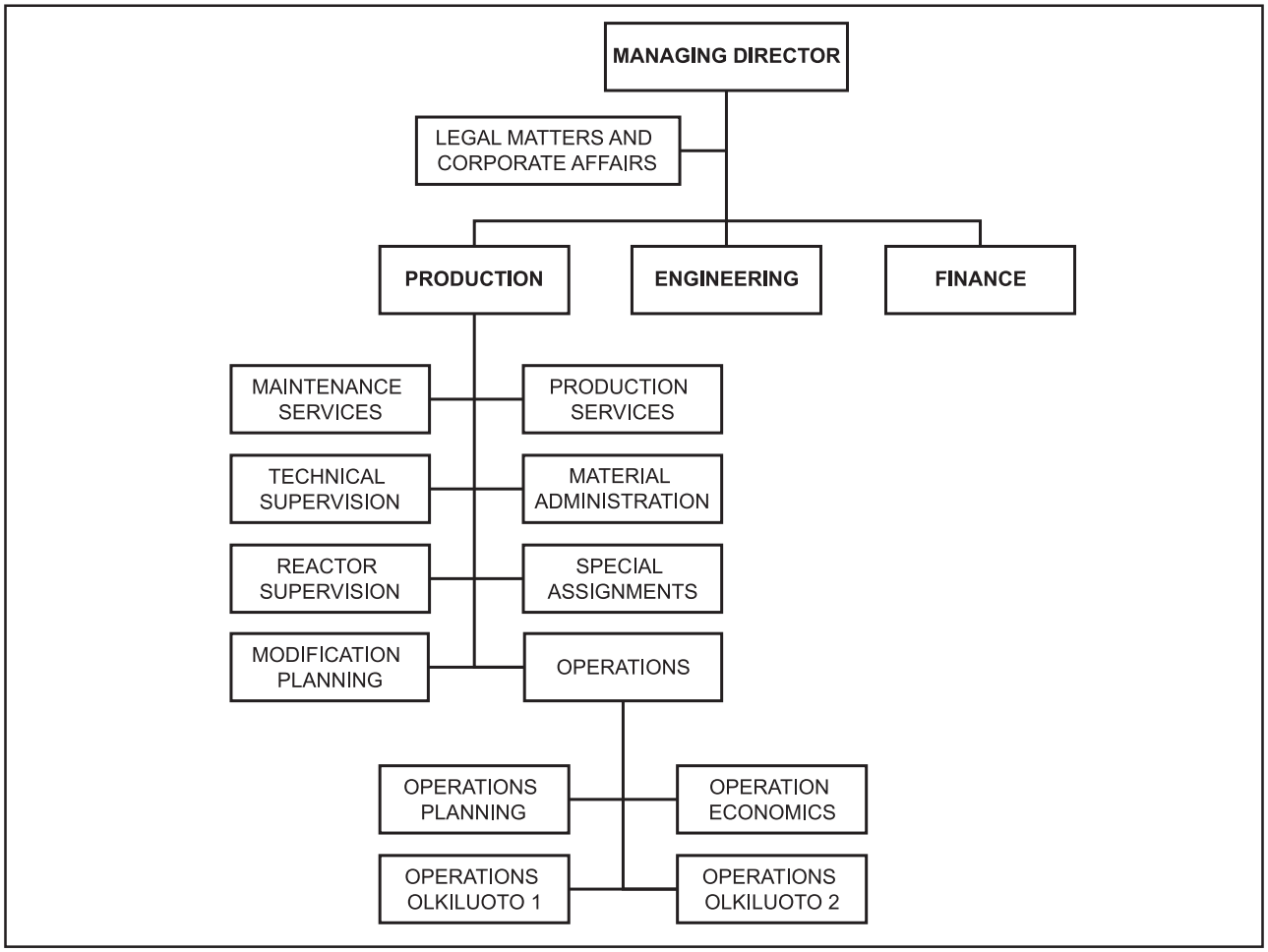


Figure 11. *The Production Department of TVO.*

sion of work they can appeal either to the Plant Meeting or to the Safety Committee and bring their concerns up for discussion.

All special and root cause analysis reports and proposed enhancements related to those incident reports are handled either in the TVO Plant Meeting or in the Safety Committee. The Plant Meeting is responsible for discussing the safety implications of reported deviations and consequential modification needs to plant systems, procedures or the Technical Specifications, monitoring ongoing modification projects and issuing recommendations to the Production Manager. The Safety Committee concentrates on the drafting, execution and supervision of general safety and operating principles by giving recommendations and statements in nuclear safety and quality assurance related matters. The recommendations of the Safety Committee are mandatory and can be overruled by the decision of the Managing Director only.

In general, TVO's management structure in relation to event investigation activities is rather decentralised. Responsibilities appear to be defined in great detail, but dispersed in several branches, groups, meetings and individuals. A great deal of related progressive failure analysis responsibilities were assumed by the Nominated Responsible Engineers (maintenance and operability foremen) in charge of particular equipment and systems. Individual accountability was being emphasized. It was concluded that the practice as a whole lacked process characteristics and that the situation posed therefore challenging demands for the co-ordination of activities and the utilisation of existing knowledge at TVO. According to the authors' impression this view was at least partly-if not unconditionally-supported by some representatives of TVO, too. The interviewees pointed out, however, that the decentralisation of responsibilities and activities was created by purpose and that the line organisation was nevertheless competent of taking care of event investigations in an appropriate manner as part of its normal operation.

During the carrying-out of this study TVO made some changes in relation to its distribution of liabilities and job descriptions. TVO reappointed the previous head of TRK who, like his deputy, also became the Chairman of KÄKRY. The immediate objective of the new Chairman was to assume a larger overall responsibility for TVO's event investigation practice and to intensify the co-ordination of related cross-functional activities. These most recent measures were clearly aimed at emphasising the process nature of the practice and developing the process ownership concept at TVO.

5.2 Investigation practices

5.2.1 Monitoring and recording of operational events

According to TVO's safety and quality policy all the employees are obliged and encouraged to report on their own failures and other observed deviations on site. This is usually done by reporting to the immediate line manager. The actual event recording practice consists of different reporting procedures and tools depending on the nature of the event.

The Operations Office and its branches have the major responsibility for the monitoring of plant operations and reporting on operational transients. The Operations Branch of the concerned unit (Olkiluoto 1 or Olkiluoto 2) is liable for the compilation of operational transient and reactor trip reports. Report drafts shall be submitted to the Heads of KKK and TRK for inspection, and to the Head of KK for approval (0-KC-00-47/8).

Observations of defects in plant components (i.e. systems, equipment or structures) that require repair shall be entered into the computerised Work Order System (TTJ) as notices of defects. Dominantly such defects that do not necessitate formal reporting to the regulator in accordance with YVL 1.5 are entered into the system. These defects may have and have in a number of cases also importance to safety or availability It is characteristic of a defect that it has either resulted in a malfunction or breakdown of a device or structure, or that it has potential for doing so under certain circumstances (latent failure). TTJ also contains corresponding work orders, failure reports and related supplementary clarifications. Compared to events reported by means of operational transient, reactor trip or special reports, failures entered into the TTJ system are numerous and dominantly of minor safety significance.

If the failure significance is classified as an immediate Limiting Condition of Operation (LCO), the failure shall be reported in the plant quarterly report to STUK in an inspection report description similar to foreign Licensee Event Reports (LER) after initial notification in the daily report.

In case of a non-technical failure, e.g. a wrong order or procedure, there are various possibilities depending on the context or consequences of the incident or error. Different reporting practices exist e.g. for process near-misses, labour accident and protection deficiencies, outage related events, and deficient instructions. There was no general purpose form overlay or procedure for the recording or treatment of such cases, except the established updating routine of changes in operating procedures. The process near-miss reporting appeared to be a relatively new practice at TVO.

TVO has two nominated responsible engineers (NREs) to monitor existing operating experience. One is responsible for internal (NREI) and another one for external (NREE) operational events. They were responsible for bringing up operational events and important deficiencies at Olkiluoto NPP as well as in other nuclear facilities for discussion in KÄKRY. The NREE was also the Chairman of KÄKRY and the Head of TRK at the time of this study.

The deputy Head of TRK told that TVO as a whole did not have particularly well co-ordinated or disciplined procedures for the recording of deviations which, in his opinion, made it difficult to handle all available information. Given the large number of possible information sources and reporting formats his comment did sound understandable. However, the Head of TRK did not share his deputy's view in this matter[2]. The authors' impression is that while important operational events and "ordinary" technical failures are likely to be detected and recorded in a reliable manner, the case with those observations and events that cannot be easily classified into any particular category is not that clear. This also relates to the further assessment of those cases (see the next Chapter).

5.2.2 Assessment and screening of operational events

KÄKRY is responsible for the assessment and screening of operational events at TVO. Most of the cases discussed in KÄKRY are provided by the two NREs responsible for internal and external events. However, anyone at TVO's organisation may propose a case of his or her selection to be considered in KÄKRY.

KÄKRY handles all operational event *reports* that relate to internal operational events at TVO (0-S-O-16/2). They include operational transient, reactor and turbine trip, special and root cause analysis reports as well as reports on failures that have resulted in an immediate LCO situation (i.e. similar to LERs). All those official event reports shall be submitted to the regulator. KÄKRY also handles major defects and failures in plant systems and equipment on grounds of their assessed importance to plant safety or availability. Those failures, including failures that have caused an immediate LCO situation, are screened from the TTJ information system by the NREI. In addition, attention is paid to process near-misses and other important observations such as outage incidents and labour protection problems. It was noted that nowadays more than half of all the cases on KÄKRY's agenda relate to such internal events that remain below the official reporting criteria specified in YVL 1.5.

With regard to external events, KÄKRY assesses Loviisa power plant's operational experience reports and all important foreign incidents. Special attention is paid to operational events that have occurred at Swedish BWR plants. Through the screening, assessment and reporting services of ERFATOM and KSU[3] TVO has access to all Swedish operational licensee event and reactor trip reports (the so called RO and SS

2 Both the current Head of TRK and his deputy participated in the interviews which were in different occasions. Since the results and conclusions of this study are largely based on the information gathered through interviewing key personnel on site, special attention has been paid to producing a true and comprehensive review of their conceptions. In some cases, e.g. in the absence of a common position, a more detailed presentation of individual views and opinions has been considered necessary for justifying the results of the analysis.

3 ERFATOM and KSU are Sweden based NPP operating experience research organisations that co-operate with utilities, major system vendors, authorities and international nuclear energy organisations.

reports) as well as to selected NRC reports. In addition, TVO gets all IRS and WANO reports (TVO is a member of WANO), and technical information from major vendors such as ABB Atom and ABB Stal. Also STUK submits all IRS reports to TVO.

In general, TVO's event recording and assessment practice of internal and external events appears to consist of three different main tracks: one operational events such as reactor trips and operational disturbances, one for technical defects and component failures, and one for other deviations and "non-technical" events[4]. KÄKRY is not responsible for all those activities since also the line organisation and its offices as well as individual system and equipment responsible foremen and technical experts have their stake in the process.

Internal and external operational events

The NREE nominates a person in charge for each new external case that is to be taken under KÄKRY's surveillance (0-S-O-16/2). His or her task is to carry out a kind of preliminary scrutiny by getting acquainted with the case and gathering more information by consulting personnel that have a good knowledge of the concerned systems, equipment or phenomena. In the next KÄKRY meeting he or she will then present the case to other KÄKRY members to initiate discussion. ER-FATOM and KSU report on their findings by means of weekly and monthly summary reports which are handled according to the same procedure. A person providing a statement will be appointed from appropriate organisational unit(s) for cases that seem to require further processing at TVO. Most important cases, e.g. major incidents, are normally presented to the Plant Meeting once the information has reached KÄKRY.

The main objective of KÄKRY is to scan through the bulk of events and observations and to assess their relevance to different technical disciplines. In practice, KÄKRY operates by holding meetings and discussing the cases on their follow-up list, requesting statements and clarifications, recommending corrective actions and following their implementation. On grounds of existing evidence it can be reckoned that events on KÄKRY's agenda are subject to a systematic screening, assessment and follow-up activities. However, this has not always been the case with *novel internal events*, e.g. observations of potential deficiencies or error situations that have *not yet* been analysed or reported by means of any formal procedure (e.g. resulting in an operational transient report). It was concluded that in this respect TVO's data acquisition and analysis activities lacked systematisation.

Technical defects and failures

There is a clear procedure for the recording and processing of defects and failures that can be easily attributed to a particular system, equipment or structure. Such defects are reported through the computerised TTJ system, and the necessary administrative liabilities in relation to repairing and reporting practices are described in great detail in TVO's procedures (i.a. in 0-KC-00-76/0 and 0-KC-U3-21/2). Each equipment and system has its own Nominated Responsible Maintenance Foreman, and he or she is responsible for the functioning of the concerned device. They carry out a great deal of TVO's data collection and assessment activities as part of their everyday duties. This decentralised system allows high technical specialisation but issues challenges for information exchange, task co-ordination and the conformity of assessment practices and results. The defects and failures that necessitate official reporting to the regulator (e.g. by means of LERs or special reports) are however brought up for discussion in the KÄKRY Screening Meeting by NREI.

Other deviations and non-technical events

When it comes to the assessment of other deviations and especially new "non-technical" events, the situation seems to be more cumbersome. It was concluded that until recently the reporting and assessment procedure for observations of potential deficiencies (e.g. inadequate working practices, planning errors etc.) that do not fulfil the

4 The categorisation reflects authors' observations and conceptions and is not directly based on TVO's documentation or official position. In addition, identified categories are not mutually exclusive, i.e. a technical failure may also result in an operational event requiring official reporting and always another kind of internal documentation and treatment.

special reporting criteria, nor relate to any specific system or equipment (i.e. technical) failure, has been defective. For instance, TVO's event investigation instructions reviewed by the authors of this study did not specify any such practices or procedures. TVO's outage and labour protection reporting practices have partly compensated this deficiency, but only partly since their applicability area is rather limited when compared to the extent and diversification of possible plant level problems and phenomena (such as organisational deficiencies etc.). However, the recently implemented process near-miss reporting practice has potential to become an efficient tool in this respect provided that it can be properly established into regular use. All process and labour protection near-miss reports and outage event reports are handled in the KÄKRY Screening Meeting.

Summary

In consequence, one could say that instead of one common recording and assessment procedure TVO had several concurrent tracks for different events and deviations. It was difficult to perceive how those tracks related to each other because there was no plant level document to illustrate their mutual interconnections. Identified deficiencies related mainly to non-transparent and complex procedures, task co-ordination and the exchange of information in relation to the assessment of technical defects and failures, and to the treatment of "non-technical" failures of uncertain safety importance (although improvement was being made). However, according to the authors' impression the assessment and classification of operational events was conducted according to the reporting requirements issued by the regulator in YVL 1.5.

The representatives of TVO had recognised some of these problems, too. The deputy Chairman of KÄKRY noted that in general the treatment of man-technology-organisation related issues has not been very systematic under the recent years. With regard to the treatment of "other deviations" TVO had reacted by developing a standard form overlay for the recording and assessment of all process errors and deviations, including those that do not require the compilation of an official event report. These measures were taken during the course of this study in 1999 and resulted in the introduction of the process near-miss reporting practice. The idea was partly based on their experiences from the recent labour protection campaigns in which near-miss incidents and safety hazards detected during outages were recorded by means of a specific data collection form and analysed afterwards. They also referred to the experience of Loviisa power plant in the appliance of so called Operational Event reporting practice (see ch. 6.2.1 and 6.2.2).

5.2.3 Analysis of safety significant incidents

According to the official reporting requirements issued by STUK in YVL 1.5, safety significant operational events and situations (hereinafter referred to as incidents) are to be investigated and reported to the regulator by means of special reports. A special report shall be prepared e.g. when the incident has importance to plant, personnel or environmental safety, or when the technical specifications have been subject to violations. Examples of such incidents are itemised in Chapter 4.2.1. Those requirements are mandatory and apply to all Finnish nuclear facilities.

At TVO, the Head of the Nuclear Safety Office determines whether there is a need for a special report. The Operational Safety Branch (TRK) will have the responsibility for the compilation of the report (0-KC-00-47/8).

According to the interviewees, inspections are conducted in teams and their members are selected on case-by-case basis depending on the necessary know-how and authority. Usually at least one subject matter expert from the Operations Office participates in the work. He or she can be e.g. one of the Branch Heads or the shift supervisor who was in charge at the time of the incident. In case of a maintenance related incident the co-ordinating foreman would most certainly be a member of the inspection team etc. The general objective is, therefore, to mobilise the front line employees, foremen and subject matter experts and to make them conduct the necessary inspections and write the report to the extent it is reasonable and possible. TRK concentrates on the co-ordination of activities and provides the necessary specialist know-how and support.

Special reports reviewed during this study appeared to be organised according to the reporting requirements specified in YVL 1.5. In short, the reports consisted of a concise summary of the incident, and sections on event description, safety assessment, cause analysis, and measures to avoid recurrence. A detailed analysis of one selected case and related inspection reports is given in Chapter 7.1.

Special reports are to be inspected by the Head of the Nuclear Safety Office (TR) and the Heads of other "concerned offices" having to do with the incident in question. Usually they involve at least the technical offices in charge of affected systems or equipment, the Operations Office in case of failures in plant operations or the operating instructions, or the Maintenance Services and/or Modification Planning Offices if the incident relates to, or has resulted from errors in repair, maintenance or modification works. Finally, the report is endorsed by the Production Manager. Each special report must be discussed in the Plant Meeting and in the Safety Committee. (0-KC-00-47/8.)

During the interviews special attention was paid to the identification and treatment of recurrent failures and common cause failure (CCF) mechanisms. According to the Head of TRK the Case Officer in charge of the report will have to conduct an assessment on the event's recurrence. In case of an operational transient or reactor trip the shift supervisor is the first one to make an assessment. If the operational event includes a deviation from the Technical Specifications the report shall also contain an assessment on possible CCF mechanisms involved in the case. The assessments are to be conducted in connection with the analysis of related data and the drafting of the report. The Head of TRK was of the opinion that the assessment worked sufficiently well.

It appeared, however, that the interviewees did not share a common view on how recurrence and CCF mechanisms were being handled at TVO. According to the authors' comprehension some interviewees did not seem to know much about the issue while others claimed that related activities were not systematic. TVO's internal event reporting instruction 0-KC-00-47/8 did not explicitly address recurrence or CCF mechanisms, either, and it did not specify those situations in which a special report shall be compiled (although a reference to the formal reporting requirements issued in YVL 1.5 was given[5]). In consequence, the authors found it difficult to form a clear picture of how historical recurrence and CCF mechanisms were actually being searched for and investigated as part of TVO's event investigation activities. When this impression was later presented to the representatives of TVO it resulted in two kinds of comments. On the one hand, it was reckoned that the issue was indeed unclear for them and that it resulted from their "inability to detect recurrent failures whereupon also the need for reporting did not exist". On the other hand, it was commented that "the criteria have been specified in the Technical Specifications and they are the same as in YVL 1.5" and that "in consequence, there should not be any uncertainties".

According to TVO's instructions a root cause analysis shall be conducted for complex incidents that have specific importance to plant safety, or relate to significant organisational deficiencies that have not been sufficiently analysed as part of other inspection and reporting practices (e.g. special reports). The main objective of the analysis is to find out those deficiencies and weaknesses in TVO's operation that need to be corrected so that the recurrence of identified incidents can be prevented. At the time of this study, MTO was TVO's root cause analysis method. (0-S-O-23/1.)

The Plant Meeting, Safety Committee or KÄKRY may decide on the preparation of a root cause analysis report. According to TVO's internal directions KÄKRY nominates the Case Officer and other inspection team members for each root cause analysis project on case-by-case basis. The Head of TRK will have the main responsibility for the initiation of the analysis and other administrative arrangements. For instance, if an external consultant is to be nominated to the post of Case Officer, the Head of TRK shall take care of requesting tenders and making contracts in accordance with the standard procurement procedure. (0-S-O-23/1.)

KKK shall have the responsibility for co-ordinating plant operations related investigations.

5 In TVO's instruction for the treatment of failure and maintenance data (0-KC-U3-21/2) recurrence and CCF mechanisms were mentioned, however.

The Case Officer is liable for making sure that the incident will be properly analysed and reported within the approved timetable (0-S-O-23/1). According to the deputy Head of TRK there were two persons at TVO who had a good knowledge and understanding of the MTO analysis and could therefore lead the project. Altogether 29 persons had attended an elementary MTO course.

At the time of this study TVO was in the process of evaluating and developing its event investigation practices and methods. On grounds of the encouraging experiences gained from the recent ASSET self-assessment (October 1997–September 1998) and peer review (November 1998) exercises, KÄKRY had decided to bring ASSET into regular use. The idea was to use ASSET for the follow-up analyses of completed event inspection reports and to laying foundations for more systematic and efficient periodic operating experience reviews. However, MTO will remain TVO's principal root cause analysis method. MTO has been and will be used for in-depth analyses of most significant incidents and operational events.

The MTO analysis procedure has been described in great detail in the instructions and includes the following phases:

- data acquisition (i.a. instructions, reports, log files, flow diagrams etc.),
- interviews,
- task analysis (how were different working stages executed, what were the major problems),
- sequence and cause analysis (the course of events in a chronological order, direct causes),
- deviation analysis (what are the differences between the concerned failure and successful cases),
- barrier analysis (the functioning of both administrative and technical barriers), and
- results and corrective measures (0-S-O-23/1, Appendix 1).

The MTO method has been originally developed from the HPES method by the Swedish utilities and KSU. MTO is a method for analysing incidents that involve complex Man-Technology-Organisation (i.e. MTO) interactions. It is based on the presumption that the human being is an integral part of any control system and that many safety and/or reliability problems result from the fact that human beings have not been taken into account in an appropriate manner in systems design, operation, or maintenance. The MTO analysis focuses especially on the identification of human and organisational factors behind the incident and aims at their removal by means of practical action proposals. The MTO report shall contain a sequence, cause and barrier analysis type of diagram to illustrate how and why the incident did take place. The idea is that the inspection results (event sequences, direct causes, deviations and breaking barriers) are embedded into the diagram to show the relationships of different contributing factors and their impact on the course of undesired events.

The Head of TRK reports on the progression of the analysis to other concerned organisational units as well as to KÄKRY and sometimes to the Plant Meeting. Once the root cause analysis report has been completed, it is signed by the Case Officer, inspected by the Head of TRK, the Head of the Quality Assurance Office (TQ), and the Heads of other concerned offices (like in case of a special report, see above), and finally approved by the Head of TR. KÄKRY maintains a list of incomplete root cause reports. TR is responsible for archiving the complete ones. (0-S-O-23/1.)

