SKI Report 01:47

Research

Operational Readiness Verification, Phase 1:

A Study on Safety During Outage and Restart of Nuclear Power Plants

Erik Hollnagel
Vincent Gauthereau

June 2001

ISSN 1104-1374
ISRN SKI-R-01/47-SE

SKI PERSPEKTIV

Bakgrund

Under 1990-talets senare hälft rapporterade de svenska kärnkraftsanläggningarna ett antal händelser som innebar att säkerhetssystemen inte gjorts driftklara efter ingrepp. SKI ställde i detta sammanhang krav på tillståndshavarna för kärnkraftsanläggningarna att genomföra översyner och analyser för att förbättra driftklarhetsverifieringen i revisionsavställningens återstartsfas. Tillståndshavarna har genomfört översyner och förbättringsåtgärder inom detta område. SKI genomförde därefter detta forskningsuppdrag för att få underlag för fortsatt tillsyn och för att driva på för ytterligare säkerhetsutveckling inom området.

Inom forskningsuppdraget genomfördes bl.a. intervjuer vid de svenska kärnkraftanläggningarna.

SKI:s syfte

Detta forskningsuppdrag har syftat till att erhålla en lägesbeskrivning av nuvarande situation avseende driftklarhetsverifiering i svenska kärnkraftverk t. ex. en beskrivning av rapporterade problem, hur avvikelserna hanteras, hur driftklarhetsverifieringen leds, organiseras och dokumenteras. Syftet var även att erhålla en litteraturöversikt av internationell forskning av relevans för problemen med driftklarhetsverifiering samt att identifiera forskningsproblem som kan leda till empiriska studier av driftklarhetsverifiering. Detta forskningsuppdrag utgör fas 1 av 3 planerade forsningsinsatser inom området.

Resultat

Projektet resulterade i: en litteraturgenomgång av relevant forskning och slutsatser, ett förslag till beskrivning av viktiga steg inom driftklarhetsverifiering och barriärer baserade på bl.a. tidigare forskning, en beskrivning och analys av den aktuella situationen i Sverige, samt förslag på fortsatt forskning.

Fortsatt verksamhet

Forskningsuppdraget har fortsatt i fas 2 som innehåller empiriska studier vid en svensk kärnkraftsanläggning och en fortsatt utveckling av en metod för att värdera säkerhetsarbetet vid driftklarhetsverifiering.

Effekt på SKI:s verksamhet

Den framtagna kunskapsöversikten har gett SKI ett stöd att användas vid tillsynsinsatser inom området. Dessutom har grunden lagts för fortsatta studier i samverkan med de svenska kärnkraftsanläggningarna och därmed möjligheter till att vara pådrivande i säkerhetsarbetet.

Projektinformation

Projekthandläggare på SKI: Per-Olof Sandén
Projektnummer: 98157

SKI Report 01:47

Research

Operational Readiness Verification, Phase 1:

A Study on Safety During Outage and Restart of Nuclear Power Plants

Erik Hollnagel[1]
Vincent Gauthereau[2]

[1]CSELAB
Department of Computer and Information Science
Linköping University
SE-581 83 Linköping
Sweden

[2]Quality Management
Department of Industrial Engineering
Linköping University
SE-581 83 Linköping

SKI Project Number 98157

Table of Contents

Summary in English.

This report contains the findings from the first phase of a study on safety during outage and restart of nuclear power plants. Operational Readiness Verification (ORV) – in Swedish called *Driftklarhetsverifiering* (DKV) – refers to the test and verification activities that are necessary to ensure that plant systems are able to provide their required functions when needed – more concretely that all plant systems are in their correct functional state when the plant is restarted after an outage period. The concrete background for this work is that nine ORV related incidents were reported in Sweden between July 1995 and October 1998. The work reported here comprised a literature survey of research relevant for ORV issues, and an assessment of the present situation at Swedish NPPs with respect to ORV.

The literature survey was primarily aimed at research related to NPPs, but also looked at domains where similar problems have occurred, such as maintenance in commercial aviation. The survey looked specifically for organisational and MTO aspects relevant to the present situation in Swedish NPPs. One finding was that ORV should be seen as an integral part of maintenance, rather than as a separate activity. Another, that there is a characteristic distribution of error modes for maintenance and ORV, with many sequence errors and omissions, rather than a set of unique error modes. An international study further showed that there are important differences in how procedures are used, and in the balance between decentralisation and centralisation. Several studies also suggested that ORV could usefully be described as a barrier system in relation to the flow of work, for instance using the following five stages: (1) preventive actions during maintenance/outage, (2) post-test after completion of work, (3) pre-test before start-up, (4) the start-up sequence itself, and (5) preventive actions during power operation – possibly including automatic safety systems.