Despite the thorough root cause analysis procedure investigation practices themselves appeared to be relatively informal. First of all, a quick review of the most recent root cause analysis reports (since the year 1994) revealed that they did not contain explicit method descriptions of how the inspection process had been carried out. A reference to the MTO methodology was always given, however. Event descriptions appeared to be clear and informative but often in writing only since *graphical* presentations, i.a. the MTO diagrams, were missing from the most recent reports. In this respect the older ones appeared to be more carefully compiled. When this remark was later presented to the representatives of TVO, the Head of TRK-who had personally participated in most root cause analysis projects at TVO-commented that from an expert's point of view the use of *the MTO graphical diagrams* does not necessarily bring in any added value to the investigation process. He continued that subject matter experts do not perceive or analyse event sequences or their causes *through* such diagrams but admitted that graphical diagrams in general

may facilitate teamwork and the transfer of information to other parties. In this respect the report's purpose of use was said to determine its outfit.

Another interesting issue was the astonishingly low number of completed (MTO) root cause analysis reports: the latest report at the authors disposal was dated on June 25, 1997. The interviewees reckoned that since the interviews required by the MTO procedure are generally regarded as "displeasing", people have not been eager to resort to the method unless necessary. Another explaining factor is that one of TVO's key persons with a significant stake in the event investigation practice was on a foreign assignment for one year which resulted in a temporary shortage of trained analysts. It is therefore speculated that due to the relatively demanding, time-consuming and delicate inspection process required by MTO TVO has not carried out as many root cause analyses as it would have possibly done had the investigation procedure been a bit more straightforward and less burdensome. When asked about the degree to which completed root cause analyses had been conducted according to the formal instructions, many interviewees did not really know. They supposed, however, that the analyses were most probably conducted "in the spirit of the MTO procedure".

In general, the interviewees appeared to be fairly critical about their investigation practices. It was reckoned, for instance, that the results of the MTO analysis were all too much dependent on the author of the report. One engineer said that inspection reports have often remained on the level of "a descriptive record of events" and continued that the question of incident prevention has not been sufficiently addressed. He claimed that "further measures are of superficial nature and very concisely specified like 'more training' or 'change the instruction' and that's it". He saw much space for improvement in this respect. One the other hand, most of the interviewees seemed to be rather satisfied with the ASSET methodology especially because of its clear structure and the straightforward assessment procedure. They were excited about the adjoining software package to support e.g. event classifications and reporting of pending safety problems. They also said that the ASSET exercise revealed "all sort of new things that had not been noticed before".

The official event reporting practice, i.e. the compilation of special, operational transient, and reactor and turbine scram reports, covers the entire operating life of the plant. Root cause analyses have been carried out from the year 1992.

5.2.4 Utilisation of investigation results

All internal event reports are to be assessed in the KÄKRY Screening Meeting. They include operational transient, reactor and turbine trip, special and root cause analysis reports and LERs (i.e. reports that are also submitted to the regulator) as well as reports on other important internal deviations such as process or labour protection near-misses. The external event reports assessed in the Screening Meeting include i.a. selected WANO, IRS and NRC reports, and *all* ERFATOM and KSU summary reports that contain information i.a. on recent operational events and noteworthy operability, design and operating and maintenance practice problems detected at Swedish BWR plants.

All special reports are also presented and discussed in the Plant Meeting and in the Safety Committee. Organisational problems that have been detected during the analyses (e.g. as a result of a root cause analysis) are handled either in the Plant Meeting or in the Safety Committee.

An overview of TVO's investigation result utilisation process and KÄKRY's main responsibilities are presented in Figure 12. KÄKRY assesses completed event reports (as described in ch. 5.2.2), puts interesting ones on follow-up list(s), requests statements and further clarifications from concerned organisational units (i.e. offices and branches), recommends corrective actions and follows their implementation. KÄKRY may also initiate a root cause analysis process on the basis of its own justification.

KÄKRY's follow-up lists contain information on requests and recommendations that relate to

- significant operational transients and events that require special reporting,
- events that are to be, or have been, investigated through the root cause analysis procedure,
- defects and functional deficiencies that have resulted in an immediate LCO situation,

- other noteworthy operational experiences (e.g. outage incidents or process near-misses), and
- significant external operational events (0-S-O-16/2).

In general, the follow-up lists had a clear and informative structure. Cases were entered into tables with specific columns for case information, actions, person in charge, responsible organisation,

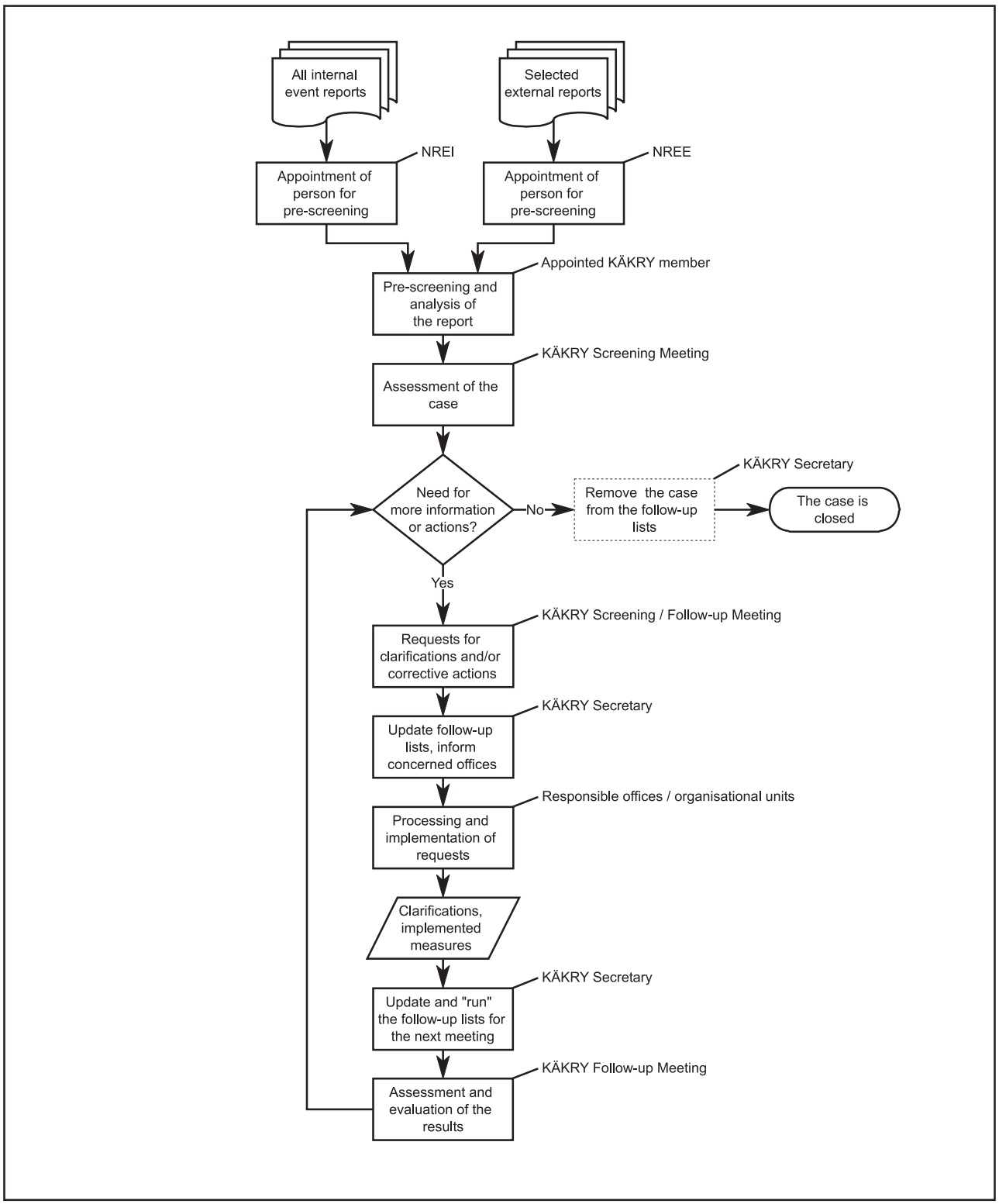


Figure 12. *Utilisation of investigation results at TVO: an overview of KÄKRY's main duties. NREI and NREE are Nominated Responsible Engineers for internal and external events, respectively.*

dead-line and remarks. The actions column contained information on necessary or already approved measures but not on their actual implementation status (the remarks column identified the closing date of the case but no explicit note on whether the corresponding measures had been actually completed was given). Events removed from the active list of open cases were deepened but still readable.

Enhancement proposals are submitted to the heads of concerned offices who will decide on the commencement of work (0-S-O-16/2). Modifications shall be handled according to TVO's plant modification procedure. Modifications in safety significant systems, plant processes or Technical Specifications, as well as significant modifications in the functioning or structure of the organisation shall also be discussed in the Plant Meeting and the Safety Committee, and endorsed by the Production Manager (TVO Ordinance, ch. 5; TVO QA Handbook, ch. 10; 0-S-O-23/1). Although KÄKRY supervises the processing and implementation of recommended actions, the concerned organisational units (offices) have the full operational responsibility for all works. At least four times a year KÄKRY assembles for a special follow-up meeting to scan through the cases on their lists and to update their processing status. In relation to the most significant issues KÄKRY has initiated the so called "top 10" list that is also regularly discussed in the Plant Meeting.

The responsibilities and practices for the evaluation of the *adequacy* and *effectiveness* of implemented *actions and* enhancements remained somewhat unclear, however. According to the interviewees implementation is followed until "there is no need for additional measures". They said that when it comes to a plant modification the case is usually closed once the corresponding Modification Proposal (i.e. the so called ME form) has been completed and approved. They noted, too, that after this the issue will be addressed again if the problem recurs whereupon also the proposed and implemented corrective measures will be re-evaluated.

It was concluded that the follow-up procedure was mainly adjusted to support KÄKRY's own administration rather than the actual implementation status or effectiveness of proposed and implemented actions. The submission of a statement request or an action proposal to a particular office is clearly a kind of break-point in the process because it is here where KÄKRY's authority ends. In principle KÄKRY could pay more attention to the actual implementation process but on the other hand one can ask if it is really worth the additional effort in the absence of more influential means of operation. Decentralised liabilities together with the lack of efficient procedures for managing cross-functional activities raise therefore questions about the effectiveness of prevailing result utilisation practices at TVO. Recent theme specific development campaigns have however alleviated this problem e.g. by providing means for reducing the backlog of pending requests and action proposals in particular offices and by providing KÄKRY with a firmer stake in the process. In addition, the developing process ownership concept may actually provide a sound basis for the management and co-ordination of cross-functional activities at TVO. Within the framework of this study it was not possible, however, to evaluate how well these arrangements work in practice. Anyway, the results of the recent ASSET exercise suggest that still more emphasis should be given i.a. to implementing remedial actions.

5.2.5 Data administration and analyses

According to the formal reporting requirements issued in YVL 1.5, each licensee shall submit an annual report on the operation of its plants during the previous calendar year to the regulator by March 1 the following year. The report shall include a description of the licensee's activities in relation to the utilisation of operational experience (e.g. initiated research and development projects) and safety studies. Such a report is prepared annually by TVO and Fortum, and it is one of their major instruments for gathering and analysing their existing operating experience.

At TVO the data analysis process (i.e. the process to analyse the bulk of investigation data) can be roughly divided into two activity areas: the analysis of *failure data* and the analysis of *existing operational event data*. In this context failure data refers to the information that is mainly stored and retrieved by means of the computerised TTJ system. It contains information (e.g.

notices of defects, work orders and failure reports) on all kinds of technical failures.

The failure reports are to be systematically followed by persons that are responsible for plant equipment and systems. According to TVO's internal directions they shall meet in their quarterly meeting to analyse the reports and to prepare a memorandum on their findings and proposed further clarifications and corrective measures. In addition, the processing status of previously requested clarifications and proposed measures shall be covered and entered into the memorandum. Special attention is to be paid to human errors as well as to the analysis of latent and recurrent failures. The memorandum shall be inspected by the Head of the Maintenance Services Office and the branch head(s) of the concerned technical office(s), and finally returned to the Production Services Office where it is filed (0-KC-U3-21/2). The former Head of TRK noted, however, that although the procedure has already been drafted "the reality and the instructions do not quite meet so far". He continued that they were in the process of putting the procedure into practice.

Twice a year failures in selected systems and components are transferred to the Nordic TUD[6] failure information database maintained by SwedPower AB (formerly Vattenfall Energisystem AB) in Råcksta, Sweden. In addition to TVO, also Barsebäck, Forsmark, Oskarshamn and Ringhals (i.e. all the Swedish NPPs) enter their failure data into the system. TVO has utilised the system to support various data analyses, e.g. in relation to the identification and assessment of CCF mechanisms in diesel generators, pressure relief valves and control rod actuators. It was concluded, however, that such analyses had been so far based on particular investigation needs rather than a regular practice.

The TUD system would provide a good basis for regular and comprehensive failure data reviews. For instance, every 2–4 years the Swedes process the failure information into a form of an equipment reliability handbook, or the so called *T-Boken*, that contains information i.a. on components' average failure frequencies and repair times, and their uncertainty distributions. TUD database is equipped with a graphical user interface to support data retrieval, classification and presentation operations, and it can be accessed directly from TVO over the Internet.

The practices to analyse the bulk of existing operational event data stored by means of operational transient, reactor and turbine trip, special and root cause analysis reports were not as clearly described as those relating to the analysis of TTJ failure data. For example, the procedure for the treatment of operational event reports (0-S-O-16/2) did not directly refer to any systematic follow-up analyses or periodic reviews. In practice the treatment appeared to be based on the compilation of various summary reports such as the annual operating experience utilisation report. In addition, TVO has prepared concise periodic summary analysis reports on reactor trips for internal working group use and identification of recurrence.

Another question is, however, to what extent possible recurrent or common cause failures can be identified by those arrangements. According to the Head of TRK the arrangements were sufficient. However, it must be emphasized that KÄKRY concentrates on the analysis of *single* event reports once they have been completed and brought to its handling-not report archives or databases-although in connection with *particular* operational events and technical failures KÄKRY had also analysed historical recurrence. Secondly, periodic summary analysis reports were not conducted on a regular basis, nor comprised any follow-up analyses (i.e. additional studies to upgrade the earlier event reports). Thirdly, TVO's operational event reports did not include any formal classification model for identified consequences, their causes or involved systems, and many interviewees did not consider that necessary, either. The authors' view is, however, that an adequate classification system would enhance the efficiency of data analyses by contributing to the identification of recurrence and CCF mechanisms, and for identification of remedial action needs, especially when the report archive grows larger.

The recent ASSET mission was however a major step forward. For the first time a large and comprehensive ensemble of completed event reports were subjected to a systematic review at

6 TUD comes from Swedish words Tillförlitlighet, Underhåll och Drift = Reliability, Maintenance and Operation.

TVO. TVO has also announced its intention to apply the method to the follow-up analysis of all operational experience reports brought to KÄKRY's consideration, and to conduct similar operating experience reviews also in the future. ASSET will enhance TVO's capabilities to detect and investigate recurrent *causes* and common cause failures mainly because of its support to event classifications and quantitative data analyses.

Some of the interviewees tended to agree with the authors' comprehension of the current situation, too. The deputy Chairman of KÄKRY confirmed that "KÄKRY does not usually analyse historical or concurrent recurrence" and continued that he did not know whether somebody else was doing it, either. He said that in the absence of a systematic practice recurrent events have been mainly identified randomly in particular situations. Another interviewee told that "we are still waiting for a more systematic follow-up procedure. In case of an event one usually knows whether there has been similar events in the past but they are not subject to any regular scrutiny".

The conclusion is therefore that until recently TVO has not had well-established and systematic practices for the identification of CCF mechanisms or recurrence in the *operational experience data*. Attention is paid to recurrence, too, but mostly in connection with particular operational events, not by means of comprehensive data analysis methods. In this respect the introduction of ASSET will however change the situation. A formal procedure for analysing the existing *failure data* did exist at the time of this study, although it was not yet fully operational and did not include detailed instructions for CCF detection in practice (recurrent causes and CCF mechanisms were however addressed in the procedure). In connection with the treatment of failure data the prevailing information technology based tools (such as TTJ and TUD) appeared to work well.

5.2.6 Reporting

Reporting to the regulator, STUK, is done in accordance with the general reporting directions given in YVL 1.5. The main characteristics of the Finnish reporting system are outlined in Chapter 4.2.1.

5.2.7 Self-assessment on strengths and weaknesses

The interviewees identified weaknesses in different areas of TVO's event investigation practice. The Head of TR said for instance that they could be better in recording deviations and bringing them to a systematic assessment. In addition, he concluded that also the inspections themselves could be more thoroughly conducted. Another deficiency related to the recognition and analysis of recurrent failures and common cause failure mechanisms. The interviewees told that they did not have systematic processes for combining the existing failure data. Thirdly, the interviewees were of the opinion that the organisation's capability to respond to KÄKRY's enquiries and proposals was not very good: "others do it very efficiently, others won't respond at all". This results in delays in the implementation of recommended enhancements. It was reckoned that this may actually mean that "people do not understand what the fundamental objectives and the value of the operational experience utilisation process actually are".

When it comes to the strengths of the prevailing situation, the interviewees said that the recent ASSET mission went well and that IAEA was satisfied with the self-assessment report. They seemed to be fairly satisfied with their experiences and the prospects of introducing the method for a regular use. In general, we were told that KÄKRY was functioning quite well and that it had got the necessary respect to take care of its duties and to get through important measures. "If the load factor remains high year after year then we are certainly doing something right." The deputy Chairman of KÄKRY concluded that "in principle the system works but more attention will have to be paid to smaller events. In addition, the response times to enquiries and statement requests need to be shortened".

5.3 Operational preconditions

5.3.1 Human resources and training

When asked about their human resource situation the deputy Chairman of KÄKRY said that their workload was not "that devastating". KÄKRY's

workload was said to be quite even because KÄKRY did not directly participate in event inspections as a team (while some of its members did). On the other hand, inspectors' workloads were sometimes peaking because they had to react on a short notice whenever something happened. In addition, they had their regular duties as well because there were no full-time employees at TVO who could solely concentrate on conducting event inspections and/or the further processing of inspection results. Therefore, a lot depends on resource allocation and prioritising.

To judge how well TVO had succeeded in this respect was not possible within the framework of this study. On grounds of statements like "I don't even know whether the event investigation practice has been assigned any specific resources or action plan" it was concluded that at least from the practitioners' point of view the practice lacked focus and resourcing although they claimed to be able to manage their duties (see the previous Chapter). For instance, the compilation of special reports was regarded as a part of TR's normal routine. According to the interviewees some help was provided by the possibility of buying services from abroad. It was estimated that the data administration and analysis services purchased from KSU and ERFATOM equal to one or two man-years each year.

Nevertheless, TVO has invested in the development of human factors expertise on site. The deputy Chairman of KÄKRY was also the Head of a Group for Human Errors. The group was founded in 1997 and consists of five relatively young employees from different offices. At the beginning, the group carried out a review and analysis of selected internal and external operational event data. The analysis focused on the characteristics of identified human errors. The group met several times and produced training materials for internal use. Nowadays they arrange training courses for other units on a voluntary basis. The general objective of the courses was not to train new inspectors but to reduce the number of human errors by helping people perceive the potential for errors and failures in their own job. The challenge is to tell people what a human error is, how they are generated, and where to look at in the immediate environment. Special attention was paid to enhancing prevailing working practices.

So far TVO has hired no academically trained behavioural scientists, however. In practice, few engineers have got acquainted with the field as part of their other duties. On special occasions TVO relies on few external human reliability consultants who know the plant well.

There is a responsible person for both MTO and ASSET methods, and they usually participate in inspections in which the concerned method is used. However, the current trend seemed to be towards ASSET. According to the deputy Chairman of KÄKRY, TVO had a dozen employees who were familiar with the ASSET software package.

5.3.2 Manuals and instructions

The general impression about TVO's instructions is that they are clear, concise and easy-to-read. They concentrate on the definition of liabilities, process descriptions are rare. We were told that this has also been the purpose. Descriptions of personal responsibility were considered very important while precise procedures were not.

When it came to the use of prevailing instructions, the interviewees' message was clear: there is no firm connection with TVO's formal instructions and the actual event investigation activities. According to the interviewees they have "separated from each other": either activities develop first after which "the instructions will be written around them", or the instructions function as "descriptions of activities or their target states". The deputy Chairman of KÄKRY compared event investigation instructions to the Technical Specifications and reckoned that while latter are being respected and complied with, the former are not so rigorously followed. He continued, however, that those two instruction are not at the same level of hierarchy at all, nor need to be either.

One of the interviewees stressed that the prevailing instructions themselves were of high quality and continued that the problem had more to do with their implementation. Another problem revealed during the interview related to the difficulty of knowing "where the instructions are and what do they include". The discussion indicated that there was a need for a kind of document management system to contain entries to all relevant instructions and to support simple data retrieval operations, such as "list all the instructions

that relate to the control of the operational experience utilisation process". One of the instructions reviewed as part of this exercise appeared to be under revision, and it was not clear to what extent its requirements were effective in spring 1999 (instruction 0-KC-U3-21/2 for the recording and analysis of failure data). The Head of TRK later specified that there has been a corresponding procedure since 1981, that it has been recently revised and that amended procedures have been commissioned. The overall conformity and coverage of TVO's instructions remains an open question since their assessment was not within the scope nor resources of this study.

TVO was not particularly happy with the requirement of YVL 1.5 according to which a special report shall be submitted to STUK within two weeks of an incident. They said that the special report is the most demanding one of all official event reports (excluding root cause analysis reports) and that in practice two weeks is just not enough for a sound treatment of such cases.

5.3.3 Information systems support

Special, operational transient, reactor scram as well as root cause analysis reports are archived as separate (Word) files. Word's Find function supports keyword searches but in the absence of a developed database solution a lot of manual work was required. However, notices of defects, work orders and failure reports are stored in the computerised Work Order System (TTJ) which supports elaborate multi criteria queries through a graphical user interface and a specific reporting tool, Business Objects. TVO has also a direct access to ERFNOVA and TUD databases maintained by KSU and SwedPower AB.

TTJ is linked to other systems that contain information on preventive maintenance and periodic testing operations. Together they form a system called the Maintenance Information System (KUPI). When asked about the utilisation of existing information systems the interviewees said that notices of defects and failure reports are to be checked as part of the event inspection procedure. It was admitted, however, that existing information systems were not always utilised in a systematic and efficient way and that a lot was based on employees' and inspectors' "gut feeling" and personal experience.

All the interviewees were of the opinion that the introduction of the ASSET programme would be a leap forward. They were especially interested in the possibility of producing KÄKRY's follow-up analysis reports with the ASSET software package, and to have an efficient tool for classifying the operational events on grounds of identified causes and consequences. Some of the interviewees also noted that if also official event reports could be produced by using ASSET the system would save a lot of time, too.

Since the TTJ system did not emphasise operational events, it was concluded that prior ASSET there has not been efficient information technology based tools to support the analysis of existing operational event data at TVO.

5.3.4 Management support

In general, the management was conceived to support the event investigation practice. However, according to the interviewees that support has *not* resulted in sufficient resources. Prioritisation and resource allocation were seen as the major problems of the practice, and to depend on the upper management decisions. Some of the representatives of TVO *seemed* to think that in the present situation the quality of their work was not at the best possible level because they had to portion out their time among several simultaneous activities. The general impression was, therefore, that the upper management was expected to provide the inspectors with greater focus and possibilities to concentrate on fewer important issues at a time.

5.3.5 Reviews and development activities

The recent ASSET mission completed at the end of 1998 and the forthcoming WANO peer review (to be carried out in autumn 1999) were seen as the most important audit projects for the time being at TVO. Prior to the ASSET mission TVO's practices for the investigation of operational events and the utilisation of operational experience had been reviewed e.g. by the Finnish regulator in 1996 (Ruuska & Rannila, 1996), and by a Swedish root cause analysis expert who is also the author of TVO's current MTO guide. An abridged

and translated version of the guide is a part of TVO's root cause analysis procedure.

When it comes to regular reviews, the follow-up report on the utilisation of operating experience is compiled annually. In addition, TVO's event investigation practice is subject to an internal QA audit every four years.

TVO's objective is to commission the ASSET method and to bring it to a daily use at the plant. This would significantly facilitate periodic operating experience reviews and provide a basis for a regular practice. At the time of this study, the ASSET procedure was being translated into Finnish. The interviewees said, too, that their intention was to try to apply the procedure for the analysis of equipment defects, erroneous instructions, and human failures.

In general, and on grounds of the recommendations of the ASSET peer review, the interviewees told that TVO aims at adjusting its investigation practices and (internal) reporting criteria to cover a greater part of such minor events that do not necessarily require the compilation of an official event report (according to the ASSET peer review report the reporting criteria for procedural and personnel failures were not comprehensive, TVO ASSET p. 17). It must be noted, however, that e.g. in 1998 more than half of all the cases on KÄKRY's agenda related to events and failures that remained below the formal reporting criteria specified in YVL 1.5 (in 1998 altogether 73 cases were addressed of which only 23 required official reporting to STUK). In addition, they aim at paying more attention to recurrent failures and to analysing the bulk of operational event data. Says an engineer: "we want to recognise and analyse the failures before their recurrence necessitates official reporting". "The problem is", he continued, "to recognise recurrence." In connection with this objective the deputy Head of TRK said that they were aiming at introducing a weekly Assessment Meeting in which all new failure reports as well as possible new significant events would be discussed and assessed by the representatives of safety, operations and maintenance functions. This was considered necessary because the current practice was too much dependent on individual activity.

6 FORTUM POWER AND HEAT OY

6.1 Managerial framework

6.1.1 Goals, policies and performance indicators

The prevention of the recurrence of identified problems was defined as the main objective of Loviisa power plant's (LPP) investigation practice. In relation to this objective, the responsible organisational unit, the Plant Safety Branch, aims at being the "collective memory" of the plant. LPP's internal directions aim at ensuring that operational experience is utilised and observed operational deviations are taken into account in a systematic way.

The concept of "deviation" is widely used in LPP's instructions. According to the official definition, a deviation is a significant defect, failure or deficiency in instructions, practices, systems, equipment, structures or the functioning of the organisation that has a degrading impact on systems availability or plant safety. It is characteristic of a deviation that operations, equipment or structures fail to comply with confirmed specifications, or the result of an operation does not fulfil given requirements. (82-12/M2.)

LPP's event investigation policy is based on cooperation between different organisational units. The interviewees pointed out that people responsible for the investigation practice avoid assuming the role of a judge or a policeman, partly because of the feedback received from other countries and nuclear facilities. Instead, the guiding principle is to decentralise activities in the organisation in a way that the people having the best possible knowledge and understanding of the concerned event and related technical challenges could join in the investigation process. This was considered a feasible way to proceed partly because of the fact that personal involvement is also likely to create better commitment to the implementation of proposed improvements. In addition, participants will have an opportunity to learn more and the investigation practice can get a good complement to its limited resources. Generally speaking, the interviewees stressed the importance of a thorough examination of operational events and the identification of factors that contributed to those events.

It was concluded that LPP's Plant Safety Branch, the body in charge of investigations, aims at developing its role towards "an internal consulting service" to provide the rest of the organisation with investigation management expertise and support in relation to inspection methods, making conclusions and communicating the lessons learned. Their way of operation was clearly based on an idea to strive for sustainable improvements by influencing people's patterns of behaviour.

LPP does not have comprehensive performance indicators for the effectiveness of its *event investigation* activities although the current practice did produce valid statistical information to support such assessments. The quantification was said to be the biggest challenge in this respect. WANO indicators were reckoned to provide some indirect feedback on the effectiveness of the whole operational experience utilisation process e.g. in the form of unplanned production losses.

Most departments and functions are subject to periodic quality assurance assessments in which the recurrence of defects, failures and deficiencies is one of the major topics. Special attention is paid to equipment and components that have to do with safety important systems and functions, such as the diesel emergency power system. Regular deviations of similar kind are regarded as clear indications of operational deficiency and inefficient or inadequate corrective measures. It was concluded that this information was being gathered and utilised in a relatively systematic man-

ner, although not processed into explicit indicators of operational excellence as noted above. The interviewees told that LPP keeps track on the number of special, operational transient and operational event (KT) reports but they did not believe those statistics to be of significant benefit to the development of a proper and reliable quality indicator for the investigation practice.

The interviewees were of the opinion that it is rather difficult to define what would it actually mean to have an efficient investigation practice. In addition, they reckoned that the results of their practice are not likely to be detectable (or influential) in the short term, either. Nevertheless, they considered their efforts successful if investigation results are efficiently utilised to support development activities and if they result in a decreasing number of previously common defects and failures.

6.1.2 Organisation and liabilities

Loviisa nuclear power plant is run by Fortum Power and Heat Oy, a subsidiary of a state-owned energy company Fortum Corporation (Fig. 13). At the plant activities are organised in five departments: Operation, Maintenance, Technical, Office, and Training Groups. Their managers report directly to the General Manager of the plant (Plant Manager). Technical Group consists of the following branches: Plant Safety, Radiation Protection, Reactor and Fuel, Quality Assurance, Chemical Laboratory, and Computer Services. Responsibility for the investigation of operational events belongs to Plant Safety Branch (PSB). The head of PSB, usually the senior member of the branch, reports to the head of Technical Group (Fig. 14).

There are four Safety Engineers working in PSB and they have their own spheres of responsibilities. One Safety Engineer has a primary responsibility for the event investigation practice (hereinafter referred to as SEE). He is liable for the screening, documentation, assessment (i.e. initial classification) and investigation of operational events. In connection with the event investigation practice, the Safety Engineer collects information on identified human errors for PSA studies. He is also responsible for making sure that produced action proposals are acknowledged in the concerned organisational units. In addition, he has the general responsibility for assessing the

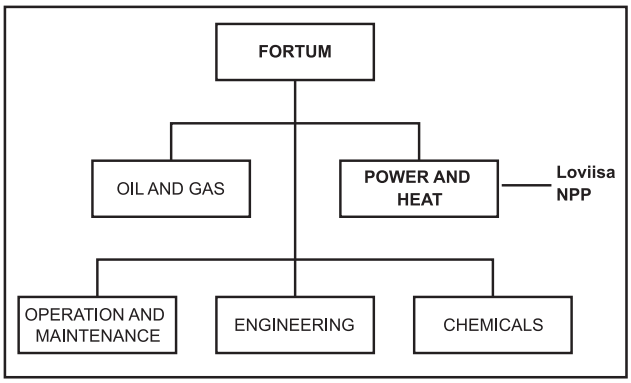


Figure 13. *Fortum Corporation organisation chart.*

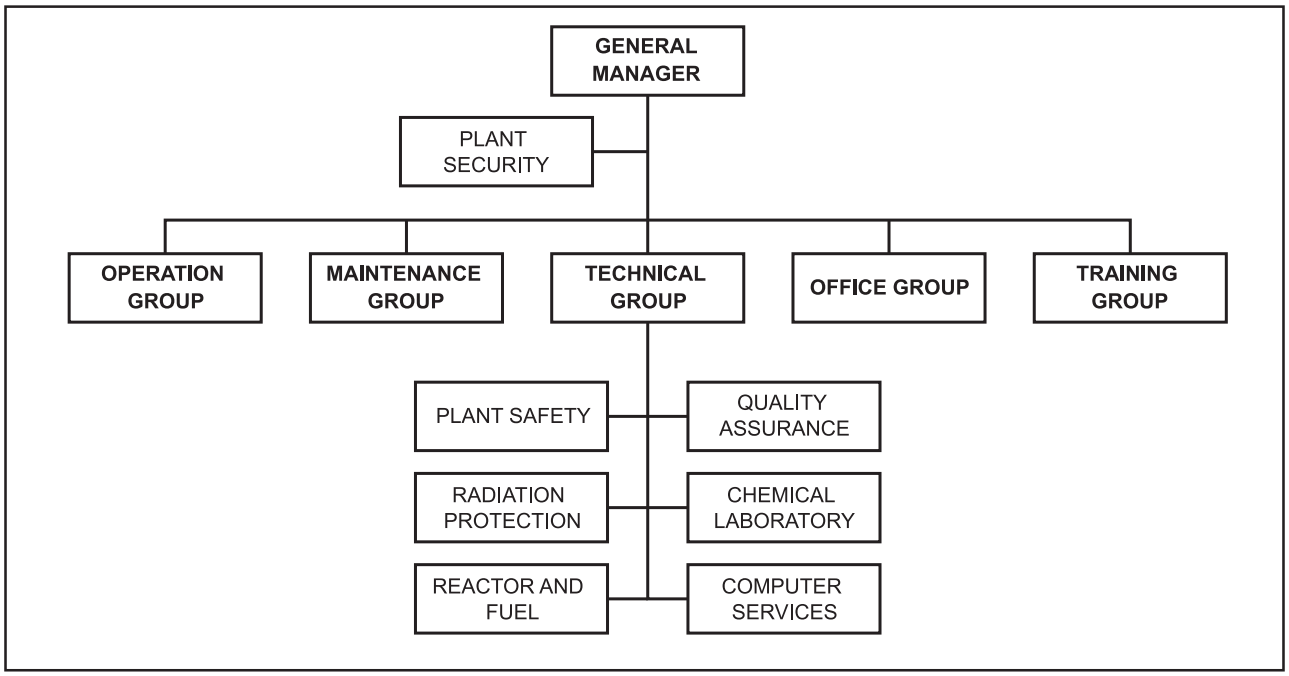


Figure 14. *Loviisa power plant organisation chart.*

effectiveness of the operational experience utilisation process at Loviisa power plant. (82-12-001/M5.)

Quality Assurance Branch (QAB) is liable for storing the operational event data, supervising the implementation of action proposals that result from the investigation process, and evaluating the adequacy and effectiveness of implemented enhancements (82-12-001/M5).

Enhancements proposed in root cause, special and operational transient reports are discussed and approved in the Quality Assurance and Safety Meeting, chaired by the Plant Manager. The meeting also nominates project managers and confirms dead-lines for approved measures and modifications. The actual operative responsibility for the implementation of approved measures lies in the concerned units. Every six months QAB provides the meeting with a follow-up report on the implementation status of the work in progress. (82-12-002/M2; 82-12-001/M5.)

According to LPP's directions the SEE has the general responsibility for the whole operational experience utilisation process (82-12-001/M5). In practice, different groups and branches are responsible for different activities. "There are [related] activities all over the organisation", reckoned one interviewee and continued that "work is being done in parallel, and in part simultaneously in different groups". Also the SEE wondered whether they had too much redundancy but assured that the prevailing situation had its advantages, too. For instance, he was of the opinion that such redundancy was likely to contribute to the independence of investigations because many related activities were actually carried out by more than just one group or team. The SEE concluded that their "possibilities to stay independent are as good as they can possibly be for a function that is located inside the organisation".

Liabilities appeared to be well defined, however. The interviewees also pointed out that PSB may freely decide on the subject of its activities and intervene in any operation or event on the basis of its own consideration. They admitted that their position was in that respect in little bit problematic but assured that possible problems were mostly attributable to personal relations instead of the organisation itself.

6.2 Investigation practices

6.2.1 Monitoring and recording of operational events

According to LPP's Quality Assurance Handbook (82-12/M2) all the employees are required to report on identified problems and deviations in a timely manner. Supervisors are explicitly supposed to contribute to the development of a working climate that encourages such behaviours on site. Group managers must provide their units and employees with adequate reporting procedures and supervise compliance with them. In general terms, observed defects, failures or deficiencies are to be reported directly to the SEE in charge of the event investigation practice, or to the immediate line manager who in turn shall convey that information to the SEE. Reporting can be done either verbally or in writing (82-12-001/M5).

The representatives of PSB were of the opinion that it is almost impossible to build a "general trap" to catch all operational events. Major defects won't cause any specific problems in this respect since they usually result in work orders and permits which end up in the Loviisa power plant information system, LOTI. There are, however, numerous minor "happenings" that do not necessitate repairs or any kind of reporting. The interviewees also reckoned that significant events do not necessarily emerge from routine reports, either, and continued that their recognition usually calls for "something extra". According to the interviewees important information was mostly conveyed in meetings or by means of direct contacts from the line organisation. In case of operational transients the control room was mentioned as an important source of information. In consequence, plant personnel's activity was considered to be of great importance to the monitoring and recording of operational events at Loviisa power plant: "people will just have to tell about them", as one Safety Engineer summed it up.

At LPP both the recording as well as initial classification of operational events are done simultaneously during the first stage of the event investigation process called "assessment" (see also the next Chapter). The recording of the event is done by compiling a specific Operational Event

Report, i.e. the KT report. This first stage is very important since it usually determines the amount of attention the event is likely to receive in the future. For instance, the KT report comprises an event classification section for the determination of necessary follow-up reporting and investigations, and the section is to be completed at this early stage.

LPP does have specific directions for the further processing of operational events but the concept of "operational event" itself remains unspecified. The problem is that there is no *explicit* procedure for the identification of an operational event although the reporting requirements themselves appear to be comprehensive, well documented and in compliance with the official instructions given in YVL 1.5 and YVL 1.11. In other words, in order to come recorded and properly assessed an event (e.g. an observation concerning an organisational deficiency or failure) needs to be first classified as an "operational event" while clear and explicit classification criteria are missing.

The interviewees admitted, too, that the content of the term operational event "is not unambiguous at the plant" and that explicit classification criteria did not exist in writing in any paper or document. The SEE noted, however, that the definition of such criteria would be a rather difficult task because "you will easily end up with a very simple and superficial document that discards many relevant and includes many irrelevant events, or a very complex set of conditional criteria that are difficult to use in practice". Therefore the best "criterion", according to the view of the SEE, "is a knowledgeable person who classifies the events on grounds of his or her engineering experience and-if need be-after consulting other subject matter experts". He continued that in this respect the prevailing organisational culture had a very important role in guaranteeing sincere exchange of information on site.

According to the interviewees operational events are identified by their practical relevance to plant operations: "it is characteristics of an operational event that it causes real or potential harm to the plant, that it is worth an intervention or that one can learn from it". They emphasized that in addition to the event's significance to plant safety the classification may also be based on its impact on economics, availability or personnel safety. Common cause failures are always operational events. In 1998 altogether 66 deviations were classified as operational events at Loviisa power plant.

In case of an identified operational event a specific KT report shall be prepared. The report shall contain a short description of the event together with some basic information i.a. on the operational state of the plant, influenced systems or equipment, and necessary corrective measures. An example of a KT report can be found from Appendices.

6.2.2 Assessment and screening of operational events

The SEE is responsible for the assessment and screening of operational events at Loviisa NPP. This is done in co-operation with the representatives of concerned organisational units. The assessment shall result in a completed KT report to identify further reporting and investigations needs. In relation to further actions there are five different tracks to be followed depending on the severity of the event:

- no further clarifications needed,
- additional clarification,
- notice (internal, to STUK, and/or to WANO),
- official event report (special report, operational transient report or reactor scram report), or
- root cause analysis report (82-12-001/M5).

The decision is largely based on the reporting directions given in LPP's internal guide 82-06-006/M3 "Loviisa 1 and 2 operational event reporting". The guide specifies the events and situations that necessitate the compilation of an official event report. The requirements correspond to those issued by the regulator in YVL 1.5. In case of an event calling for "a comprehensive handling and analysis" a separate root cause analysis shall be conducted. An additional clarification is to be conducted for those operational events that do not require the compilation of an official event or root cause analysis report but that have relevance to operational safety, availability, plant economics, training, or the development of the quality assurance system (82-12-001/M5). The main phases of the assessment and screening of operational

events at LPP are presented in Figure 15.

Anyone working at the plant can come up with a proposal for preparing an additional clarification. Proposals are to be submitted to the immediate line manager, or directly to the SEE. The SEE will decide on the preparation of the clarification together with a nominated contact person responsible for the system, equipment or area of operation in question. Additional clarifications are not subject to formal requirements. The SEE and the nominated contact person may therefore define the extent of the study on case-by-case basis. Additional clarifications may be carried out either by the SEE himself, or another person in the concerned organisational unit. Necessary corrective measures, persons responsible for proposed measures as well as timetables shall be specified in the clarification, or in the corresponding KT report. (82-12-001/M5.)

As part of the initial assessment the SEE tries to identify such operational events that have been caused by a human failure. The work is based on the review and further assessment of the events covered by existing KT reports. For the SEE this is a kind of "side-line duty" to be done without any additional resources or specialist support. Having found such an event the SEE will classify the event i.a. in terms of its detection, consequences, and probable causes. The findings will be registered into a specific human failure report, and its event classification scheme appears to be much more elaborated compared to that of a regular KT report. Human failure reports provide data for LPP's PSA function. For an example of a human failure report, see Appendices.

The interviewees reckoned that it is very much up to the people in charge of the assessment how things proceed. They have a significant personal responsibility for the adequacy of the initial assessment process since apart from the formal

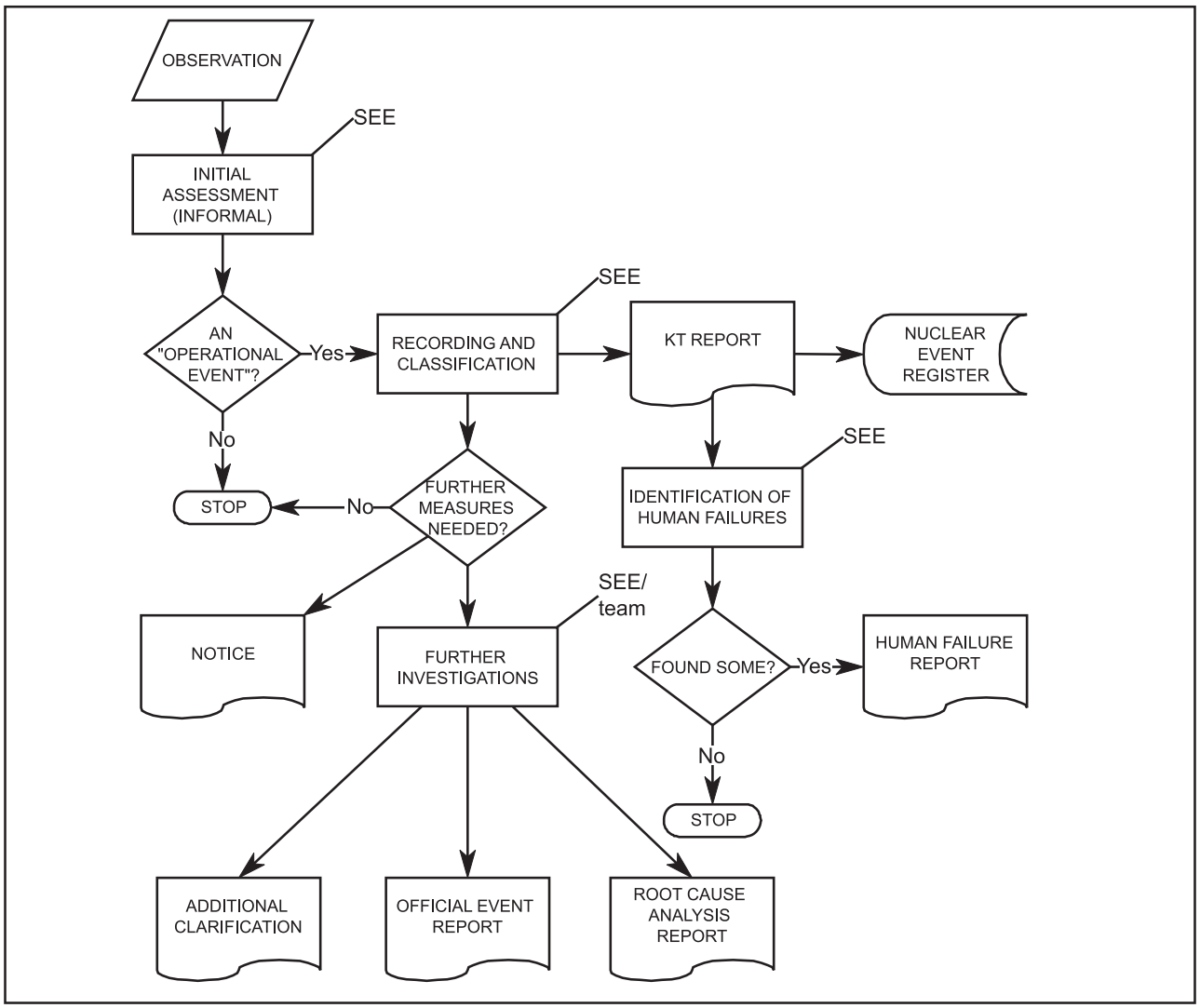


Figure 15. *Assessment and screening of operational events at Loviisa power plant.*

reporting requirements there are just few other formal arrangements to support their work. On the one hand, the Plant Meeting may decide on the compilation of a KT report e.g. on the basis of information provided by the SEE. This is not the regular practice, however, because the weekly Plant Meeting mostly concentrates on the administrative side of plant operations. On the other hand, the matter may be discussed in the LPP Quality Assurance and Safety Meeting provided that it emerges in connection with the processing of some other event or measure already on the agenda. The LPP Quality Assurance and Safety Meeting is more substance oriented than the Plant Meeting, but not directly responsible for initial assessments or classifications, either. As a result, additional support is to be acquired by means of more informal patterns of co-operation between the PSB staff and subject matter experts.

Operating experiences gained at other nuclear facilities are assessed by Operational Experience Group of Fortum Engineering, an independent research and development arm of Fortum Corporation. LPP participates in its activities through nominated representatives.

6.2.3 Analysis of safety significant incidents

Safety significant operational events and situations are to be investigated and reported by means of special reports. The reporting directions given in YVL 1.5 apply to all Finnish nuclear power plants. Therefore, Fortum's special reporting practice bears in this respect much resemblance to that of TVO. YVL 1.5 defines the situations in which a special report shall be prepared as well as the contents of the report.

The Plant Manager, Group Head, Operations Engineer or Safety Engineer may decide on the compilation of a special report and the initiation of investigation. The Operations Engineer has the main responsibility for the work. The Safety Engineer is liable for assessing the safety implications of the incident (82-06-006/M3).