In the field survey interviews were conducted with technical staff at most of the Swedish NPPs. It focused on which solutions the various NPPs had developed to cope with the problem, and which steps had been taken specifically to improve the efficiency of ORV. It was soon found that ORV could not be separated from the rest of the work done in a NPP during outages since many of the proposed solutions have a broad scope.

An analysis of the nine Swedish ORV cases had found weaknesses in four main areas: administration processes, management, human performance, and control room layout. Relative to these, the Swedish NPPs have implemented several technical and organisational solutions. Among the former are an overall re-qualification scheme, blocked safety functions, computerised operational position control, and central indications in the control room. Most of the technical solutions have been part of the design of the newer plants, since to implement them in older plants requires essential changes both in the station and in the control room. The organisational solutions comprised operational readiness plans, systematic ways of working, new instructions, co-ordinated testing, and the use of redundant or independent controls. Special emphasis was put on how the NPPs planned their outages, how the plans were implemented, and how deviations were handled. Issues related to learning from experience were also investigated. It was found that although all the NPPs approached the ORV issues in a serious and efficient manner, the solutions could be different corresponding to the characteristics of the organisation.

Finally a number of questions, which still need answers, were identified. One is how new procedures or new barriers are accepted and assimilated into the safety culture. A second concerns the demarcation of systems for which ORV is required, i.e., the boundary between safety and non-safety systems. A third is how complex technical solutions influence the operators' work. Finally, it is proposed to continue the study by looking more closely at the differences between three levels, or types, of tests: object test, system test and (safety) function test. This should aim to analyse the different steps of testing in order to understand the non-trivial relations between tests and safety. The study should take place at a single NPP during partial/sub-outages (subavställningar), since these periods allow empirical work to be conducted in an appropriate environment with better accessibility to technical staff than during full outage period.

Svensk sammanfattning

Denna rapport innehåller resultaten från den första fasen av en studie rörande nertagning och omstart av kärnkraftsverk. Driftklarhetsverifiering (DKV) är en term som används för att beskriva de test- och verifieringsverksamheter som är nödvändiga för att försäkra att kraftverkets system fungerar när de behövs – mer utvecklat att alla system befinner sig i rätt tillstånd när kraftverket startas om efter att ha varit nertaget. Bakgrunden till detta arbete är nio DKV-relaterade händelser som rapporterats i Sverige mellan Juli 1995 och Oktober 1998. Det arbete som presenteras här baseras på en litteraturgenomgång av relevant forskning rörande DKV-frågor och en sammanställning av den nuvarande situationen av DKV vid svenska kärnkraftverk.

Litteraturgenomgången var primärt inriktad på forskning kopplad till kärnkraftverk, men berörde även domäner där liknande problem förekommer, såsom flygunderhåll. Särskilt beaktades organisatoriska aspekter och MTO-aspekter relevanta för kärnkraftverk vid litteraturgenomgången.

Ett resultat var att DKV bör ses som en intergrerad del av underhållet, snarare än en separat verksamhet. Ett annat är att det finns en karakteristisk distribution av feltillstånd för underhåll och DKV med många sekvenser av fel och förbiseenden, snarare ett antal unika kombinationer av feltillstånd. Vidare visade en internationell studie att det finns viktiga skillnader i hur procedurer används samt i balansen mellan decentralisering och centralisering. Flera studier föreslog också att DKV kan beskrivas som ett barriärsystem i förhållande till arbetsflödet, till exempel om följande fem steg används: (1) förebyggande åtgärder vid underhåll/nertagning, (2) Post-test efter genomfört arbete, (3) pre-test innan uppstart, (4) själva uppstartsekvensen och (5) förebyggande åtgärder under gång – möjligen med automatiska säkerhetessystem.

Intervjuer med teknisk personal på i stort sett alla svenska kärnkraftverk genomfördes under fältarbetet. Dessa fokuserade på de lösningar som utvecklats på de olika kraftverken för att hantera DKV-problemet och speciellt på vilka åtgärder som genomförts för att förbättra effektiviteten av DKV. Det upptäcktes snart DKV inte kan separeras från övrig verksamhet som genomförs under en nertagning eftersom många av de föreslagna lösningarna hade ett vitt omfång.

En analys av nio svenska DKV-fall påvisar svagheter på fyra övergripande områden: Administrativa processer, ledning, mänskligt beteende och kontrollrumsdesign. I anslutning till detta har de svenska kärnkraftverken infört flera tekniska och organisatoriska lösningar. Bland de förstnämnda finns re-kvalificerings scheman, spärrade säkerhetsfunktioner, datoriserad driftlägeskontroll och centrala indikeringar i kontrollrummet. De flesta tekniska lösningar har varit en del av de nya anläggningarna, eftersom en implementering i de äldre anläggningarna skulle kräva stora förändringar både i kraftverket och själva kontrollrummet. Organisatoriska lösningar bestod i driftklarhetsplaner, systematiska arbetsätt, nya instruktioner, koordinerad testning och användandet av redundanta eller oberoende kontroller. Särskild tyngdpunkt lades vid hur kärnkraftverken planerade sina revisionsavställningar, hur dessa planer implementerades och hur avvikelser från dessa hanterades. Frågor rörande hur erfarenheter tagits till vara undersöktes också. Det upptäcktes att samtliga kärnkraftverk närmades sig DKV-frågor på ett seriöst och effektivt sätt, men lösningarna kunder variera beroende på organisationernas karaktär.

Slutligen identifierades ett antal frågor som fortfarande måste besvaras. En är hur nya procedurer och barriärer accepteras och assimileras i säkerhetstänkandet. En andra rör avgränsning av system för vilka DKV krävs, t.ex., gränsen mellan säkra och icke-säkra system. Ett tredje är hur komplexa tekniska lösningar påverkar operatörernas arbete. Det föreslås slutligen att studien bör fortsättas genom att undersöka de tre nivåerna, eller typerna av test, närmare: komponenttest, systemtest och (säkerhets) funktionstest. Inriktningen bör vara att analysera de olika stegen av testning för att förstå de icke-triviala sambanden mellan testning och säkerhet. Studien bör genomföras vid endast ett kärnkraftverk under subavställningar, eftersom dessa perioder tillåter att empiriskt arbete bedrivs på ett korrekt sätt och med större tillgång till teknisk personal än under en komplett nedtagning.

OPERATIONAL READINESS VERIFICATION, PHASE 1: A Study On Safety During Outage And Restart Of Nuclear Power Plants

1. Introduction

This report presents the findings from the first phase of a study on Operational Readiness Verification – Phase 1 – A study on safety during outage and restart of nuclear power plants (Best nr. 98157). The first phase of the study comprised two parts: (1) a literature survey of research relevant for ORV/DKV issues, and (2) an assessment of the present situation with respect to ORV/DKV.

The literature survey was primarily directed at research related to NPPs, but did also consider other sectors where similar problems have been known to occur, specifically maintenance and ORV within commercial aviation. The survey looked specifically at organisational and MTO aspects in the present situation at the Swedish NPPs. This survey resulted in an overview as a basis for developing more specific research issues that will put MTO aspects in focus.

The work in this phase of the study made use of established knowledge and methods from the study of barrier systems and functions, from work with high-reliability organisations and total quality management, as well as cognitive ergonomics and cognitive systems engineering.

This report, which comprises the results from the literature study and the survey, aims to provide a comprehensive overview of current practical issues and problems in handling ORV/DKV, and the research issues that can be derived from that. While the authors believe that this overview is of value by itself, it can serve as a basis for specifying concrete problems that can be made the subject of further empirical and analytical studies. These problems are presented as the last section of this report.

The work reported here has been carried out from October 2000 to July 2001. The work would not have been possible without the unreserved co-operation of numerous staff members at the Swedish NPPs who so willingly gave their time and effort to participate in the study. The authors would also like to thank Gerd Svensson, Staffan Forsberg, Ola Svenson, and Martin Fridleifer, for valuable and inspiring discussions throughout the project.

2. Literature Survey

The first part of this report presents the result of the literature survey. As noted above, this primarily covered text sources available within the nuclear domain, but in addition looked at the technological domains in general, specifically process control and aviation.

2.1 Definition And Discussion Of Terms

Operational Readiness Verification (ORV) – in Swedish called *Driftklarhetsverifiering* (DKV) – refers to the test and verification activities that are necessary to ensure that a plant system is able to provide its required function at the required time, more concretely that all plant systems are in their correct functional state when the plant is restarted after an outage period. In basic language, it refers to the activities that are needed to ensure that systems are able to work as they should and as they have been designed to do.