The special report is based on a standard form overlay which is to be supplemented with necessary attachments, i.e. plotter graphs, computer log files, PI diagrams and complementary analyses. The report is organised according to the requirements specified in YVL 1.5 and 82-06-006/M3, LPP's corresponding instruction. In short, the special report includes a concise summary of the incident and clarifications on the course of events, safety assessment, causes of the incident and measures to avoid the recurrence of such incidents in the future.

All special reports are subject to a circulation before they are submitted to the regulator. The circulation shall always include "safety" and "operations". Other functions are to be determined according to the case. During the circulation, the report shall be inspected and approved by nominated representatives of the concerned functions. In addition, all special reports shall be presented and discussed in Loviisa Nuclear Safety Committee (LYTT) which assembles for its regular meeting six times a year. (82-06-006/M3.)

A root cause analysis may be conducted for safety significant incidents that require special reporting and whose root causes can not be adequately identified or analysed as part of the regular inspection procedure. However, independent of the safety significance of the case, the Plant Manager, Group Head, or LYTT may decide on the preparation of a root cause analysis report. The decision may be based e.g. on perceived deficiencies in the functioning of the organisation, common cause failure mechanisms or recurrent defects in some system or equipment that could possibly result in a safety significant incident or considerable economic losses (82-12-002/M2). In consequence, a root cause analysis may also be conducted for such events or phenomena that do not fulfil the reporting requirements given in YVL 1.5 and which therefore do not necessitate the preparation of an official event report to the regulator.

Root cause analyses are carried out by a special task force, or investigation team, nominated by the Plant Manager or his deputy. According to LPP's internal root cause analysis instructions the team shall primarily consist of persons who know the case and who have been trained to conduct the analysis. Special attention shall be paid to their experience, understanding of plant behaviour, technical know-how, human factors expertise, co-operative skills, and impartiality. The investigation team will usually include

- one Safety Engineer, usually nominated as the head of the team,
- two subject matter experts from appropriate functions, and
- one methods expert, or an external subject matter consultant (82-12-002/M2).

The division of tasks and duties within the team is to be done on case-by-case basis. In case of a significant incident more than four members may be nominated to the team. Also the Plant Manager may participate because in such a case "the team must have enough authority to decide on necessary corrective measures", as one interviewee pointed out. In case of a minor event of no particular safety significance, the Safety Engineer may conduct a more limited analysis by himself. (82-12-002/M2.)

The main objective of a root cause analysis is to minimise the possibility for the recurrence of the identified incident. Therefore, the analysis shall result in the specification of corrective measures by aid of which identified defects, failures or exceptional phenomena are to be removed. The feasibility and adequacy of proposed actions, e.g. in terms of necessary and available resources, shall be considered separately after the completion of the analysis. (82-12-002/M2.)

In LPP's root cause analysis instructions the analysis shall include the following phases:

- acquisition and verification of necessary information,
- event reconstruction and cause clarification by means of an adequate analysis method,
- identification of corrective measures,
- verification of proposed corrective measures,
- compilation, inspection and endorsement of the root cause analysis report (82-12-002/M2).

There is no specific method or procedure for conducting root cause analyses at LPP. The idea is that the investigation team will choose its tools and methods according to its needs and the nature of the case. The most commonly used root cause analysis method is a modification of HPES that has been simplified to fit in LPP's needs. Another is the so called "path method", a technique developed in collaboration with LPP and IVO Power Engineering (currently Fortum Engineering) several years ago. Applied methods and the course of the investigation procedure ought to be specified in the resulting analysis report. The interviewees stressed the importance of a clear and informative reporting practice.

Root cause analysis reports are based on team consensus. Once all the investigation team members have approved the report it will be submitted to the Plant Manager for a final endorsement (in case the Plant Manager has not personally participated in the investigation as a team member).

Applied practices appear to be relatively informal. For instance, LPP's root cause analysis reports reviewed in this exercise do not provide the reader with any precise method descriptions, nor references to any other methods or manuals according to which the investigations could have been carried out. However, the most recent reports since 1997 usually comprise HPES type diagrams to illustrate event sequences and the impact of identified causal factors on analysed incidents. The interviewees told that a lot of time and efforts are invested in interviews and document reviews, and this also seems to be the case on the basis of the root cause analysis reports assessed in this study. An in-depth analysis of selected cases and related special and root cause analysis reports can be found in Chapter 7.2.

The interviewees were mainly satisfied with the current incident analysis practices. They said that existing tools are sufficient, provided that they are utilised in a proper manner. According to the interviewees the identification of individual and organisational performance shaping factors and root causes has been one of the main issues in the development of existing analysis methods. For the time being they thought they had been fairly successful in solving such cases although not always: "every now and then you have a feeling that you did not quite find out all the essentials, but that is something you really cannot avoid". Prevailing methods and practices were told to be subject to constant re-evaluation: "they are being tested again and again" as part of the regular investigation practice.

The official event reporting practice, i.e. the compilation of special, operational transient, and reactor and turbine scram reports, covers the entire operating life of the plant from the late 1970s to the present. Root cause analyses have been carried out from the year 1992. The KT

reporting practice was introduced in 1994 for recording outage events, and has been in regular use in its present form since 1995.

6.2.4 Utilisation of investigation results

Enhancements proposed in root cause, special, operational transient, and reactor and turbine scram reports are to be discussed in the LPP Quality Assurance and Safety Meeting. The meeting may endorse them as proposed, decide on complementary studies or measures, or discard the proposed enhancements on the basis of its own justification. The meeting also nominates project managers and sets dead-lines for confirmed measures and modifications. QAB is liable for supervising their processing and implementation in the concerned organisational units, and evaluating the adequacy and effectiveness of implemented enhancements (82-12-001/M5). An overview of LPP's investigation result utilisation activities is given in Figure 16.

Root cause and special reports are also submitted to LYTT for a safety assessment. LYTT may propose additional recommendations which shall be taken into consideration according to LPP's internal direction 82-03-003 "Handling of Loviisa Nuclear Safety Committee's recommendations at Loviisa power plant". (82-12-001/M5.) . In general, the requirements concerning the treatment of reported events appeared to be rather comprehensive and precise.

Nevertheless, descriptions concerning the processing and utilisation of investigation results are limited to the administrative side of the issue and do not comprise concrete guidelines e.g. for learning from identified deficiencies. For instance, the extent to which human failure report data is being utilised remains an open question since excluding PSA neither the interviewees nor LPP's internal directions assigned any other objectives for the practice. The absence of more substantial guidelines together with overlapping responsibilities of PSB and QAB raise questions about the

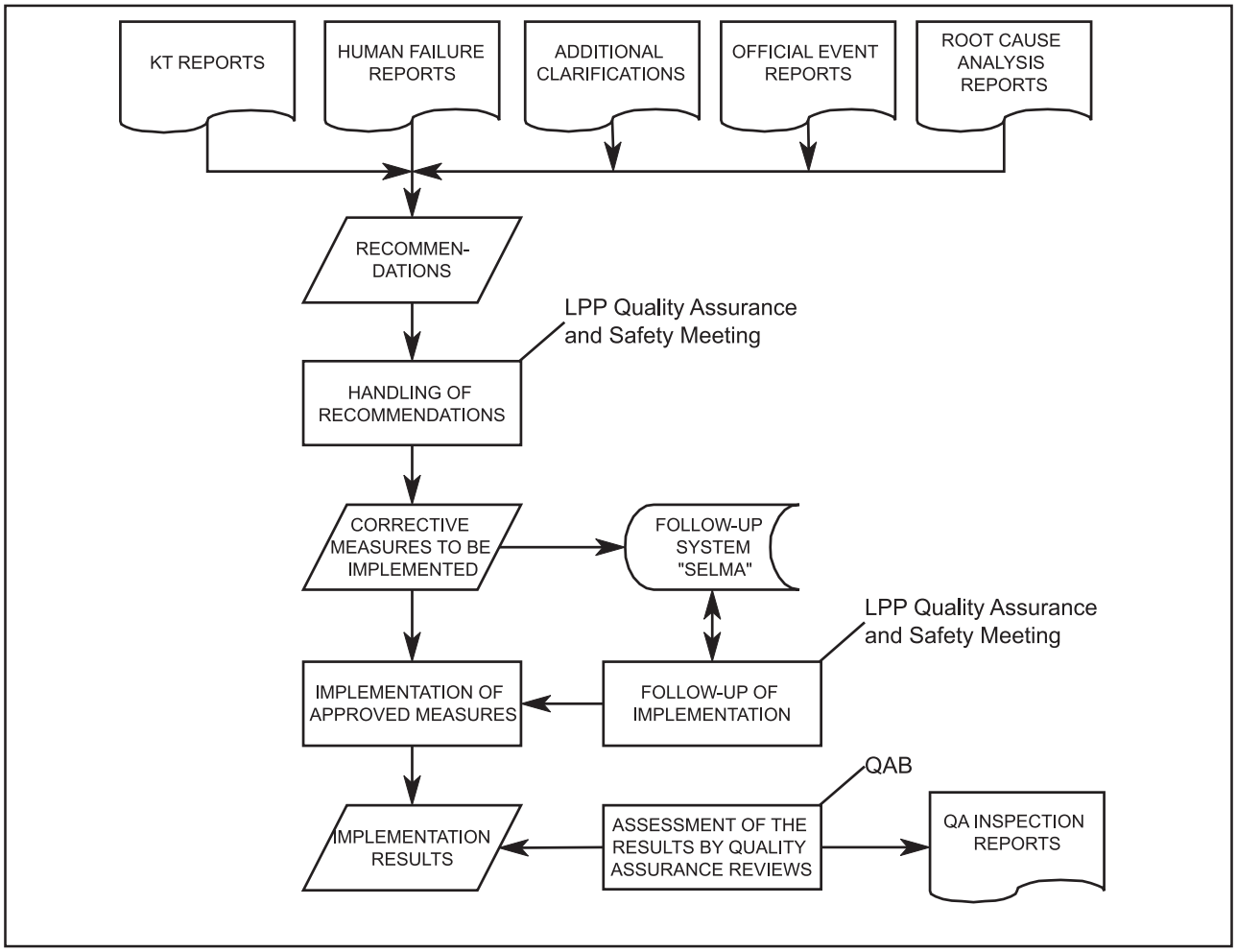


Figure 16. *Utilisation of investigation results at Loviisa power plant.*

effectiveness of prevailing information management practices at LPP. The SEE assured, however, that the feedback loop from QA was functioning very well and that he could take full advantage of their work and results. Within the framework of this study it was not possible to evaluate how efficiently investigation results were actually being utilised.

6.2.5 Data administration and analyses

In addition to annual follow-up reports on the utilisation of operational experience, the Quality Assurance Branch, QAB, has the responsibility for the preparation of an annual Quality Assurance and Safety Meeting report. According to the interviewees these practices in part aim at the identification of common cause failure (CCF) mechanisms by means of a systematic review and analysis of existing operational event data. Moreover, the SEE personally considered the search and identification of CCF mechanisms to be his main duty. Nevertheless, LPP's CCF detection activities appeared to be fairly inconsistent.

Both Safety Engineers were of the opinion that "whenever something happens, one should go and see whether there are signs of other similar incidents in the past" and that "also other people have such responsibilities to ... conduct continuos analysis". They admitted, however, that "for the time being, it does not happen in reality" and that "while some people do it, others do not". In addition, access to the LPP Nuclear Event Register, a database for both internal and external operational event, was limited. This led us to a conclusion that depending on the type of the event and affected systems the event is likely to receive a very different treatment when the search for CCF mechanisms is concerned. Nevertheless, the SEE assured that all significant operational events as well as failures involving defects in important safety systems or equipment (covered by the Technical Specifications), were subject to a systematic and continuous screening process. In case of root cause analysis, special, operational transient and KT reports this had to be carried out manually (see ch. 6.3.3).

It is worth mentioning that LPP's internal directions do not say anything about the *recognition* of CCF mechanisms, although an *identified* common cause failure has been mentioned as an example of such an incident that may require the compilation of a root cause analysis report (82-12-002/M2). A logical conclusion is that there is no formal procedure for the identification of CCF mechanisms at LPP although some employees and units appear to have assumed a personal responsibility for taking care of the job. However, there are formal processes to support the identification and monitoring of the *historical recurrence* of deviations. This is done e.g. by means of regular Quality Assurance audits that cover all the main functions of the organisation.

6.2.6 Reporting

Reporting to the regulator, STUK, is done in accordance with the general reporting directions given in YVL 1.5. The main characteristics of the Finnish reporting system are outlined in Chapter 4.2.1.

KT reports are mainly designated for internal use, not for official reporting to the regulator. However, the resident site inspectors have an unlimited access to all plant data, and may therefore acquaint themselves with completed KT reports on request. This was considered a very important principle to guarantee a sound working climate since people command different attitudes towards the exchange of confidential information and supervision. The SEE himself was an advocate of "open-doors policy" and in favour of a transparent inspection and reporting practices.

6.2.7 Self-assessment on strengths and weaknesses

In general terms, the interviewees were relatively satisfied with LPP's investigation practice. The current custom of mobilising the line organisation in event investigations was considered to work well and to be of great importance to the practice. Major weaknesses were identified in the areas of quantitative performance evaluation, information systems support, and the utilisation of existing investigation results and plant data.

6.3 Operational preconditions

6.3.1 Human resources and training

The interviewees were of the opinion that they had enough competent personnel to take care of their duties. During outages peaking workloads put strain on the system but compared to many other facilities their situation was regarded as a rather good one.

The PSB staff train plant personnel to contribute to event investigations. Since 1995 more than 100 employees have participated in the compilation KT reports at LPP, and all the foremen have had an opportunity to participate in a way or another. As a result, there is a large pool of people having at least a modest acquaintance with event investigation activities. With the support of these people the Plant Safety Branch, PSB, may assume responsibilities well beyond the capacity of its own limited resources. The major challenges for this kind of on-the-job type training were attributed to the layman's attitude towards the use of formal models and methods. The Safety Engineers think they have succeeded fairly well so far although "it has not been very easy".

The Safety Engineers have attended several WANO courses since the year 1995. IAEA and the Finnish regulator, STUK, have provided them with ASSET training. The representatives of the plant have also participated in international peer-reviews on other nuclear power plants, and that experience was conceived as an useful additional plus for LPP's own investigation practice. According to their own impression the Finnish know-how is of high calibre and well comparable with international standards.

In connection with the annual refresher course in Operations, Maintenance and Technical Groups the SEE gives presentations on selected operational events. The issues are usually picked and chosen from previous year's reports and experiences, or on the basis of the feedback received from the line organisation. It was concluded that such signs of personnel initiative-provided that they are common and well rooted to the everyday life of the plant-may significantly increase the overall effectiveness of LPP's investigation practice.

6.3.2 Manuals and instructions

Instructions were generally given a good degree in terms of their adequacy and applicability. The present tendency is towards more practical instructions. Before people were "frightened" by thick manuals such as the original path method procedure for conducting root cause analyses. Nowadays, the procedure is light and the idea is to provide the necessary guidance as part of the investigation process. The general impression is that LPP's instructions are clear, concise, and easy-to-read. The overall conformity and coverage of LPP's instructions remains an open question since their assessment was not within the scope nor resources of this particular study.

The YVL-guides were considered to be of proper content and itemisation. The SEE noted that the guides did not impose disturbing constraints on LPP's activities and that they had enough room for their own initiative, too. Occasional disagreements between the plant and the regulator e.g. on the correct interpretation of given instructions, or the safety significance of particular operational events, do not directly relate to the YVL guides themselves.

6.3.3 Information systems support

There are several information system for different purposes at Loviisa power plant. The operational event data recorded by means of KT reports end up in a computerised Nuclear Event Register. It also contains information on selected external incidents. Special, operational transient, reactor scram as well as root cause analysis reports are archived as separate files. Information on approved measures and modifications in relation to previously identified and analysed incidents are stored in a computerised follow-up system (SELMA). The bulk of identified defects and failures of minor safety importance are stored in the Loviisa power plant information system (LOTI).

All operational events result in a separate KT report based on a standard form overlay in MS Word. The SEE fills in the form and stores the file in a predefined folder on the network hard disk. After that another person is responsible for transferring the data from the completed file to the

Nuclear Event Register. The database can be accessed by a graphical user interface. The interface programme supports some simple data retrieval operations, such as browse and search by event name, but it does *not* support elaborate multi criteria queries *nor* free text searches. Completed KT reports may also be accessed from LOTI by event name, but not on the basis of their contents. Only Safety and Quality Assurance Engineers have been authorised to use the LPP Nuclear Event Register.

In KT reports operational events are classified in different categories on the basis of further reporting and investigations needs. They are not (formally) classified according to their consequences or identified contributing factors. Such a formal classification scheme can be found from special reports but they exist in writing only. This means that the introduction of a more developed data retrieval function would call for significant modifications in both the existing computer system and the prevailing event reporting practice itself. In consequence, data analyses have to be carried out manually and they require "a lot of work and the prophet's gift", as the SEE summed it up. When it comes to the search of common cause failure mechanisms the conclusion clear: there is no efficient information technology based tools to support such activities at LPP. However, in case of minor defects and deviations the LOTI system seems to provide the plant personnel with a much better support.

The interviewees were well aware of the aforesaid limitations. They admitted they have had system integration problems and that they have not succeeded in solving them so far. The goal is one integrated system and one common database for all plant data, including KT as well as old operational transient and special reports. At the time of this study such development activities were already in progress.

6.3.4 Management support

The Safety Engineers were satisfied with the current status of PSB. They felt they can make themselves heard and let the management know what they are thinking. They were of the opinion that since the new Plant Manager was earlier in charge of the Maintenance Group, and because the new Head of Maintenance used to work as a Safety Engineer in PSB before his present appointment, the situation was likely stay good, or even get better, in the future.

6.3.5 Reviews and development activities

All the main functions of Loviisa power plant are subject to periodic Quality Assurance Reviews. They aim at detecting potential deviations from the LPP's quality system and identifying its deficiencies and development needs. The reviews focus on functions that are of specific importance to the safety or reliability of plant operations (LO1&2 FSAR, ch. 13.5). Identified deviations, deficiencies and development needs are recorded in a QA inspection report which comprises the following sections:

- scope of the review,
- implementation status of corrective measures resulting from previous reviews,
- identified deficiencies to be corrected,
- other observations to be taken into account,
- assessment of internal operational events and their historical recurrence, and
- evaluation of the effectiveness of proposed and implemented corrective measures.

The reviews are carried out and the inspection reports are prepared by the Quality Assurance Branch, QAB. Each QA inspection report is brought up for discussion in the Quality Assurance and Safety Meeting (LO1&2 FSAR, ch. 13.5). In 1998 altogether twelve QA inspection reports were completed. According to the SEE all groups and branches are to be reviewed "annually or semi-annually". On grounds of a closer examination of the concerned reports it seems more probable that the review has been scheduled to take place every second year (the preceding review for all the branches reviewed in 1998 had been carried out in 1996). The Plant Safety Branch has been subject to the QA inspection practice since April 1999.

Both the Finnish regulator, STUK, and Fortum Corporation's external inspectors conduct audits on site. In 1997 LPP's technical functions, including the operational experience utilisation process,

were audited by a Canadian expert on assignment of Fortum Power and Heat Oy. According to the SEE the findings have been useful, although "by no means always positive".

The major development activities relate to the utilisation of the line organisation as part of the event investigation practice, and the specification of a new computerised information system. With regard to the investigation practice, the question is about proceeding along the current track and developing the patterns of co-operation with other organisational units even further. In addition, their intention was to hire a student to prepare a master's thesis on the development of the existing human failure reporting practice currently run by the SEE. When it comes to the new information system, the timetable was still open.

7 REVIEW OF SELECTED CASES AND INSPECTION REPORTS

An in-depth analysis of selected cases (i.e. operational events or incidents) and related inspection reports from the three participating organisations was carried out as part of this study. Selected cases and their inspection reports, as well as the criteria for their selection, were itemised in Chapter 2.4.

The ideal model C: Requirements for event inspection methods, is the basic framework for the analysis and evaluation of selected cases. The main emphasis is put on the specific requirements concerning the issues to be covered in event inspections and related inspection reports. However, also the requirements given in ideal models D: Requirements for the follow-up analysis, and E: Requirements for periodic operating experience reviews, are taken into account to the degree they are applicable in the following "renewed" follow-up analyses of the selected cases.

Therefore, in addition to the coverage of significant issues, also thoroughness of the analysis, clarity of the describing text as well as the outlining format and structure of the reports (see 2.3.4) are important. Moreover, issues such as event classification to clarify and outline what, how and why had happened, action proposals for the prevention of recurrence, suitability of the report format and the classification scheme for periodic event data analysis needs, and the connections between different reporting systems are noticed in the compilation of the evaluation comments.

In order to make the presentation of the following case based reviews more logical and understandable, the "follow-up analyses" of the incident cases, including detailed comments to the utility reports, are presented here in the Chapter 7. After this incident case specific review, the compiled evaluation comments to both STUK's and utilities' inspection methods and reporting practices are to be found in the Chapters 8.1.2, 8.2.2 and 8.3.2.

7.1 Teollisuuden Voima Oy

The first case study comprises both an initiating event and latent failures to be inspected. The evaluators' detailed *comments, improvement proposals* or *questions* are given in *italics* in the following analysis.

Case: Olkiluoto 1. Neutron flux trip limits left too low after isolation valve capacity test.

TVO reports:
- Root cause analysis TVO 1-TR-R1-2/94,
- Special report 1-TR-R7-1/94,
- Reactor trip report 1-KK-R6-1/94,
- ASSET Event Analyses, No. 27 and No. 28,
- Work orders, No. *TL 1941183 and* No. *TL 5003032.*

ID information: unit, date, time, descriptive title, inspectors, report date:
- Unit: TVO 1;
- Dates of detection: 24.05.1994 reactor scram SS 10 F/F at 20.04 o'clock; and 05.06.1994 protection channel trips 531K951H8 at 11.13 o'clock
- Inspectors: OHa, JuS, MiK, PNo, BCH.
- Root cause report date: 29.11.1994.

STUK TAPREK report (the incident data base of the regulatory body) :
- 111/ 28.11.1996

Immediate consequences of the incident:
The case comprises two interrelated incidents:
- 24.05.1994: The first part of the cascade event sequence lead to reactor scram (SS10) prior to R194 because the trip limits to be lowered for a test were wrongly defined.

- 05.06.1994: The second part of the event sequence lead to one neutron flux scram channel (SS101) to trip repeatedly during the start-up from R194 because the limit settings had remained too low.
- Affected systems, equipment and structures: 531K951-954 H6 F/F (SS10, E4); 531K951H8 (SS101, E41), K952-K954

Operational conditions and major process parameters prior to the incident:

- 24.05.94: An exceptional steam isolation valve capacity test requiring plant-start up prior to the refuelling outage R194, Thermal power raised to 28,6 % as the reactor scrammed.
- 05.06.94: Plant start-up after the refuelling outage R194. Reactor power 56 % as single channels tripped.