ORV is an important issue because NPPs (Nuclear Power Plants) regularly have periods of outage and maintenance, during which many systems are disconnected and disassembled. Throughout these periods the NPP is effectively off-line and the reactor is shut down. Before the NPP can be restarted and brought on-line, it is necessary to ensure that all systems are ready. This means verifying that repairs and modifications have been completed and have achieved the intended effects, that the systems have been assembled correctly, that they can be operated or activated according to their functional specifications (design criteria), and that the power plant as a whole – as a complex assembly of subsystems – is able to function. The latter is particularly important since a NPP is a system characterised by complex interactions and tight couplings, to use the terms of Perrow (1984).

The situation is nevertheless not unique for NPPs, since all technologically complex systems – and in principle all technological systems – require that some kind of maintenance is carried out on a regular or semi-regular basis. (As an aside, the same may also be said for social systems and organisations.) One important issue is whether the system is in continuous use and has to be taken out of production mode as a whole in order for the maintenance to take place. For some systems maintenance can be done while the overall system is still running, for instance by having redundant subsystems (as in the electrical grid and most communication systems). For other systems, predominantly in the transportation domain (airplanes, trains, ships, and – perhaps – land vehicles), periods of maintenance and operation are interspersed in a regular fashion, often because the systems by their very nature are incapable of functioning reliably for very long periods of time. In all cases, however, regular or scheduled maintenance is essential, because unscheduled maintenance usually is associated with costly interruptions of normal functioning and/or accidents with potentially significant negative consequences.

In all cases where maintenance is done, there are usually strong economic demand both to have as few maintenance periods as possible and to keep each maintenance period as short as possible, hence to bring the system back into operation as soon as possible. Yet since maintenance by its very nature is a disruption of normal functioning, it is also necessary to ensure that the system is able to function as required when the maintenance has been completed. This is accomplished by means of special tests that generally are referred to as operational readiness verification.

2.2 ORV As Post-And Pre-Condition Testing

ORV can in principle take place in two different ways, as a post-condition test or as a pre-condition test.

ORV as post-condition takes place at the completion of a work activity, such as modification or repair. It is considered to be a post-condition test, because the purpose of the maintenance work is to ensure that the subsystem functions in a specific manner, i.e., it that the goals of the maintenance activities have been achieved. Since maintenance always requires some kind of disassembly of the subsystem, it is prudent to conclude the reassembly by ensuring that the subsystem functions as required. (In principle, the maintenance also involves disconnection and reconnection between subsystem and system, but this is considered in the following.) This type of post-condition ORV is done for each subsystem, hence in a piecemeal fashion. The principle is illustrated in Figure 1.

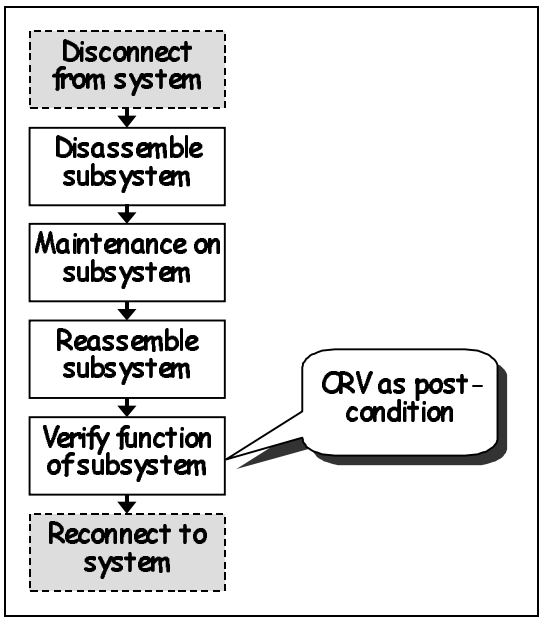

Figure 1: ORV as a post-condition.

ORV as pre-condition takes place before the beginning of an activity. For outages and maintenance ORV as pre-condition is the test of readiness that is carried out after disconnected subsystems have been reconnected, either in groups or as a whole, but **before** the plant is restarted. It is considered a pre-condition test because its purpose is to ensure that everything is ready before something is begun, typically before the restart of the plant is initiated. ORV as a pre-condition is not a substitute for ORV as a post-condition, but rather implies that ORV as a post-condition has been successfully performed. ORV as a pre-condition is necessary because some (considerable) time may have gone after the post-condition test during which the readiness status of subsystems may have changed. Furthermore, ensuring that each sub-system functions by itself does not logically ensure that the combination or aggregation of subsystems will also work. The principle is illustrated in Figure 2.

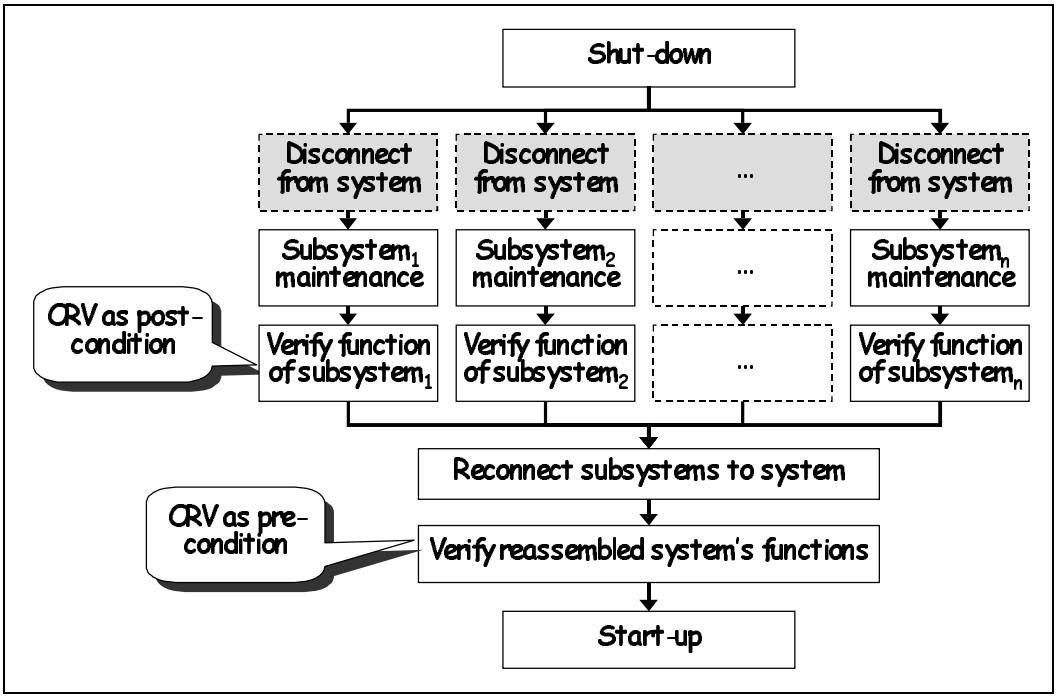

Figure 2: ORV as pre-condition.

The distinction between the two types of ORV is potentially important because they may require different approaches. Certainly, ORV as a post-condition can take place locally and be integrated into the maintenance and repair procedures. In contrast, ORV as a pre-condition will usually require considerable co-ordination and planning with regard both to time and space. The two kinds of ORV may therefore require different resources and involve different types of risks.

2.3 Main Sources For The Literature Survey

The primary sources for the literature survey have been journals and databases that were available on-line – which at the present time covers all the major journals and periodicals in the field, as well as all major conferences. This includes journals such as "Nuclear Engineering & Design", "Reliability Engineering & Systems Safety", "Journal of Hazardous Materials", "International Journal of industrial ergonomics", and "Safety Science".

In addition, the following reports produced by the different NPPs have been made available, based on a decision taken by SKI in July 2000 (ref: 8.09-000879), and have constituted a valuable source of information.

- Oskarshamn 1, 2, och 3 - Sammanställningsrapport - DKV-gruppens svar på SKIs skrivelse 8.09-000879

- Redovisning av åtgärder inom området verifiering av driftklarhet - Ref: FQ-2000-485 (Forsmarks kraftgrupp)

- Redovisning av åtgärder inom området verifiering av driftklarhet - Ref: 1702517 (Ringhals)

- Barsebäck - Ytterligare redovisning av åtgärder inom området verifiering av driftklarhet - Ref: P-200012-26

Despite the very large number of sources that could be searched in the open literature, the outcome has been relative modest. This can either be because the search criteria have been too narrow, or because there is a scarcity of literature and reports relating to this particular problem. The former option can be ruled out by the fact that the search did find a number of highly relevant references, cf. below. That the number of references was few is therefore interpreted as an indication of the scarcity of material.

A considerable number of replies to search criteria such as "operational readiness" were found in the military field. A perusal of the sources revealed, however, that the term referred to preparations for operational readiness in the sense of stand-by capacity, for instance for military units on high alert. This is quite different from the issue addressed by the ORV project, and these sources were therefore not considered further.