...and explanatory process and computer recordings to illustrate its progression:

Computerised disturbance recordings and alarm lists included in the reactor trip report 1-KK-R6-1/94.

Means of detection and the situation in which the incident was discovered:

- 24.05.94. Tripping of reactor scram SS10 occurred at 28,6 % reactor power before the thermal power level specified for the steam isolation valve capacity test was reached.
- 05.06.94: Neutron flux monitoring channel alarms occurred at ca. 56 % power levels during four successive start-up attempts after the refuelling outage.

The course of events (event sequence from the origin up to and including the recovery actions in a chronological order):

1) In 1984, within the first power (108 % = 100%) uprating of the reactor, the flow/flux trip limits H3-H6 were added as a modification into the reactor protection system.
2) The old trip conditions and limits were renamed by the new names E41, E42, SS101, SS102 and the changes were introduced in the system documents, operating and testing instructions.
3) *The corresponding changes were however omitted in the Technical Specifications*, e.g. *in the operation domain figures showing the scram and power limitation trip limits.*
4) *In the 90's, a second power uprating was planned to be introduced in the near future.*
5) A real plant level test was needed to ascertain the main steam isolation valve's closing capability at a high steam flow value of 360 kg/s.
6) 04.05.1994: *The earlier commissioning test program for the steam isolation valve capacity test was changed to correspond the new operational conditions for valve testing.*
7) The test program defined the lowering of the settings of the reactor trip conditions SS10 and E4 (531K951-K954 H8 and H7) *to facilitate an exceptional protection function during the test of the valve 311V004.*
8) The confused definition of the neutron flux limit resulted in the F/F trip limits of SS10 and E4 to be calculated for the 60 % setting values instead of calculating the needed limits of SS101 and E41 for the test.
9) 14.5.1994–3.05.1994: In parallel to the handling of the exception permit from the Technical Specifications for the trip limit lowering, the related operation order 1-KK-Y-6/94 and work order TL 1941183 were prepared.
10) Refuelling outage R194 was just beginning and in the evening of 24.05.1994 the plant was in the start-up state and the power was raised for the steam bypass operation to be conducted as part of the programmed isolation valve test.
11) 24.05.1994 at 20.04 o'clock: The reactor scram on SS10 F/F broke off the test as the reactor power increased to ca. 25 %.
12) The incorrect trip limits were restored and the correct reactor protection trip limits SS101/E41 were selected for lowering to 60 % prior to the new attempt to perform the special valve test.
13) *No changed work order was prepared after the reactor scram* although the functional objects of the setpoint lowering actions were changed to the SS101/E41 limits. The test supervisor did not consider changed trip limits, either.
14) The reactor power was raised again and the testing was performed on 24.05.1994 according to the 311-valve test program requirements.

15) 25.05.1994: After the successful valve testing, two restoration attempts of the setpoints (SS101) were done by the instrument technician. The attempts were prevented by the control room due to disturbance risks in the following reactor pressure vessel test, and secondly to the following shutdown procedure to the cold shutdown state.
16) 25.05.1994–05.06.1994: The SS101 and E41 trip limits were left too low (at 60 % of the basic levels) and they remained unrestored during the refuelling outage R194.
17) 05.6.1994: During the plant start-up after R194 the channel A 531K981H8 of the scram condition SS101 trips at 11.13 o'clock.
    The tripping of the A channel occurred at altogether 4 successive power raising attempts to ca. 56 % until the alarms were found to be not inadvertent.
18) The tripping relays of the neutron flux A channel of 531 H6 SS10 was blocked, the unrestored limits were set to the correct higher values and the blocks were removed as the reactor power had been reduced to ca 60%.

Problems encountered in managing and controlling the operational situation:

25.05.1994: The attempts to restore the trip limits after the successful valve testing had to be prevented by the shift supervisor due to reactor scram risks in the ongoing reactor pressure vessel test. Secondly, the aim was to prevent disturbances in the following plant shutdown procedure to the cold shutdown (R194 work activities starting).

Use and adequacy of approved procedures and instructions:

No clear practice or procedure was used for making or approving changes in the work order (permit).

Direct and root causes of the incident (the cause-effect chains explaining the case):

A part of the documentation changes (e.g. in the Technical Specifications) was omitted as the technical modification of the flow/flux trip limits in the reactor protection system was done in 1984.

The functional objects of the protection limits to be exceptionally changed during the capacity testing of 311V4 were not correctly identified in the definition and preparation of the test program.

Preparation of a renewed work order and permit was omitted in the stressed disturbance situation after the erroneous testing and reactor scram.

The restoration of the SS101 and E41 trip limits was forgotten during the refuelling outage R194.

In case of a human failure, the work task in which the error occurred (the failure origin):

Obs. The primary causes of the incident, which significantly contributed to the initiation and propagation of the event sequence, were not sufficiently enough established in the corresponding MTO root cause analysis report at the end of 1994.

The event and cause diagram (TSA) of the MTO method structures and clarifies the error sequence. However, in this case the TSA does not indicate well the deviations from the normal procedure (deviation analysis), nor broken organisational defensive barriers (barrier analysis of reviews) thoroughly enough. In general, TSA diagrams, or simpler diagrams of similar purpose, are usable tools for organising,clarifying and structuring event sequences.

Obs. The ASSET follow up event analysis summaries performed by TVO during 1998 identified the direct and root causes better than the narrative MTO root cause analysis report in this case. However, in the completed ASSET analysis reports (ERCAF) the number of occurrences to be thoroughly studied was limited to only one per incident.

Common cause failure (CCF) mechanisms, origin and interconnections to other systems:

Both the incidents (24.5.94) and (5.6.94) are classified as human common cause failures (HCCF) of safety related equipment.

Efficiency and adequacy of both technical and administrative barriers...

Deficient review and approval testing programs (The confused definition of the trip conditions and limits passed through the whole organisation from the preparation of the test program to the preparation of work orders and permits.

Checking and approval of changes in work permits and work planning?

...and in case of a technical failure, the adequacy of operability verification activities:

Deficiencies in operability verification prior to the plant start-up from the refuelling outage (no periodic testing of the relevant neutron flux trip limits) were identified.

Evaluation of historical recurrence (incl. local repairs, inspections etc.):

The root cause analysis report considers another event (special report 1-KK-R7-1/84), where during the maintenance outage R184 the restoration of the blocked reactor protection conditions SS13 in channels B and C *were* forgotten and were not identified in operability tests after the outage work.

Obs. The possible additional recurrence cannot in this case be easily clarified.

TVO has recently subjected the bulk of those incidents in 1993-1997 that were reported to the regulator to their first comprehensive periodic operating experience review (ASSET self assessment). Periodic operating experience reviews for systematic identification of historical recurrence of the causes and evaluation of the achieved effects to prevent the recurrence are strongly encouraged.

Availability of important safety systems:

No functionally critical unavailability of safety system.

Incident's significance in terms of nuclear, personnel and radiation safety:

The errors and omissions in the protection limit settings did not have any effects on plant safety. Because the exceptions in the protection limit settings were not detected in the operability verification tests at the end of R194, the utility considers the incident exhibiting weaknesses in the procedures.

Obs. The incapability to identify the confusion in the definition of the reactor protection conditions/limits that were subjected to exceptions exhibits also a weakness in the organisational performance.

Necessary immediate and long term corrective actions and their expected effects:

Obs. The allowed operation domain figure in the Technical specifications is updated to show the changed limits and names for the trip conditions 516 SS101/ E41 and SS102/ E42.

The checking and approval quality of changes in testing programs should be enhanced.

The procedure to change work permits and work documents shall be agreed.

The checks of neutron flux trip limit setpoints were added to the operability verification programs to be done before starting-up from the refuelling outage.

Obs. The good ASSET follow-up event analysis summaries performed during 1998 clearly identify the corrective action needs in testing programs/ orders compared to the MTO root cause analysis report.

Event recording and classification system (the event report is completed with classification for searches and periodic event data analysis purposes):

Obs. The incident reports do not include any classification codes which could help in searching for and pinpointing specific and recurrent event types and recurrent problems, failure modes and causes. (Find searches from WORD documented report texts can however be done.)

Obs. Such data and trend analyses are today possible. This requires sound classifications and event descriptions (i.a. narratives in writing) and an ability to take advantage of existing information technology based tools and data analysis methods. TVO failure history reports stored in their Work Order System (TTJ) present an example of a good classification system. The Swedish ERFNOVA and STAGBAS incident information systems contain examples of classification models for "RO and SS" incident data.

Reference to other related investigations, such as work orders and failure reports:

A good list of references is given in the root cause analysis report.

Obs. A recommendation is made to include the related work order titles and numbers in the reference list to enhance data integration and to facilitate further co-ordination of activities between different organisational branches.

7.2 Fortum Power and Heat Oy

The first case study comprises a latent failure to be inspected. The evaluators' detailed *comments*, *improvement proposals* or *questions* are given in *italics* in the following analysis.

Case: Loviisa 1. Common cause failure of TL 22 air fans to start due to incorrect connection diagram.

FORTUM reports:
KT 47/97, iv4797, Work nr *255395A*

ID information: unit, date, time, descriptive title, inspectors, report date:
- Unit: LO1;
- Date of detection: 23.09.1997;
- Time: 01.40;
- Title: Common cause failure of TL22 fans (no start);
- Inspector: JIA;
- Report date: 15.10.1997

STUK TAPREK report (the incident data base of the regulatory body):
No TAPREK report available.

Immediate consequences of the incident:
The technical specifications (TS) require plant to be brought into a shutdown state without delay (when both TL22 fans are found inoperable during power operation).

Affected systems, equipment and structures:
KZ: TL22D001, TL22D002; Lno: LIZ = other instrumentation equipment.

Operational conditions and major process parameters prior to the incident:
Power operation.

...and explanatory process and computer recordings to illustrate its progression:
Not applicable.

Means of detection and the situation in which the incident was discovered:
At fan start-up attempt after fans had stopped during the periodic testing of the YZ36 protection system (performed every four weeks).

The course of events (event sequence from the origin up to and including the recovery actions in a chronological order):
1) A plant protection system test (YZ36) was performed *in which case the containment isolation valves must close and the TL22 fans must stop.*
2) After the YZ36 test both supply air fans of the containment vacuum and the purification system (TL22) failed to start *on the following start-up attempt.*
3) According to the TS requirements, the preparations for the plant-shutdown were started at 01.40 o'clock.
4) Parallelly, the instrumentation technician on duty was called to the plant and the repair work started at 02.50 o'clock. One fan (TL22D001) was made operable at 03.00 o'clock.
5) Whereupon the TS requirement on plant shutdown without delay revoked.

Problems encountered in managing and controlling the operational situation:
Not applicable?

Use and adequacy of approved procedures and instructions:
The limiting condition rules for operation were applied according to the TS. It was however decided that the possible excessive requirements of the TS are checked because the exhaust air fans and the TL22 system were capable of maintaining the containment under negative pressure.

Direct and root causes of the incident (the cause-effect chains explaining the case):
The failure origin was an *incorrectly designed* connection diagram used on 17.9.1997 for repairing the limit switch of a *single* closing damper SO1, causing *a latent CCF preventing the start of the fans D001 and D002.*

Obs. In order to steer the event investigation and to ameliorate the outlining of the event report, a field on Causes should be added to the KT report in addition to the fields of Event Description and Corrective Actions.

In case of a human failure, the work task in which the error occurred (the failure origin):

The incorrect connection diagram had according to LOTI (the Loviisa Power Plant Information System) search possibly been designed as part of the modification work on the object performed on 05.07.1997?

Obs. The origin and cause of the incorrect design work resulting in the "crosswise" connection diagram were not included in the KT report.

Common cause failure (CCF) mechanisms, origin and interconnections to other systems:

The repair work done according to an *incorrectly designed connection diagram* of the limit switch of the closing damper SO1 caused the latent CCF of the fans D001 and D002.

This event originates thus from a dependent human shared equipment fault (HSEF) of the change-over switch of the fans that has caused multiple components not to start?

Efficiency and adequacy of both technical and administrative barriers...

Obs. Analysis of the possible ineffectiveness of the defensive barriers is not included in the KT or Human Failure (iv) reports.

...and in case of a technical failure, the adequacy of operability verification activities:

Obs. Not included in the KT or iv-reports, but should preferably be covered in them. E.g. planning of a better automation installation check and functional test could in a similar case prevent failures to remain latent after modifications!

Evaluation of historical recurrence (incl. local repairs, inspections etc.):

Seems neither to be included in the KT or iv-reports: no systematic treatment of the bulk of these reports exists!

Availability of important safety systems :

Inoperabilities qualitatively treated in the KT report. Unavailability time given as 1 h in the iv-report.

Obs. According to the LOTI work order history classifications and calculations for the work No. 255395A, the unavailability times given for the fans TL22D001 & D002 were however 2629,6 and 2659,2 hours respectively.

Incident's significance in terms of nuclear, personnel and radiation safety:

The INES classification was 0 (below scale). The justification for the INES classification given by the plant was that the TL22 system does not cause initiating events or have any impact on identified accident sequences.

In the KT report 47/97 the event significance has been classified as not requiring other or deeper inspection reporting.

Necessary immediate and long term corrective actions and their expected effects:

Provisional repairs for restoring the first TL22 fan's operability were done 23.09.1997.

An additional work order for the second fan D002 was prepared (255397).

After the 23.9.97 repairs, the crosswise connections in the connection diagrams and functions were checked and tested, and the original design documents were corrected.

A work order for the coming 1998 maintenance outage was prepared in order to recheck the problematic connections.

Event recording and classification system (the event report is completed with classification for searches and periodic event data analysis purposes):

KT reporting is a good and systematic event reporting practice available for the users of the plant computer network. An exemplary classification in the KT reports is made with respect to the reporting requirements.

However, KT reports are not completed by any classification to support periodic operational experience reviews, systematic identification of recurrent events, causes, or their consequences, or ranking of pending corrective action programs.

Obs. A systematic classification should preferably be introduced in the KT reports for clarifying the significance of the event and outlining the event information, too.

The portion of the KT reports involving human errors is complemented by Human Error (iv)-reports which are registered in LOTI and used as

human reliability and CCF data for PSA studies.

Obs. The classification scheme for human errors and their causes is generally good but should be complemented by introducing options for Design Deficiency and Work Planning Deficiency. In addition, the classification of involved working groups should be completed by introducing options for Design branch and Work Planning branch (lacking work order step?) .

Obs. In addition, the search of recurrent error causes and problems should be facilitated by the classification codes and the study of underlying KT and iv-information.

Reference to other related investigations, such as work orders and failure reports:

The work orders on corrective actions performed in connection with the concerned event should preferably be referenced, too (work numbers).

The second case study on Loviisa NPP incidents is also a latent failure.

Case. Loviisa 2,1. Unallowed disconnection of back-up emergency feedwater pump for preventive maintenance during power operation.

FORTUM reports:
Root cause analysis LO1-K863-6, LO2 special report 1/97, KT 01/97, iv0197, *Work nr 232176A.*

ID information: unit, date, time, descriptive title, inspectors, report date:

- Unit: LO 2 ,1;
- Date of detection: 14.01.1997;
- Daily report, Preventive maintenance of back-up emergency feed-water pump in violation of the technical specifications;
- Inspectors: JIA, PIR;
- Root cause report date: 09.06.1997

STUK TAPREK report (the incident data base of the regulatory body):
134/11.06.1997

Immediate consequences of the incident:

The erroneous violation of the technical specifications (TS) rules did not result in operational consequences.

However, the violation resulted in a decision to prepare a special report and a root cause analysis report for identification of necessary measures to prevent recurrence and *to facilitate organisational learning.*

Affected systems, equipment and structures:
KZ: 22RL97D001.

Operational conditions and major process parameters prior to the incident:
Power operation, Thermal power 99,9 %.

...and explanatory process and computer recordings to illustrate its progression:
Not applicable.

Means of detection and the situation in which the incident was discovered:

The safety engineer observed from the daily report 14.1.1997 the ongoing work on RL97D001 and questioned its work provisions.

He pinpointed that preventive maintenance during power operation is not allowed without an exception of some equipment specifically listed in the technical specifications.

The course of events (event sequence from the origin up to and including the recovery actions in a chronological order):

1) The planned maintenance work 232176A "Periodic inspection of the back-up emergency feedwater pump diesel" included in the RL970 package was omitted due to a lost work order during the LO2 maintenance outage *(LO1: 20.7.96–21.9.96 and LO2: 21.9.96-14.10.96).*
   The maintenance work to be done during the LO2 maintenance outage (96LAT 16) did get the start permit from the shift supervisor on 25.9.1997.
2) The safety measures of the package had been restored and the pump operability test prior to plant start-up was done on 9.10.*1997 without calling back the lacking work permit 232176A.*
3) On Friday 11.10.1997, the LO2 plant start-up from refuelling state to *hot standby* was going on. The lost work order appeared and it was detected that the work 232176A had not been done.

4) A need of forced transfer of the work from the outage to the power operation period was discussed in an evening meeting between the control room work planner, the shift engineer and the maintenance foreman.
5) *A note on the transfer of the work order was entered into the LOTI Work Order subsystem and the existing work order (paper) document was hand-corrected immediately, but without any formal approval. The omitted work was then not entered into "the list of works transferred from outage", maintained by the control room work planner function.*
6) Due to these work planning and management failures, the transfer was not treated or decided in the next day's (12.10.1997) outage meeting.
7) The original work order document (i.e. the one relating to the transferred task) wandered after the LO2 start-up into the "post box" of the maintenance foreman *instead of the work planners' box (where it should have been submitted).*
8) The undone and "transferred" work order did thus not undergo the necessary safety review circulation (TMT). Instead, the "outage number" on the LOTI/TMY display was changed by the work planning on 09.01.97 to "operation period number 97KÄY17".
9) The maintenance foreman sent the work order document to the control room with an adjoining message to start the work on Monday morning 13.1.1997.
10) The check of the 22RL97D001 work provisions done by the shift supervisor showed their connection to the outage work provisions.
    The shift supervisor misinterpreted the limiting conditions for operation specified in the TS by assuming that the exception list allows preventive maintenance for 22RL97D001 during power operation, and consequently gave the permit to start the maintenance work.
11) The safety engineer observed from the daily report of 14.1.1997 that his work provisions from the outage period 1996 and the ongoing work on RL97D001 were found violating the TS limiting conditions for operation.
    This observation resulted in immediate recovery actions of equipment operability, informing the regulatory body (STUK) and decisions on the preparation of special and root cause analysis reports to investigate the event.

Problems encountered in managing and controlling the operational situation:
Not identified.

Use and adequacy of approved procedures and instructions:

Ineffective procedures for detection and follow-up of unfinished work orders prior to restoring the work packages to operable subsystems ?

No clear procedure for the use of the control room maintenance planner' diary, although the control room maintenance planner per se is a good practice.

No clear procedure existed for the checking and treatment of possible transfers or cancellations of outage works.

No effective routines for the treatment and acceptance of possible changes in work orders and permits?

Direct and root causes of the incident (the cause-effect chains explaining the case):

Forgetting the planned work order for the periodic check of the pump diesel 22RLD001 during outage.

Registrating the work order transfer in LOTI/TMY prior to an approval for a change in work plans.

Work order did not undergo a new safety review (circulation) after the change.

In case of a human failure, the work task in which the error occurred (the failure origin):

An outage maintenance work package was restored operable by the control room although an underlying work order was unfinished.

The knowledge of limiting conditions for operation (LCOs) of the TS was insufficient among work planning branch, maintenance foremen and shift supervisor.

Unclear responsibilities in relation to decisions and approval of work planning and work permit changes within the maintenance department.

Obs. The causes of human errors and organisational weaknesses including their origin should be more deeply clarified. E.g. in the root cause analysis report, the maintenance management of the plant comments on the need of clarification and prevention of causes of undone works and missing detection in the event as the outage work package was restored operable.

Obs. The cause-effect chain diagram clarifies the error sequence, but does not illustrate the organisational (and partly operative) defensive barriers that were broken.

Obs. Generally the originating errors and their causes should be better clarified and/or classified in order to identify the necessary remedial measures instead of local corrective actions only, especially in case incidents when a root cause analysis is needed.

Common cause failure (CCF) mechanisms, origin and interconnections to other systems:

Not CCF, *but another type of dependent failure?*

Obs. The work on 22RL97001 affected two units. It caused inoperability (?) and complicated (?) work planning activities at both units because the pump diesels 22RL97D001 and 11RL94D001 are common for both units LO1 and LO2.

This incident and the work permission since 25.9.1997 was thus a dependent human shared equipment fault (HSEF) mechanism that affected also the LCOs of the LO unit 1 after its start-up to power operation on 21.9.1997?

Efficiency and adequacy of both technical and administrative barriers...

An outage maintenance work order package was restored operable by the control room although a related outage work was not returned.

Obs. Checking and approval of changes in work planning?

Obs. A thorough analysis of the ineffectiveness of the defensive barriers is not included in the root cause analysis report. A good way to structure and present the whole analysis of lacking or broken barriers is shown in the MTO event, cause and barrier analysis diagrams (see e.g. in HPES investigators training manual or root cause analysis reports compiled in the year 1994 at Olkiluoto NPP). They provide the reader with a well structured picture of the case in a single glance.

...and in case of a technical failure, the adequacy of operability verification activities:

A subsystem test was carried out by the control room before one outage work permit was returned to the control room.

Evaluation of historical recurrence (incl. local repairs, inspections etc.):

The root cause analysis report considers another event (KT 58/96), where a maintenance outage work on repair of an 11FL transmitter was transferred 17.9.1997 due to a lacking spare part at the end of the LO1 maintenance outage.

The work order was returned to the work planning branch and the work 237193A was carried out on 18.11.1997 by using outage work provisions although the plant was in the state of power operation. The work order did not undergo any previous safety review circulation, either.

Obs. A possible additional recurrence cannot be easily assessed since the bulk of KT and iv-reports is not subject to any specific periodic, statistical or qualitative, review based on a formal classification of causes etc?

Availability of important safety systems:

Unavailability time 13.-14.01.1997 of the pump diesel 22RL97D001 due to preventive maintenance during power operation given as 38 h in LO2 the special report 1/97.

Obs. The work permit on the preventive maintenance 22RL97D001 during the LO2 maintenance outage caused a "complex LCO" for LO unit 1 when the unit was restarted from its maintenance outage and brought to the power operation state on 21.9.1997? (It should be noted that LCOs allow one inoperable redundant subsystem out of two, up to and including the plant operational state of hot readiness. AOT for single subsystem repair is 21 days?)

Incident's significance in terms of nuclear, personnel and radiation safety:

The follow up evaluations of temporary and integrated risk increases due to the unallowed preventive maintenance 13.1.1997-14.1.1997 during power operation of LO2 were done by using PSA in the LO2 special report 1/97.

Based on their evaluation, the plant considered the incident's safety significance as minor.

Obs. This Loviisa risk follow-up approach of safety related incidents is considered as an exemplary approach and well complements the "deterministic" FSAR, TS and INES based safety evaluations.

Obs. From the employees' safety point of view it should have been evaluated how an outage maintenance work package was restored operable by the control room although an underlying work order was unfinished.

Necessary immediate and long term corrective actions and their expected effects:

1) The work order transfers from the outages will be handled within the maintenance branches and the activities will be described in approved maintenance activity procedures (done in the "work order and planning routines" 82-07-001/ M4/6.5.1998)
2) The formal responsibilities concerning changes in work orders and permits (e.g. transfers) in the maintenance activity procedure 82-07-001 should be defined and training arranged (The root cause analysis group considers the procedure as a very large one and recommends its division into parts).

   The evaluators recommend additionally that the large and complicated guide on work order and planning routines should be formally modelled as a process in order describe the maintenance routine in a more understandable, structured and simpler way. This could also facilitate a better identification of the possible need of additional defensive barriers as well as smoothing up the maintenance planning, work order and operability verification process.
3) *No work permits shall be given for work orders corrected by hand notes. Transferred work orders shall be deleted and new ones done. The list of works transferred from the maintenance outage shall be reviewed by the safety engineer.*

   Obs. The evaluators recommend additionally that the routines for safety and correctness checking and approval of changes in the work planning and work orders are evaluated and enhanced on demand.

   Obs. The evaluators recommend additionally that the routines for work completion inspection prior to operability testing are checked and enhanced if need be.
4) *The evaluators recommend additionally that additional training on technical specification rules and their understanding of the work planning personnel and maintenance foremen should be considered, if need be.*

   Obs. Corrective Actions proposed in the inspection report(s) should be completed with expected effects and structured to correspond the list of identified Causes in order to help understanding and the prevention of recurrence.

Event recording and classification system (the event report is completed with classification for searches and periodic event data analysis purposes):

Obs. The special reports submitted to the regulatory body include a number of classification codes which could facilitate a later search of specific event types and possible recurrent causes.

Obs. In the classification list, several causes could be given, especially in case of a complicated event sequence. The cause action classification list in the Human Failure Report should preferably be refined to include options for Design Deficiencies and Changes, and Work Planning Deficiencies and Changes.

Reference to other related investigations, such as work orders and failure reports:

An exemplary list of references is in the root cause analysis report.

8 EVALUATION RESULTS

8.1 Radiation and Nuclear Safety Authority

8.1.1 Evaluation of the organisational framework and investigation practices

The goals of Radiation and Nuclear Safety Authority's (STUK) investigation practice were only partly documented and of rather general nature. In addition, a clear policy statement and action plan on how to proceed in practice were missing. On the one hand, licensees were encouraged to enhance and develop their practices on a voluntary basis. But on the other hand, a pre-scriptive approach towards regulation was nevertheless considered necessary. It was concluded that although the present policy has contributed to the introduction and use of more elaborate event inspection methods at Finnish nuclear power plants, it has also resulted in a situation in which power companies have expected STUK to be able to identify possible deficiencies in their investigation methods or practices (on the grounds that their reporting arrangements appear to have been geared to satisfy STUK's requirements rather than their own reporting needs. Under the last few years Fortum and TVO have nevertheless assumed a more active role in this respect). STUK's area of responsibility and main duties as well as the division of liabilities between STUK and the licensees were anyway clear to all parties.

STUK did not have any explicit performance indicators for measuring the effectiveness of its investigation practice. Effectiveness was of course being assessed on a more qualitative basis, e.g. on ground of the degree to which STUK had managed to contribute to significant improvements at plants. How this information was being used remained an open question, however. Liabilities in relation to STUK's own investigation activities appeared to be clearly defined.

STUK has a good access to plant information through its resident site inspectors and the formal reporting system described in YVL 1.5. Criteria for initiating an investigation have been explicitly defined but there seems to be no formal procedure for the initial assessment of new events and observations. The reliability of the assessment process seems to be dependent on the individual know-how and experience of a relatively small number of senior officials.

The event classification model included in the data collection form was considered to be well developed. It was evaluated that the form provided a good framework and guidance for inspections, although employees of other branches did not always utilise the form in an appropriate manner. Since the form is to be completed on the computer, the event data was also automatically stored in STUK's Event Register Database, TAPREK. TAPREK appeared to be easy to use and to provide good support for various data retrieval operations. In this respect STUK was clearly ahead of TVO and Fortum (TVO and Fortum had well developed information systems for the treatment of failure data but their operational events were usually registered as separate text files and were not usually entered into any plant level database to contain all events and failures).

STUK did not conduct systematic or regular reviews of the existing operational event data. In connection with the inspection of a particular case, the case officer is however supposed to pay attention to indications of corresponding events and failure mechanisms in the past, which are to be itemised in the TAPREK report. There is no procedure for such a task, however. In consequence, it is very much up to the inspection team members and the case officer to what extent and

how TAPREK is utilised. STUK has nevertheless purchased research services from other research institutions e.g. for identification and analysis of common cause failure mechanisms in the maintenance data and in some special reports.

STUK appeared to have enough competent personnel to run the event investigation practice. Interested employees are encouraged to join in the practice, and training was provided on-the-job. It was noted, however, that the practice was suffering from lack of focus and inadequate allocation of work and resources. For instance, inspectors find it difficult to concentrate on their work because of increased number of other assignments and duties for inspection of operational safety. It was estimated that such fragmentation is likely to decrease efficiency and motivation as well. However, in this study no signs of deteriorating performance were identified. Development activities were not supported by regular reviews or audits at the time of this study.

8.1.2 Evaluation of applied inspection methods and selected inspection reports

The event classification model included in the data collection form provided a good framework for the evaluation of STUK' methods for the inspection of new events and the follow-up analysis of significant incidents.

Based on the case specific evaluation, it can be noticed that the inspection reports have a clear outlining format and structure, the describing text is usually of good clarity, and the event classification model has potential to outline what, how and why had happened. The report format and its classification scheme were suitable for periodic data analysis needs, and adequate references to the utility reports sent to STUK were given.

A more detailed analysis of the TAPREK inspection and reporting practice resulted in the identification of the following deficiencies and improvement proposals:

- The original parts of the event sequences, the originating failures and causes should be better studied in the case of latent failures.
- A distinction between preliminary and final inspection reports from the utilities to STUK should be considered ("similar" to the Swedish reporting routine of safety related occurrences, i.e. the RO reporting routine).
- In the description and follow-up of the corrective actions taken by the utilities more attention should be paid to expected and achieved effects of those actions.
- Work planning deficiencies (not only design deficiencies) should be itemised in the classification model of corrective actions, failure events and error causes.
- Lacking or broken defensive barriers (technical and organisational) should be surveyed more thoroughly in the inspection reports, more attention should be given to the potential barrier options given in the classification model.
- Pilot data retrieval operations on grounds of a selected combination of classification codes and free text information on the TAPREK forms are recommended for enhancing the identification of recurrence and trends of safety significant failure modes, problems and events, and facilitating benchmarking between the units (Objective: periodic TAPREK experience reports?).
- Categorisation of events and their reporting ambition into different classes according to their relative importance could be considered (compare with SKIFS 1998:1 or precursor studies). In this respect the INES classification system appears to be too general.

8.2 Teollisuuden Voima Oy

8.2.1 Evaluation of the organisational framework and investigation practices

It was evaluated that the goals of Olkiluoto power plant's (TVO) event investigation practice were in general clearly and explicitly defined and documented. A pro-active approach towards safety was being emphasized and the prevention of the recurrence of events was generally regarded as a very important objective for the practice. However, it was not quite clear to what extent TVO's key per-

sonnel did share a common view of what kind of operating experience feedback policy they should adhere to in the future.

TVO did not have any particular indicators for the effectiveness of its event investigation practice. Nevertheless, it was concluded that the major problems of the practice had been identified and that in general people tended to be well aware of what was going on at the plant. An overall impression is that TVO is clearly in the process of strengthening its event investigation competence.

Liabilities appeared to be clearly defined but very decentralised. It can be said that until recently TVO's event investigation practice had not been organised nor understood as a *process* with one process owner (i.e. responsible person and/or unit) clearly in charge of all related activities at the plant. Instead, the investigation practice consisted of a set of distinct activities to be carried out in different offices, branches and informal groups without firm co-ordination. That was regarded as an obvious deficiency. According to the authors' impression the situation made it rather difficult to manage cross-functional activities and to fully utilise existing knowledge. In addition, the Group for Operating Experience (KÄKRY) did not appear to command much formal authority in the organisation and could not therefore influence the implementation of proposed corrective actions in an efficient way. However, during the execution of this study TVO carried out changes in its organisation which are likely to alleviate these problems. For instance, there was an obvious intention to establish the process ownership concept into practice and to provide the Chairman of KÄKRY with a larger overall responsibility for TVO's event investigation activities.

TVO had several procedures for the threatment of operational events, technical failures and other deviations depending on their characteristics and safety significance. It was evaluated that in general the assessment of both internal and external operational event reports, major technical failures and other events that were brought to KÄKRY's consideration did work well. Moreover, the procedure for the treatment of technical failure data was evaluated to be relatively good although it did not contain specific instructions to support recurrence and common cause failure detection, and although decentralised liabilities and consequential difficulties in task co-ordination posed a challenge to its implementation.

There was no common plant level document to provide a comprehensive overview of the existing event and failure recording, assessment and investigation activities at TVO. In consequence, for an outsider it was rather difficult to figure out how different assessment procedures actually related to each other, and what usually happens (or is supposed to happen) before the event ends up on KÄKRY'a agenda (especially if the event is of non-technical nature and if its safety importance is uncertain). It is worth emphasizing that although KÄKRY's sphere of responsibilities was very well documented, KÄKRY did not concentrate on the assessments of *new* internal events and observations. KÄKRY's focus was on the assessment of event reports, i.e. cases that have *already* been inspected to some extent. This led to a conclusion that TVO's practices in relation to the recording and initial assessment of events and observations were not as explicit and transparent as they could possibly have been. For instance, the process near-miss reporting practice introduced during the carrying-out of this study in 1999 was not referred to in other event investigation instructions.

TVO's root cause analysis method is MTO and it was well documented. However, many interviewees were of the opinion that the MTO procedure was heavy and rather "displeasing" to the plant personnel. This was reckoned to be one reason behind the fact that the number of completed MTO reports had remained low and sometimes delayed during the recent years.

Maybe the most difficult part of this study related to assessing how the treatment of recurrent failures and common cause failure (CCF) mechanisms was organised at TVO. This difficulty was in part related to complex and non-transparent procedures as noted above, and in part the fact that TVO's personnel had different and sometimes conflicting views on the issue. The authors' conclusion is that TVO did not have *regular and systematic* procedures for the identification and analysis of recurrence or CCF mechanisms in the *operational event data*.

The conclusion was based on the following

observations: First, many of the representatives of TVO were of the opinion that their recurrence and CCF detection activities lacked systematisation and that in the absence of a systematic practice such events were mainly identified randomly in particular situations. Secondly, the deputy Chairman of KÄKRY stated that they did not analyse historical or concurrent recurrence on a regular basis. Thirdly, recurrence or CCF mechanisms were not explicitly mentioned in TVO's instructions for internal event reporting (0-KC-00-47/8) or treatment of operational event reports (0-S-O-16/2). In consequence, it was concluded that existing measures to identify recurrence or CCF mechanisms in the operational event data had to be based more on situation specific needs and campaigns or individual initiative rather than on a well established and regular practice. This is a clear deficiency that ought to be paid more attention to at TVO.

However, the situation is not that straighforward. At TVO the main responsibility for the assessment of recurrence and CCF mechanisms belongs to the case officer in charge of the concerned event report. The Head of TVO's Operational Safety Branch assured that the system worked sufficiently well. It appeared, too, that KÄKRY had addressed recurrence in connection with particular case studies, and that concise summary reports on reactor trips and special reported cases had been occasionally prepared for internal use. In addition, the recent ASSET mission in 1998 covered all operational events reported to the regulator between 1993 and 1997, and resulted in a comprehensive analysis, classification and ranking of pending safety and operability performance problems. TVO also had a procedure for a systematic treatment of *failure data* stored by means of notices of defects, work orders and failure reports in the computerised Work Order System. That procedure obliged responsible maintenance foremen together with technical experts to search for signs of recurrent and multiple failures from the system and to process their findings into summary reports and proposals for corrective measures. Therefore it is fair to say that TVO had invested time and efforts in this area, too.

Prior to the recent ASSET self-assessment and peer review conducted in 1998, TVO has not had a systematic practice for the follow-up analysis of completed event reports. Provided that the ASSET system will be introduced into regular use at TVO, that it will be used for the follow-up analysis of completed event reports on a regular basis, and that the analyses will also cover such "minor events" as process and labour protection near-misses that are not normally reported to the regulator, the event investigation process as a whole will become more organised. Such an arrangement would also facilitate the carrying-out of comprehensive periodic operating experience reviews in the future.

Apart from the identification and treatment of recurrent failures it was evaluated that KÄKRY does good work in assessing both internal and external inspection reports, requesting statements, recommending corrective actions and supervising their implementation. KÄKRY has an important role in conveying the lessons learned to the rest of the organisation e.g. by carrying out development campaigns in particular problem areas.

In connection with the analysis of operational preconditions it was noticed that at least from the interviewees' point of view the event investigation practice lacked focus and resourcing. People appeared to have many simultaneous assignments of which many were to be conducted more or less like "side-line" duties. Instructions were usually clear and easy-to-read but they did not provide the reader with an overall view of the practice. In addition, there seemed to be discrepancies between the written word and the actual operating procedures. On the other hand, it can be concluded that TVO was progressing in the fields of training, reviews and development activities. TVO had no academically trained behavioural scientists on its payroll but it had invested in its own human factors training. In addition, TVO purchased related consulting services which in part alleviated lacking resources.

8.2.2 Evaluation of applied inspection methods and selected inspection reports

The ASSET self assessment and peer review of 5 years' operating experience performed at TVO during 1998 provided a good possibility to compare its analyses and results with the evaluation results of this study.

Follow-up analysis of incidents

The ASSET follow-up analyses of reported events conducted by TVO exhibit a high quality. The method and format for doing ASSET event analysis report summaries on single events is systematic and good. However, additional improvement proposals and needs appear:

- The ASSET format facilitates event description with a chronological list of occurrences, but only one of these occurrences per event analysis was selected for further scrutiny, i.e. the analysis of direct and root causes. However, in many cases, several significant causes in the event sequence can be identified and analysed by the method.

Periodic review of operating experience and identification of recurrence

TVO ASSET self assessment comprised a good and systematic review of 132 events occurred/reported to the regulator during 1993-97.

- In addition, the entire population of events (not only those that have been reported to the regulator) should be systematically identified (incl. other important events identified during refuelling outages and failures entered into the Work Order (TTJ) system) and analysed in order to identify new significant "latent" events and to further enhance the safety and operability of the plant. Ordinary "single failures" may involve common failure modes, recurrent and multiple defects building up "organisational problem events or nearby failures". Thus they should undergo a systematic analysis for the prevention of recurrence (Laakso, Pyy & Reiman, 1998). One reference of periodic operating experience review on reactor trips was already in use for self assessment at TVO.

Besides, the systematic analysis of the operating experience of motor operated valve drives showed that symptomatic repairs were usually directed to individual equipment, and that root causes were not well corrected on either them or similarly affected equipment (Hänninen & Laakso, 1993). In this study some of these remedial needs are justified, and they can be recognised from the ASSET self assessment results, too.

- Starting up the collection and analysis of failure data according to the TVO guide (0-KC-U3-21/2) on grounds of the TTJ information system is strongly encouraged. In addition, the utilisation of modern data analysis tools to retrieve and compile selected data by using classification codes or free descriptive text searches would be beneficial in a similar way as already demonstrated for the TUD data.
- Periodic operating experience assessments should also be directed to human and organisation related problems and not limited to the technically oriented way of analysing problems (Bento 1997).
- Now the ASSET self assessment report presents only a ranking of pending problems at general level and a list of several remaining actions. However, the ranking (priorisation) of the actions which compete for the same resources and personnel attention has been missing. The newly introduced a ranking list "10 at top" may help the resource allocation at the plant meeting and implementation.

The ASSET self assessment showed how well repairs to eliminate the pending local problems (symptoms) and the remedies to prevent recurrence were implemented. The recurrence of failures was too high.

- It is recommended that in addition to problems and action programs, also the expected and achieved operability effects of proposed and implemented actions should be more closely addressed by e.g. KÄKRY.

Root cause analysis and other event reports relating to the selected cases

Following deficiencies and improvement proposals of the incident inspection methods and reporting could be still identified:

- The threshold between root cause analysis and other operational event reports should be established and more clearly based on their significance.
- The initiating parts of the event sequences, the originating failures and causes should be better studied in case of significant initiating events and latent failures. Analysis of primary causes and errors committed in originating work tasks, with respect to possible common causes such as deficiencies in work planning or engineering specification, should be pinpointed.
- The analysis criteria on activity, procedure and human related problems causing incidents are not comprehensive. The root cause analysis should include human and organisation related problems and should not be limited to the technically oriented way of analysing the problems.
- Failed or broken defensive barriers (technical and organisational) should be surveyed in root cause reports more thoroughly and illustrated by simple and informative block diagrams (In the recent years' root cause analyses, i.e. MTO analyses, the useful but resource demanding task of preparing event and cause analysis diagrams seem to lack in many cases).
- Thus a systematic method for root cause analysis (e.g. based on MTO and ASSET philosophies) should be established into routine use at TVO. Additional training is necessary for an efficient use and understanding of advanced root cause analysis methods, if they are not used by event analysis specialist only.

It is important to learn an incident inspection and reporting methodology capable of dealing with a large number of events with a relative ease. TVO plans to continue internal reassessment of operating events using the ASSET methodology which should be encouraged.

- The evaluators recommend TVO to start to apply the ASSET event analysis format to analyse the inoperability failures in the systems and components, involving LCO requirements of the technical specifications, in addition to those events that have been described in the quarterly reports. Identification and monitoring of possible trends and recurrent failures in safety systems should be facilitated, and the recognition and implementation of remedial actions should be emphasised, too.
- The same or a simplified version of the ASSET analysis routine, taking into account the several causes approach, could also support / provide a feasible framework and methodology for follow-up analyses of other internally reported noteworthy events which mainly originate from the refuelling and maintenance outages.
- *Complementing of internal* classification codes into the incident inspection reports is recommended to enhance understanding of the safety and operability significant failure modes, problems and events, and to support better identification of their recurrence or multiplicity.

8.3 Fortum Power and Heat Oy

8.3.1 Evaluation of the organisational framework and investigation practices

It was evaluated that the goals of Loviisa power plant's (LPP) event investigation practice were in general clearly and explicitly defined and documented. A pro-active approach towards safety was being emphasized and the prevention of the recurrence of events was generally regarded as a very important objective for the practice. In addition, the main investigation policy alignments e.g. in relation to the role of the Plant Safety Branch (PSB) and other units were well articulated and evidently applied in practice, too, although not always documented. It appeared that quantitative indicators had not been developed or sufficiently used for assessing the effectiveness of LPP's event investigation practice. Like in case of TVO, prevailing performance measurement systems were mostly too general to provide the practice with precise and useful feedback. It was assumed, however, that the application of regular quality assurance reviews as well as the annual internal

operating experience feedback reports partly compensated that deficiency.

Liabilities were clearly defined. In addition, the event investigation practice was partly organised in a form of process, including a nominated process owner and a documented procedure on how to proceed from event recognition through assessment and reporting to the implementation of corrective measures and their evaluation. This was regarded as a big plus and a definitive advantage for the practice. Certain amount of redundancy in work was detected mainly because of the overlapping responsibilities of the PSB and the Quality Assurance Branch (QAB). Although it was speculated that the situation was likely to make it more difficult to utilise the existing operating experience data, the Safety Engineer in charge of the event investigation practice (SEE) assured that the feedback loop was functioning well and that he could take the full advantage of existing results.

In general, PSB appeared to have a firm status at LPP as well as enough integrity and independence to adhere to an operating policy of its choice. PSB seemed to be proficient in managing cross-departmental activities, too, e.g. in mobilising the line organisation in the investigation practice.

The recording and assessment of new events and observations was relatively well organised at LPP, thanks to the Operational Event (KT) reporting practice. It appeared to provide a feasible tool for the treatment of all kinds of deviations, including those that cannot be necessarily attributed to any particular systems or equipment failure. KT reports lay good foundations for a systematic assessment and classification of operational events as well, but at the time of this study the assessment procedure itself was rather informal and highly dependent on the SEE's personal know-how and judgement. It was concluded, too, that the compilation of Human Failure Reports was not closely related to the mainstream inspection and development activities.

At LPP root cause analysis tools and methods can be chosen on the basis of case specific needs. In principle that's OK, provided that the necessary methods expertise is available. In addition, it can be presumed that there is a documented and approved procedure for each method that the licensee has used or may use. It was noted, however, that LPP's current root cause analysis method, a modified version of HPES, was not documented. A reference was given to HPES training material but it was not in Finnish, nor included a precise description of the prevailing practice, either. Moreover, LPP's root cause analysis reports reviewed as part of this study did not include references to any method, although they should have included according to LPP's existing root cause analysis instruction. These are clear procedural deficiencies to be corrected irrespective of the adequacy of achieved inspection results.

Another procedural deficiency has to do with the identification of common cause failure (CCF) mechanisms. There are no instructions in writing to specify concrete procedures or arrangements for CCF *detection*, although some attention has been paid to the treatment of already *identified* CCFs. However, the SEE seems to invests a lot of his time in (manual) screening of existing operational event data. On the other hand, "ordinary" technical failures entered into the Loviisa power plant information system (LOTI) were not subject to any systematic CCF screening activities although LOTI itself could provide a good support for them. Nevertheless, by means of the regular quality assurance reviews LPP seemed to have a possibility to gather information on the historical recurrence of failures relating to particular functions or organisational branches.

It was concluded that LPP was relatively strong in the area of investigation result utilisation. According to the authors' evaluation LPP had adequate arrangements for assessing the safety implications of inspection results, for processing proposed enhancements and supervising the implementation of recommended actions, and for evaluating the effectiveness of enhancements in particular functions, systems and equipment. This is largely based on the active role, clear agenda and decisive authority of the LPP Quality Assurance and Safety Meeting, but also on the fluent cooperation of safety and QA functions. Accordingly, a big plus to LPP.

There seemed to be enough competent people to take care of investigations, and their average workload did not seem to be too high. On-the-job type of training appeared work quite well, too, on the grounds that the SEE was visibly proud of

their achievements in that area. However, LPP had not considered it necessary to recruit any academically trained behavioural scientists so far. As a result, and like in the case of TVO, a selected group of engineers took care of human factors related issues on the basis of practical experience, training, and the use of common sense. It must be emphasized, however, that this study did not give rise to any particular doubts about LPP's capability to address those issues in an appropriate way. In the area of information technology there were nevertheless much more to be done. Current systems were not very well integrated and they did not provide the event investigation practice with sufficient support especially when it comes to data analyses.

8.3.2 Evaluation of applied inspection methods and selected inspection reports

The KT (Operational Event) reporting system provides a good and standardised structure for screening and identification of significant events at the Loviisa NPP (see Appendices). KT reports define the further reporting needs e.g. by indicating whether a special or root cause analysis report has to be prepared. Until the end of 1998, a KT report had been prepared for altogether 207 events. Most of the KT reports fall below the official reporting threshold specified by the regulator. For instance, less than 20 % of the KT reports completed in 1998 related to such events that required official reporting to STUK.

Follow-up analysis of incidents

The PSA Human Failure Reports (in the analysis also referred to as iv-reports) are follow-up analyses of those KT reported events that exhibit human failures. In the recent years about half of the KT reports have resulted in a Human Failure Report. It appeared, too, that an increasing portion of all KT reported events also result in a Human Failure Report (which is a good thing). Human Failure Reports include a detailed classification of identified errors, and information on their discovery, causes, impact on safety systems including the redundancies, and preventive actions (see Appendices).

The Human Failure Reports are aimed at identification of human errors and CCFs for the PSA studies (Jänkälä, Vaurio & Vuorio, 1987). They are stored in the LOTI information system, but were not used for any periodic, human error related, operating experience review at the time of this study. Some recommendations for consideration:

- The search of recurrent error causes and problems could be facilitated by the help of the existing human failure classification codes and their underlying KT event report information. The next step could be a trend analysis of dominant human failure related events and an evaluation of the effects of the corrective actions and remedies to prevent recurrence.
- The present human failure classification model of error causes should be complemented by introducing options for Design Deficiency and Work Planning Deficiency. The classification of involved working groups should consequently be completed by introducing options for the Design branch and Work Planning branch.

Periodic review of operating experience and identification of recurrence

The Olkiluoto ASSET self assessment comprised a good and systematic review of 132 events' population occurred during 1993-97. There was no corresponding method or practice at the Loviisa NPP. It is important to learn an incident inspection methodology capable of dealing with a large number of events for identification of recurrence with a relative ease.

- FORTUM should consider to perform a similar or corresponding periodic self-assessment of operating experience when a population of five years' KT reports is available,
- In addition to KT reported events, also selected work orders should be analysed in order to identify new significant "latent" events and to further enhance the safety and operability of the plant.
- Continuing and further developing the ways of collection, classification, analysis and utilisation of failure data according to the Loviisa

power plant maintenance planning, maintenance optimisation and plant lifetime management routines, and periodic maintenance reporting are strongly encouraged. The utilisation of modern data analysis tools together with the application of adequate classification codes and event descriptions is in this respect necessary.
- Periodic operating experience assessments should also be directed to human and organisation related problems and not be limited to the technically oriented way of analysing problems (Bento, 1997).
- It is recommended that in addition to problems and action programs, also the expected and achieved effects of proposed and implemented actions should be more closely addressed.

Operational Event Reports and root cause analyses relating to the selected cases
- KT reports: a field on Causes should be added to the KT report to steer further event investigations and reporting.
- The KT report does not include any formal classification model to support periodic operational experience reviews, systematic identification of recurrent events or their causes, or ranking of corrective action programs.
- A systematic classification of event's relative significance (a more detailed one than in the INES scale) should be considered for the KT reporting for outlining the event significance, information and facilitating further data searches.
  Remark: The special reports submitted to the regulatory body include a number of classification codes which could facilitate searches of specific event types and possible recurrent causes.
- Root cause reports: The initiating parts of event sequences, the originating failures, and causes should be better studied in case of latent failures. Analysis of primary causes and errors committed in tasks in which the errors were committed, with respect to possible common causes such as deficiencies in work planning or engineering specification, should be pinpointed.
- The analysis criteria on activity, procedure and human performance related problems are not comprehensive enough. In general, human and organisational factors should be more clearly addressed in the root cause analysis reports.
- Failed or broken defensive barriers (technical as well as organisational) should be more thoroughly surveyed, and could be illustrated by informative block (event sequence, cause and barrier) diagrams.
- Thus a more systematic method for root cause analyses and reports (e.g. based on HPES/MTO and ASSET philosophies) should be established, documented and implemented for routine use.

9 CONCLUSIONS AND RECOMMENDATIONS

9.1 Radiation and Nuclear Safety Authority

Major advantages and good practices

The Finnish regulator, STUK, has contributed to the introduction and use of more elaborated event inspection methods and practices in the Finnish nuclear industry, especially in the 90's as STUK's own event investigations started. STUK has a good access to plant information and operational event data. STUK has established a good framework for its own investigation practice through clear and well documented inspection and event classification criteria. The TAPREK database is a good and usable information system and provides substantial support for the practice. Generally there are enough competent personnel for the carrying-out of own selective incident investigations, reviewing utilities's inspection practises and reporting, and motivating them to further develop their incident analysis methods and practises.

Major deficiencies and their consequences

1. A clear policy statement and an action plan for STUK's own event investigation practice was missing. From the licensee's point of view this means difficulties in anticipating STUK's expectations, reactions and demands in advance although YVL 1.5, i.e. the guide that determines the official reporting requirements, had established its position in the Finnish nuclear power community. When it comes to STUK itself, it seems probable that this deficiency has at least partly contributed to their problems in task allocation and internal development campaigns in general.
2. It was concluded that STUK's stringent and prescriptive supervisory approach with only minor common R&D efforts with power companies does not encourage initiatives at plants. In addition, the development and introduction of new (voluntary) practices at plants easily result in excessive paperwork and/or in a situation in which the plant should be prepared to run several overlapping and resource-consuming processes at the same time to meet its own inspection needs and to fulfil the formal reporting requirements issued by the regulator.
3. STUK did not have any explicit performance indicators for evaluating the effectiveness of its investigation practices. As a result, it is difficult to gain reliable information on the degree to which the practice reaches its goals. On the other hand, since STUK's goals were only generally specified at the time of this study the introduction of a developed performance measurement system would anyhow have been a very difficult task to accomplish.
4. STUK did not conduct regular and systematic reviews of the bulk of existing operating event data in addition to some limited efforts done earlier by the senior officials. Given the fact that also the licensees' data analysis activities were lacking systemisation, it is quite obvious that a number of important recurrent, common cause and latent failure mechanisms are yet to be identified at Finnish nuclear power plants.
5. The event investigation practice lacked focus and the inspectors suffered from fragmented job descriptions. It is estimated that this is likely to have a negative impact on the coverage, thoroughness and methodicalness of STUK's event investigation practice. However, this study did *not* indicate any concrete signs of such negative developments so far.
6. There were no regular audits or R&D projects. This means that the success of various development activities is very much dependent on senior officials' personal views and engagement.

Recommendations

1. Reconsider and document the main goals of the practice in a more precise way, evaluate the adequacy of the current prescriptive approach and issue an open policy statement and action plan to specify the main operating principles of the practice.
2. Consider together with the utilities to conduct an independent analysis of occurred human and organisational related incidents. This could yield interesting results from the task performance, procedure or defensive barrier failure point of view.
3. Develop performance measurement of the practise, pay more attention to periodic and systematic data analyses and utilise the potential of the TAPREK system more efficiently.
4. Ensure that inspectors can concentrate on their work in accordance with the prevailing and also future policy alignments.
5. Introduce a regular auditing practice and engage in benchmarking excercises with other regulators, and establish joint R&D (i.e. not only assessment) projects with utilities and researchers.

9.2 Teollisuuden Voima Oy

Major advantages and good practices

TVO's goals were clearly defined and documented. KÄKRY has an important role in conveying the lessons learned to the organisation and campaigning in particular problem areas. Co-operation with Swedish utilities and research organisations has potential for sharing useful information. A no-blame investigation atmosphere contributes to the quality of inspection results. The new process near-miss reporting practice provides a sound framework for the recording and assessment of novel events and observations of non-technical nature. There is a clear emphasis on personnel training, reviews and development activities.

These advantages are demonstrated by the progressive ASSET self assessments and plans for a systematic collection and analysis of failure data. TVO is clearly in the process of strengthening its event investigation and identification competence.

Major deficiencies and their consequences

1. TVO has no particular performance indicators for evaluating the effectiveness of its event investigation practice. In consequence, it has been difficult to gain reliable information on the degree to which the practice reaches its goals (which were precisely defined and documented).
   Remark: The recently performed ASSET self assessment of operating experience indicates a high recurrence of failures and presents therefore both a kind of indicator of the overall effectivess of TVO's operating experience utilisation process and an extensive list of remaining actions.
2. The event investigation practice lacked process qualities which was characterised by the dispersion of responsibilities into different offices, branches and informal groups. This in turn had resulted in various problems of task co-ordination and co-operation. In consequence, existing information and available resources were not utilised as efficiently as they could have been utilised.
   Remark: As a result of a recent organisational change, the Chairman of KÄKRY has a larger overall responsibility for TVO's event investigation practice and related activities. The process ownership concept is now being emphasised.
3. The recording and assessment of new internal events lacked systematisation and clear operating principles. There were various possible reporting channels but no common plant level document to clarify their mutual interconnections to provide a big picture of the system. It was evaluated that due to this complexity there is an *increased probability* that events and observations with uncertain technical origin and of minor immediate safety significance will remain unrecorded and/or without proper further assessment.
   Remark: The new process near-miss reporting practice is aimed to reach such events that do not necessarily require official event reporting to the regulator or relate to any particular equipment failure. This is an obvious improvement. However, still more work is required to enhance the transparency of TVO's event recording and assessment system in general.

4. There were no *regular and systematic* practices for identifying recurrence or common cause failure (CCF) mechanisms in *the operational event data*. Manifestations of such mechanisms were therefore likely to be treated as single events or failures, and the probability of not identifying the actual root causes of those events was consequently estimated to be relatively high.
   Remark: Recurrent faults and CCFs have been addressed in the procedure for the collection and analysis of failure and maintenance history data. In addition, both operational event and technical failure data have been subject to several data analysis campaigns with varying scope and intent.
5. KÄKRY, the Group for Operating Experience, did not command much formal authority nor decisive position in the organisation, and the event investigation practice as a whole appeared to lack focus and adequate resourcing. The key personnel seemed to suffer from their fragmented job description, characterised by a large number of various additional assignments of which many directly related to the investigation practice itself. Lack of formal authority made it difficult to influence the processing and implementation of requested clarifications or corrective actions in responsible organisational units.
6. In general, a clear distinction between the formal procedures and the actual practice was detected. In the long run such a situation will eventually decrease the stature of existing instructions in general which in turn is likely to increase risk levels in other safety significant operations.
   Remark: This is especially true with regard to the application of the current MTO root cause analysis procedure. The procedure itself was comprehensive and well written but deficient implementation and lack of well trained personnel have resulted in signs of degradation of the inspection quality as well as delays in root cause reporting.

Recommendations

1. Assume a process view to developing the investigation practice. Provide the Chairman of KÄKRY with necessary resources and authority to enhance task co-ordination and exchange of information. Define and develop TVO's core processes by establishing stronger links between single tasks and more general objectives of operation.
2. Develop performance measurement. With regard to this objective try to specify and operationalise the existing goals of the practice.
3. Proceed with the recent process near-miss reporting practice. Give more emphasis to simplyfying event recording and assessment procedures. Document their mutual interconnections e.g. by means of a general plant level procedure to cover all event investigation and reporting activities at TVO.
4. Create a more systematic procedure for the identification of recurrent failures and common cause failure mechanisms, especially when it comes to the *failure* event data.
5. Develop information technology based tools to support greater data integration. Take a tailored ASSET method and related computerised tools into regular use so that they meet both TVO's and STUK's needs concerning event inspections and reporting, follow-up analyses and periodic operating experience reviews.
6. Make sure that the results and recommendations of inspection reports, reviews and audits are taken into account, that approved enhancements are implemented and that their effects are followed up. In this respect consider providing KÄKRY with greater authority to influence implementation.
7. Pay attention to task allocation and try to reduce the amount of "side-line" duties. Get rid of instructions that do not work in practice and develop instructions together with practices. These problem areas can, and should, be addressed in connection with more general process development activities.
8. Create a strategy document for the operating experience feedback process (including goals, acceptance criteria, action plan etc.). In general, the incident analyses have well identified the means to eliminate the direct causes by repairs, but still more emphasis should be given to prevent recurrence by implementing remedies. A more effective feedback can be achieved by focusing the root cause analyses on significant events, the work tasks in which the

originating errors occurred, and the weaknesses of defensive barriers, and by implementing periodic operational experience reviews (such as ASSET self-assessment).

9.3 Fortum Power and Heat Oy

Major advantages and good practices

Fortum's goals were clearly defined and documented, and the main investigation policy alignments were well articulated and apparently applied in practice, too, although not always documented. The practice possessed process characteristics including a nominated process owner and a clear action plan resulting in a practical distribution of tasks and co-ordination of activities. The event investigation practice appeared to have enough independence and integrity.

The prevailing Operational Event (KT) reporting practice provided a sound framework for the recording and assessment of novel events and observations. The Human Failure Reports contained a fairly comprehensive event classification model that could be tailored for analysing all significant operational events. A no-blame investigation atmosphere contributes to the quality of inspection results and the line organisation was successfully mobilised to contribute to the event investigation practice. Personnel training appeared to have been successful, and enough resources had been allocated to the practice.

The regular quality assurance audits provided information on the historical recurrence of failures and made it possible to monitor performance in specific organisational branches and functions. In addition, investigation results were assessed and utilised in a fairly systematic and authorised manner.

Major deficiencies and their consequences

1. Fortum has no particular performance indicator system for evaluating the effectiveness of its event investigation practice. In consequence, it is difficult to gain reliable information on the degree to which the practice reaches its goals (which were precisely defined and documented).

   Remark: However, the recent annual reports of internal operating experience feedback provide valid summary and trend information, i.a. on the number of internal operating event reports, and the relative ratios of the official reporting to the regulator, to help assess effectiveness on a more general level.
2. Although the KT reporting practice provides a good support for the initial assessment of operational events, the assessment process itself is rather informal and very dependent on the responsible person's expertise and judgement. There is no explicit definition of an operational event, either, nor explicit criteria for their classification apart from the formal reporting requirements issued by the regulator. In consequence, a number of interesting events may remain unrecorded and consequently beyond further assessment. Nevertheless, the KT reporting practice as a whole works reasonably well and is certainly of significant benefit to the plant.
3. There is no detailed document in Finnish to describe how to conduct root cause analyses. This means that the coverage of completed reports as well as the treatment of cases may significantly depend on the person or team in charge of the inspection. This in turn is likely to have a negative impact on the average quality of the reports. In addition, reports compiled without any firm method or structure are more often difficult to understand, especially when one is searching for a particular piece of information or certain kind of phenomena from a larger ensemble of reports.
4. There are no instructions in writing to specify concrete procedures or arrangements for the detection of common cause failure mechanisms. This task is taken care of by a nominated person in charge of the event investigation practice. Any change in his position in the organisation may therefore change the situation as well.
5. Current information systems do not support comprehensive data analyses. The maintenance and operational event data are stored in different systems and the integration of existing information requires manual work. In such a situation the threshold for conducting time-consuming and laborious data analyses is obviously high-and again-dependent on the individual initiative.

Recommendations

1. Develop the performance measurement of the practise to further increase its effectiveness.
2. Develop the KT reporting practice to include a written procedure for an initial classification of recorded events and observations according to the characteristics of their consequences and immediate contributing factors. Itemise the Causes in the KT report form. Engage more people into the KT reporting practice, integrate the Human Failure reporting practice to the mainstream investigation activities and utilise that information more efficiently.
3. In general, the incident analyses have identified well the ways to eliminate the direct causes by repairs, but still more emphasis should be given to prevent recurrence by implementing remedies. A more effective feedback can be achieved by focusing on the root cause analyses of significant events, the work tasks in which the originating events occurred, such as design or work planning, and the weaknesses of defensive barriers, and by implementing periodic operational experience reviews.
4. Establish a formal procedure and computer aided tools for conducting and reporting root cause analyses to meet both Fortum's and STUK's needs and requirements.
5. Endeavour to alleviate the existing data integration problems. Take practical steps to renew the plant information system.
6. Establish a systematic procedure for the identification of common cause failure mechanisms.
7. Carry out a periodic plant level operating experience review by ASSET or some other feasible method and extend it to the KT reports, other underlying inspection reports as well as to screening of other applicable events to be identified from the present plant information system (LOTI).
8. Develop further the strategy document and include an action plan for the operating experience feedback process to support and direct prevailing data analysis and reviewing activities. This can be done e.g. on the basis of Chapter 12 (Utilisation of operating experience, treatment of deviations and corrective actions) of the current Quality Assurance Handbook.

REFERENCES

0-KC-00-47/8 (1995). Olkiluodon ydinvoimalaitoksen käytöstä laadittavat raportit. Ohje. Olkiluoto: Teollisuuden Voima Oy.

0-KC-OO-76/0 (1994). Häiriön selvittäminen Olkiluodon ydinvoimalaitoksella. Ohje. Olkiluoto: Teollisuuden Voima Oy.

0-KC-U3-21/2 (1998). Vikatietojen keruu ja analysointi. Ohje (luonnos). Olkiluoto: Teollisuuden Voima Oy.

0-S-O-16/2 (1997). Ydinvoimalaitosten käyttökokemusraporttien käsittely. Ohje. Olkiluoto: Teollisuuden Voima Oy.

0-S-O-23/1 (1996). Ydinvoimalaitostapahtumien perussyiden selvitys TVO I/II:lla. Ohje. Olkiluoto: Teollisuuden Voima Oy.

82-06-006/M3 (1997). Loviisa 1 ja 2, Käyttötapahtumien raportointi. Menettelyohje. Loviisa: Imatran Voima Oy.

82-12/M2 (1998). Laadunvarmistuskäsikirja. Loviisa: Imatran Voima Oy.

82-12-001/M5 (1997). Käyttötapahtumien käsittely ja hyödyntäminen. Menettelyohje. Loviisa: Imatran Voima Oy.

82-12-002/M2 (1997). Tapahtumien perussyiden analysointi. Menettelyohje. Loviisa: Imatran Voima Oy.

Andognini, G. (1998). Lessons from plant management for achieving economic competitiveness for evolutionary reactors. A paper for the IAEA Symposium on Evolutionary Water Cooled Reactors: Strategic Issues, Technologies and Economic Viability, Seoul 30 November – 4 December.

ASSET (1998). ASSET guidance for self assessment. Standard outline of the self assessment report. Report of the safety performance, safety problems and safety culture on the basis of the operational events. January 1998. Report by B. Thomas. Vienna: International Atomic Energy Agency.

Bento, J.-P. (1990). Kurs i MTO-analys. Nyköping: Kärnkraftsäkerhet och Utbildning AB.

Bento, J.-P. (1997). Analys av MTO-relaterade händelser i de svenska kärnkraftverken (1994–996). Nyköping: Kärnkraftsäkerhet och Utbildning AB.

Brolin, S. (1987). Forsmark 2. Analys av inträffade snabbstopp. 1985-1986: Vattenfall Forsmarksverket (PF rapport No. 125/87).

Brolin, S. (1988). Forsmark 2. Analys av rapportervärda omständigheter (enl. STF). Åren 1985-1988. Vattenfall Forsmarksverket (PF rapport No. 555/88).

Dahlgren, K., & Skånberg, L. (1993). Felaktigt utförd provning av rörböjar i system 321 (Rapport No. 8.13-930477). Stockholm: Statens Kärnkraftinspektion.

Ericsson, P.-O. 1999. Correspondence and examples on RO incident analysis and classifications with Per-Olof Ericsson and Ralph Nyman, Swedish Nuclear Power Inspectorate. 23.04.1999, 18.6.1999 and NKS/SIK-1(92)44.

Hawkes, N. (1999, January-February). Reporting risk: How the media do it. Nuclear Europe worldscan, pp. 35–37.

Hollnagel, E. (1998). Cognitive reliability and error analysis method (CREAM). Oxford: Elsevier Science.

HPES—Investigators Training Manual. (1992). Issue 1, December 1992. Pp. 53–61.

HSG65 (1998). Successful health and safety management. A guide prepared by the British Health and Safety Executive. Suffolk: HSE Books.

Hänninen, S., & Laakso, K. (1993). Experience Based Reliability Centered Maintenance - An Application on Motor Operated Valve Drives. Finnish Centre for Radiation and Nuclear Safety, In STUK-YTO-TR 45. ISBN 951-47-7171-0. 61 p.

Jacobs, R., & Haber, S. (1994). Organizational processes and nuclear power plant safety. Reliability engineering and system safety, 45, 75–83.

Jänkälä, K., Vaurio, J. & Vuorio, U. (1987). Plant specific reliability and human data analysis for safety assessment. Vienna. IAEA-CN-48/78.

Laakso, K., (1984). Systematisk erfarenhetsåterföring av driftstörningar på blocknivå i kärnkraftverk (A systematic feedback of plant disturbance experience in nuclear power plants). Otaniemi: Tekniska Högskolan, Institutionen för Energiteknik. Thesis.

Laakso, K, Pyy, P, Reiman, L. (1998). Human errors related to maintenance and modifications (Report No. STUK-YTO-TR 139). Helsinki: Radiation and Nuclear Safety Authority.

LO1&2 FSAR (1997). Loviisan voimalaitoksen turvallisuusseloste. Loviisa: Imatran Voima Oy.

Mankamo, T., Björe, S., & Olsson, L. (1992). CCF analysis of high redundancy systems. Safety/relief valve data analysis and reference BWR application (SKI Technical report 91:6). Stockholm: Swedish Nuclear Power Inspectorate.

NEA/CSNI/R(97)15/PART1 (1998). Improving reporting and coding of human and organisational factors in event reports. Issy-les-Moulineaux: Committee on the Safety of Nuclear Installations, OECD Nuclear Energy Agency.

NEA/CSNI/R(97)5/PARTS 1 & 2 (1997). Latent failures of safety systems. Issy-les-Moulineaux: Committee on the Safety of Nuclear Installations, OECD Nuclear Energy Agency.

NEA/CSNI/R(98)17, Vol. 1 (1999). Identification and assessment of organisational factors related to the safety of NPPs. State-of-the-art report. Issy-les-Moulineaux: Committee on the Safety of Nuclear Installations, OECD Nuclear Energy Agency.

NEA/CSNI/R(98)17, Vol. 2 (1999). Identification and assessment of organisational factors related to the safety of NPPs. Contributions from participants. Issy-les-Moulineaux: Committee on the Safety of Nuclear Installations, OECD Nuclear Energy Agency.

NEA/SEN/SIN/WG1(98)17 (1998). Modification and requalification problems following outages. Issy-les-Moulineaux: Committee on the Safety of Nuclear Installations, OECD Nuclear Energy Agency. Draft.

NKS/SIK-1 (1994). Safety evaluation by living probabilistic safety assessment and safety indicators. Final report of the Nordic Nuclear Safety Research Project SIK-1. Edited by Laakso, K. Copenhagen: Nordic Nuclear Safety Research (NKS).

NUREG/CR-6093 (1994). Barriere, M., Luckas, W., Whitehead, D., & Ramey-Smith, A. An analysis of operational experience during low power and shutdown and a plan for addressing human reliability assessment issues. Washington: U.S. Nuclear Regulatory Commission.

Rasmussen, J. (1993). Market economy, management culture and accident causation: New research issues? A paper for the Second International Conference on Safety Science, Budapest.

Reason, J. (1995). A systems approach to organizational error. Ergonomics, 38, 1708–1721.

Rochlin, G. (1993). Defining “high reliability” organizations in practice: A taxonomic prologue. In K. Roberts (Ed.), New challenges to understanding organizations (pp.11-32). New York: Macmillan.

Rollenhagen, C. (1998). Handledning i händelseanalys. Råcksta: Vattenfall Energisystem AB.

Shrivastava, P. (1992). Bhopal. London: Paul Chapman Publishing.

Simola, K. & Maskunitty, M. (1995). Loviisan voimalaitoksen laitossuojausautomaation vanhenemistutkimus (Report No. STUK-YTO-TR 86). Helsinki: Radiation and Nuclear Safety Authority.

SKIFS 1998:1 (1998). Statens Kärnkraftinspektionens föreskrifter om säkerhet i vissa kärntekniska anläggningar. Allmänna råd om tillämpningen av av Statens kärnkraftinspektionens föreskrifter enligt ovan. Stockholm: Statens kärnkraftinspektion.

TVO ASSET (1998). ASSET peer review of the Olkiluoto NPP self assessment of safety performance, safety problems and safety culture on the basis of the operational events, Finland 4–10 November 1998 (Report No. IAEA/NSNI/ASSET/98/02). Vienna: International Atomic Energy Agency.

TVO Ordinance. Olkiluodon ydinvoimalaitoksen johtosääntö. Luku 5: Käyttöön kohdistuva tarkastus ja seuranta. Olkiluoto: Teollisuuden Voima Oy.

TVO QA Handbook (1995). Käytönaikainen laadunvarmistuskäsikirja. Luku 10: Seisokkitoiminnot ja muutostyöt. Olkiluoto: Teollisuuden Voima Oy.

Wahlström, B., & Gunsell, L. (1998). Reaktorsäkerhet; En beskrivning och en värdering av säkerhetsarbetet i Norden (Report No. NKS/RAK-1(97)R8). Risø: NKS Sectretariat.

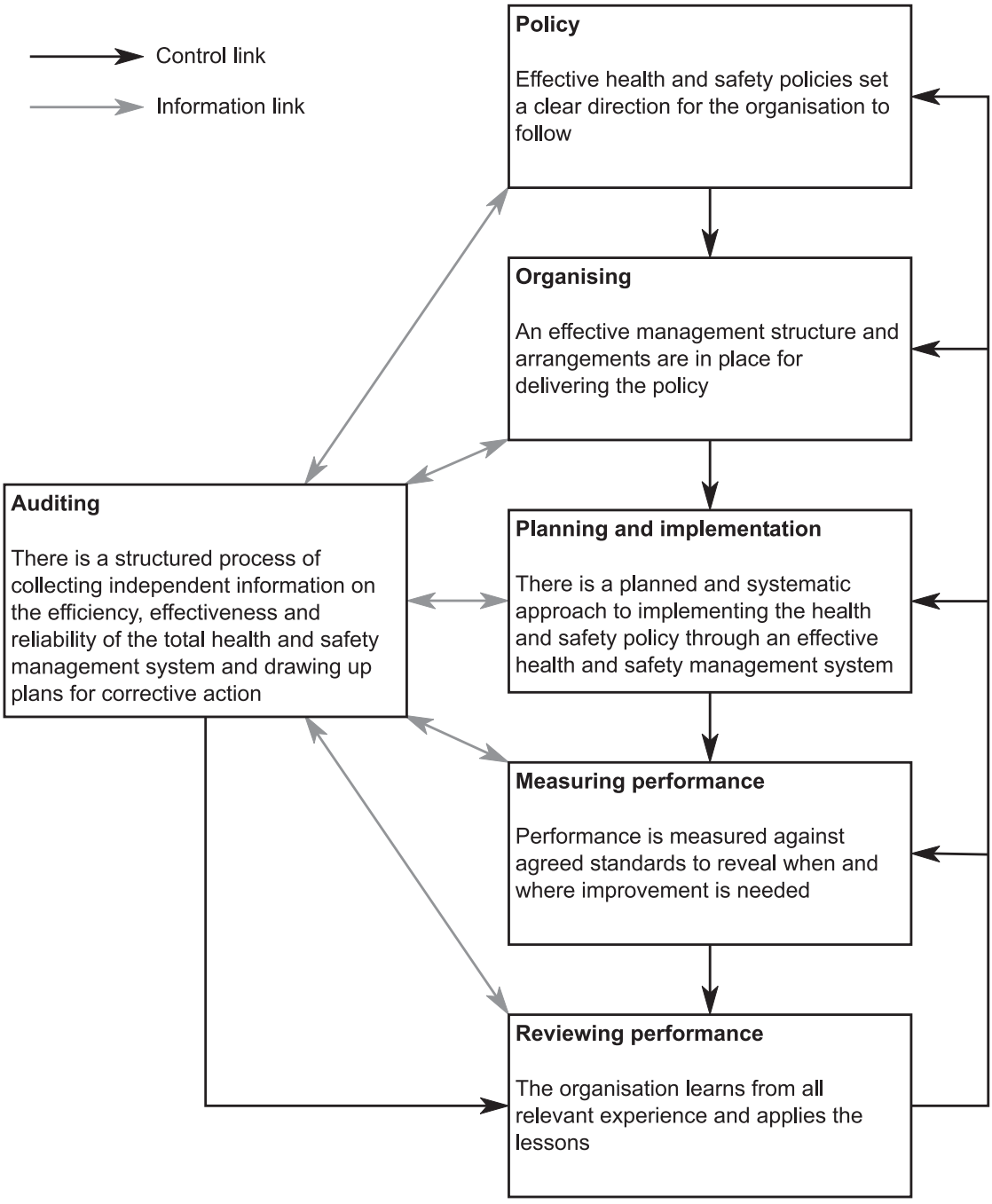
YTO 7.4 (1996). Kotimaisten ydinlaitosten käyttötapahtumien arviointi. Ohje. Helsinki: Säteilyturvakeskus.

YTO 7.5 (1996). Käyttötapahtumien vakavuusluokittelu. Ohje. Helsinki: Säteilyturvakeskus.

YVL 1.5 (1995). Reporting nuclear power plant operation to the Finnish Centre of Radiation and Nuclear Safety. Helsinki: Radiation and Nuclear Safety Authority.

YVL 1.11 (1994). Nuclear power plant operational experience feedback. Helsinki: Radiation and Nuclear Safety Authority.

APPENDIX 1 KEY ELEMENTS OF SUCCESSFUL HEALTH AND SAFETY MANAGEMENT ACCORDING TO THE UK HEALTH AND SAFETY EXECUTIVE



Source: HSG65 (1998)

PARAGRAPH 24.5 OF STUK'S DATA COLLECTION FORM ORGANISATIONAL DEFICIENCIES*

APPENDIX 2

a. The incident was caused by or it related to a violation of the technical specifications which resulted from:

a1. Error or slip in following the regulations
a2. Wrong interpretation
a3. Contradiction between the technical specifications and other instructions
a4. Inadequate regulations
a5. Other reason: <itemise>
a6. Concerned articles in the technical specifications: <itemise>

b. An erroneous assessment of incident's safety significance which related to:

b1. Conflicting safety and availability goals
b2. Underestimation of safety significance
b3. Other: <itemise>

c. The incident was caused by or it related to a measure that was in conflict with the rules and regulations of the quality assurance system or other administrative processes:

c1. Error or carelessness in following the instructions
c2. Compliance with instructions was not supervised
c3. Instructions were not known
c4. Instructions were inadequate
c5. Conflicting instructions
c6. Missing instructions
c7. Other: <itemise>
c8. Concerned instructions: <itemise>

d. The incident related to deficiencies in the practice of maintaining instructions characterised by:

d1. Missing instruction
d2. Instructions were not up to date
d3. Unclear responsibilities in developing instructions
d4. Inadequate distribution of instructions
d5. Deficiencies in issuing and assuring the quality of instructions
d6. Other: <itemise>

e. Deficiencies related to operations:

e1. Insufficient resources in work planning or execution
e2. Work planned or done by an inexperienced subcontractor or a temporary employee
e3. Deficiencies in operational management
e4. Inadequate superintendence
e5. Inadequate or insufficient training
e6. Lack of adequate work experience
e7. Other: <itemise>

f. Deficiencies related to the co-operation between separate organisational units:

f1. Unclear definition of liabilities
f2. Deficiencies in mutual exchange of information
f3. Conflicting objectives
f4. Neglect of common objectives and schedules
f5. Other: <itemise>

g. Deficiencies related to the reporting of the incident:

g1. The performer did not report to his or her foreman adequately
g2. Plant management was not adequately informed
g3. STUK was not adequately informed
g4. Other: <itemise>

* Translation from Finnish into English by the authors.

APPENDIX 3 LOVIISA POWER PLANT OPERATIONAL EVENT REPORT (KT REPORT)

LO1	**x**		**OPERATIONAL EVENT**	**No.**	9/96
LO2				**Writer/date**	JIA 10.4.96
Distribution					
Event date			14.3.96	**Classification inspected by**	dates & signatures
Event			Overheating of a fuse switch		
Operational conditions			Power operation	**Code (KZ)**	12EW04C, TF13D001
Contact persons			EIM		

Event classification				
	x	No further clarifications		Special report
		Report		Report on turbine trip
		Separate clarification		Report on reactor trip
		Disturbance report		Root cause analysis

Description of the event

An internal, S-stage contact of a fuse switch overheated and, as a consequence, an insulation burned a little causing some smoke. Smell of smoke revealed the malfunction in a fuse switch. A fuse switch has been made up of four parallel contacts.

No clear cause for the overheating was found. The contacts had evidently darkened and some normal burning marks could be seen on them. The common spring of the contacts had been clearly slackened but the loosening of the spring can be caused by the overheating, i.e. it is not the reason but the consequence.

The fuse switch was totally renewed (work number 227819).

Corrective actions

Some fuse switches, carrying corresponding load or more, will be inspected during the 1996 annual outage.

PSALO1 HUMAN FAILURE REPORT

A

1. Object (KZ) ☐

2. **LO1** ☒ 3. **LO2** ☐ 4. KT report number ☐

5. Event date ☐ 6. Writer, date ☐

B

Erroneous action _____

_____

_____

C

Situation in which the error was made

1. Periodic testing or return ..... ☐
2. Preventive maintenance ..... ☐
3. Failure search ..... ☐
4. Equipment removal/return ..... ☐
5. Failure repair ..... ☐
6. Response to a transient not initiated by a human failure ..... ☐
   6.1 Erroneous diagnosis ..... ☐
   6.2 Erroneous measure ..... ☐
7. Other: _____ ☐

8. Normal operation ..... ☐
9. Startup ..... ☐
10. Shutdown ..... ☐
11. Outage ..... ☐
12. Remarks: _____ ☐

D

Working group(s) involved

1. Operators ..... ☐
2. Instrumentation maint. .... ☐
3. electrical maint. ..... ☐
4. Mechanical maint. ..... ☐
5. Outside contractor ..... ☐
6. Other: _____ ☐

APPENDIX 4 LOVIISA POWER PLANT HUMAN FAILURE REPORT

E	**Impact of the error**
	1. Reactor trip ☐ 2. Turbine TG1 trip ☐ 3. Turbine TG2 trip ☐ 4. Loss of power, _____ % ☐ 5. Other: _____ ☐
E	**Impact on safety systems**
	6. Red. 1 _____ ☐ 7. Red. 2 _____ ☐ 8. Red. 1 _____ ☐ 9. Red. 2 _____ ☐ 10. Unavailability time _____ 11. Remarks: _____
F	**Means of detection/discovery of the error**
	1. Alarm/trip ☐ 2. Symptoms (immediately) ☐ 3. Shift inspection ☐ 4. Periodic testing ☐ 5. Preventive maintenance ☐ 6. On demand ☐ 7. Quality control ☐ 8. Repair or functional test after the repair ☐ 9. Random casual inspection ☐ 10. Inspection before startup ☐ 11. Other: _____ ☐
G	**Probable causes of the erroneous action**
	1. Written procedure exists ☐ 2. Performed according to the procedure ☐ 3. Erroneous or defectice procedure ☐ 4. Procedure misunderstood ☐ 5. Procedure not followed ☐

	6. Wrong procedure selected		
	7. Performed according to oral instructions		
	8. Oral instructions not followed		
	9. Oral instructions misunderstood		
	10. No written procedure available		
	11. Task too difficult		
	12. Situation misunderstood		
	13. Carelessness, mistake		
	14. Hurry, stress		
	15. Inadequate or insufficient training		
	16. Missing communications channel to the field		
	17. Inadequate control room displays		
	18. Insufficient control means in the control room		
	19. Delayed, although an appropriate measure		
	20. Other: _____		

H **Preventive actions taken**

1. Modification of a procedure		4. Addition of inspections	
2. Modified training		5. None	
3. Plant modification		6. Other: _____	

Description: _____

I **Recommendation** _____

_____

_____

J **Source of information**

1. Operational transient report		4. Root cause report	
2. Reactor or turbine trip report		5. Separate clarification	
3. Special report		6. Other: _____	

APPENDIX 5 AN EXAMPLE OF A DETAILED ROOT CAUSE ANALYSIS FORM

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

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

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

TVO I ☒ II ☐ Equipment place identification number: 656 T003 Work number: 45738, (45739, 45740) Year: 1992 Date (fault detected): 26.08.92 Time: 11.15 Date (repair started): 26.08.92 Time: 13.00 Date (work finished): 26.08.92 Time: 17.36

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

1. 656 K433 L2 T3 low level alarm. T3 will not be filled.

2. The power cabling to the outdoor pump cut at the erection work place of start-up transformers.

3. Failure reports 1245739 and 1245740 done.

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

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

II. IDENTIFICATION OF THE ERROR TYPE

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

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

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

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

AN EXAMPLE OF A DETAILED ROOT CAUSE ANALYSIS FORM **APPENDIX 5**

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

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

1. 656 P031 / failure report 45739 / 26.08.92 and 656 P011 / failure report 45740 /26.08.92.

2. The power supply cables cut to the fuel supply pumps 656 P031 and 656 P011 of the two day fuel tanks of the emergency diesel generators (report).

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

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

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

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

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

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

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

APPENDIX 5 AN EXAMPLE OF A DETAILED ROOT CAUSE ANALYSIS FORM

IV. INFORMATION ON THE WORK TASK WHERE THE ERROR OCCURRED

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

1. Cable charts outside the wall of the plant not kept up to date during the construction period of the plant.

2. Own maintenance worker cut as ordered the "extra"380 V cables at the erection work place of the additional start-up transformers (612).

3. The cut was done in order to facilitate the erection of the additional 110 kV cabling.

The action was (1-2 types): preventive maintenance ☐ repair ☐ modification ☒ periodic test ☐ interval _____weeks functional test ☐ other ☐ date (possible or certain): 19.08.1992

Complementary description:

1. The power cables were encapsulated but not documented and the cables thus thought to be "out of use" cables needed during the earlier plant construction period only.

2. The "unexpectedly"found cables had no voltage due to standstill of the related fuel supply.

The causing action occurred during (1-2 types): cold shutdown of reactor ☐ refuelling ☐ hot shutdown of reactor ☐ nuclear heating ☐ hot standby of reactor ☐ power operation ☒ starting up ☐ shutting down ☐

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

AN EXAMPLE OF A DETAILED ROOT CAUSE ANALYSIS FORM **APPENDIX 5**

V. THE ORIGIN AND DEPENDENCE OF THE FAULT

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

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

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

Explanatory description:

1. Cable charts outside the plant walls were not kept up to date. *2. In addition, unnecessary cables from the plant construction period were known to lie under the earth level.*

Consequences of the error (e.g. unavailability time of equipment or system):

Consequence classification in failure report: A ☐ B ☐ C ☐ D ☐ E ☐ F ☒ G ☐ H ☐ I ☐

Delay time (from originating work task until fault detection): about 168 hours.

Total unavailability time: about 174 hours.

Complementary information (e.g description of consequences):

APPENDIX 5 AN EXAMPLE OF A DETAILED ROOT CAUSE ANALYSIS FORM

VI. NOTES ON POSSIBLE INEFFECTIVENESS OF DEFENSIVE BARRIERS

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

Complementary information (e.g. identification number of TechSpec test or preventive maintenance task or explanation, if checking task existed):

Error was not detected in organizational check (independent QA and QC, performed prior, during or after the work task): Deficient review of design ☒ work planning ☐ start-up testing program ☐ deficient acceptance inspection ☐ other review or inspection ☐, which_____

Complementary information (e.g. which possible other review or check actions could have detected the error):

VII. PROPOSAL OF ALTERNATIVE REMEDIAL MEASURES

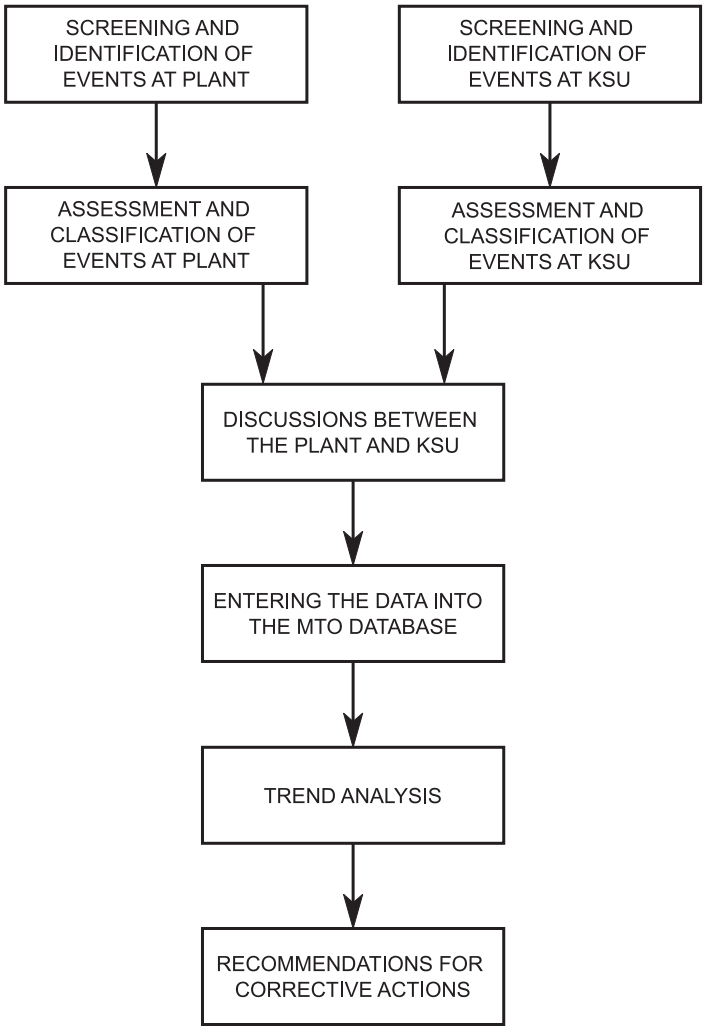
The problem can be corrected (or already corrected and the success possibly evaluated) by:

1. Cable charts concerning areas outside the plant walls were prepared to an up to date status.
2. Procedures were prepared for identification of cables found during digging work and for cutting off power cables. The procedures are in use (e.g. cable radar, cutting needs work order.)
3. An increase of the fuel margins in the day tanks for the diesels was implemented by making the tank level L2 higher.

Source: Laakso (1998).

THE KSU MODEL FOR A PERIODIC OPERATING EXPERIENCE REVIEW OF MTO RELATED EVENTS

APPENDIX 6



Source: Bento (1997)

STUK-YTO-TR-reports

STUK-YTO-TR 159 Huhtanen R (VTT). Fire spread simulation of a full scale cable tunnel.

STUK-YTO-TR 158 Honkamaa T, Kukkola T. Description of Finnish spent fuel encapsulation plant and encapsulation process. Phase I Interim report on Task FIN A 1184 of the Finnish support program to IAEA Safeguards.

STUK-YTO-TR 157 Sirkiä P, Saario T, Mäkelä K, Laitinen T, Bojinov M (VTT). Electric and electrochemical properties of surface films formed on copper in the presence of bicarbonate anions.

STUK-YTO-TR 156 Jussila P. On groundwater flow modelling in safety analyses of spent fuel disposal. A comparative study with emphasis on boundary conditions.

STUK-YTO-TR 155 Nikkinen M, Tiitta A, Iievlev S, Dvoeglazov A, Lopatin S. Specification of a VVER-1000 SFAT device prototype. Interim report on Task FIN A 1073 of the Finnish Support Programme to IAEA Safeguards.

STUK-YTO-TR 154 Pöllänen R, Ilander T, Lehtinen J, Leppänen A, Nikkinen M, Toivonen H, Ylätalo S, Smartt H, Garcia R, Martinez R, Glidewell D, Krantz K. Remote monitoring field trial. Application to automated air sampling. Report on Task FIN-E935 of the Finnish Support Programme to IAEA Safeguards.

STUK-YTO-TR 153 Koukkari P, Laitinen T, Olin M, Sippola H (VTT). Vertailu kaupallisten laskentaohjelmien soveltuvuudesta metallioksidien termodynaamiseen stabiilisuustarkasteluun.

STUK-YTO-TR 152 Bojinov M, Laitinen T, Mäkelä K (VTT). The influence of modified water chemistries on metal oxide films, activity build-up and stress corrosion cracking of structural materials in nuclear power plants.

STUK-YTO-TR 151 Niemi A (ed.) (Kungl Tekniska Högskolan). Studies on coupled hydromechanical effects in single fractures. A contribution to DECOVALEX II Task 3 'Constitutive relationships of rock joints'.

STUK-YTO-TR 150 Betova I, Bojinov M, Laitinen T, MäkeläK, Saario T (VTT). The properties of and transport phenomena in oxide films on iron, nickel, chromium and their alloys in aqueous environments.

STUK-YTO-TR 149 Suolanen V, Ilvonen M (VTT). Generic uncertainty model for DETRA for environmental consequence analyses. Application and sample outputs.

STUK-YTO-TR 148 Elfving K. Ydinvoimalaitosten paineastioiden määräaikaistarkastuksissa käytettävien NDT-järjestelmien pätevöinti.

STUK-YTO-TR 147 Norros L, Kettunen J (VTT). NDT-tarkastajien toimintatavat ammattitaitoa ja tarkastustehtävää koskevien käsitysten perusteella.

STUK-YTO-TR 146 Lempinen A (TKK). Mechanical stability of bentonite buffer system for high level nuclear waste.

The full list of publications is available from Radiation and Nuclear Safety Authority (STUK), phone +358-9-759881, http://www.stuk.fi/.