Additional replies turned up in relation to issues such as risk analysis, safety culture, and accident reporting. However, neither of these had any direct relevance for the ORV issues.

3. Specific findings

Since the number of clearly relevant items found by the literature survey was quite limited, we have decided to give a short account of each of them, and point to the findings and suggestions that are of particular relevance for the ORV study. The items are presented in no particular order.

3.1 General Analysis Of Human Performance Problems

Bento (1988) performed an analysis of human performance problems in Swedish NPPs, based on 165 scrams and 1318 LER (Licensee Event Report) cases collected over a period of five years. The data were analysed with respect to the system or component affected by the events, the personnel category involved, the location of the occurrence, the type of work, the type of inappropriate action, and the causal category ("root cause"). In relation to the present study the most interesting finding was the difference in the distribution of contributing causes over the two conditions of scram and LERs, specifically the following:

- In terms of the category of people involved in the occurrences, scrams were dominated by operation personnel and the I&C department (55% and 18% respectively), while LERs were more evenly distributed over larger categories of people. In fact, the mechanical department provided the largest contribution (25%), with operation personnel, I&C department, and electrical department all being less than 20%.

- In terms of work type, scrams were dominated by operation, test and calibration (51% and 35% respectively), while LERs were dominated by maintenance and

repair (45%). Operations, in fact, came in fourth place with a contribution of about 11%.

- In terms of inappropriate action type, scrams were dominated by untimely actions (about 26%), followed by confusion, other action (inappropriate action), omission, and extraneous action – all having a contribution between 17-21%. For LERs, the order of importance was more or less reversed, with extraneous actions having a contribution of more than 30%.

- Finally, in terms of root causes, scrams were dominated by human variability and work place ergonomics, which together accounted for about 50% of the causes. For LERs the dominating cause was work organisation followed by work place ergonomics and not following procedures, cf. Figure 3. Together these three categories of causes account for about 45% of the cases.

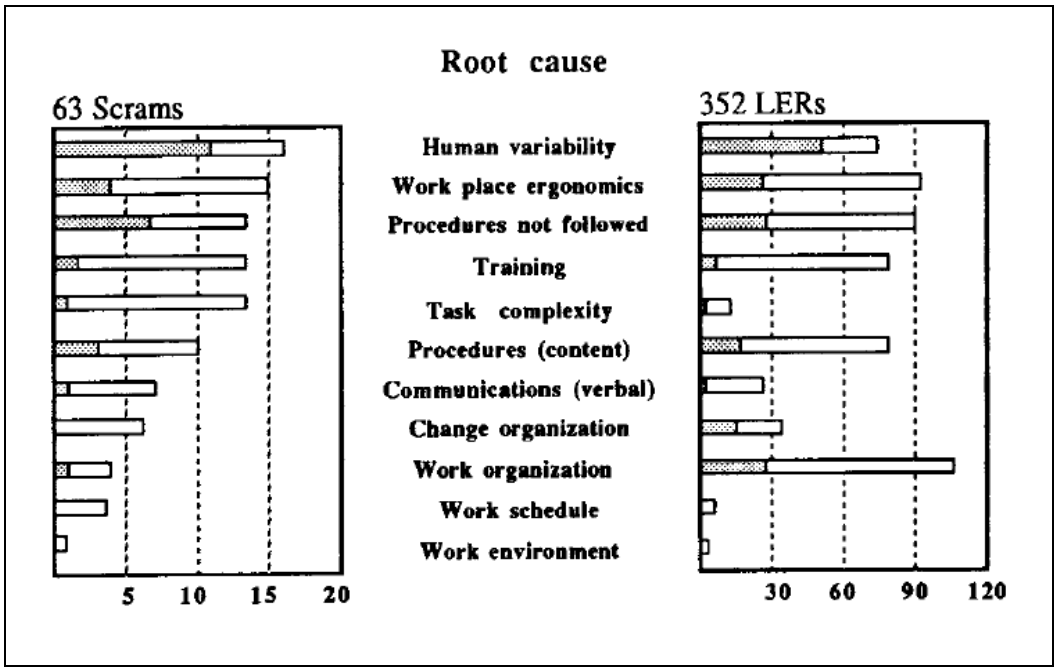

Figure 3: Root causes from Swedish LERs (after Bento, 1988).

Even though the analyses were not specifically directed at outages and ORV, the differences in the distribution of contributing causes between scrams and LERs is striking. In general, scrams are mainly due to actions in the control room, and in particular to untimely acts. LERs, on the other hand, can occur for many different reasons and involve many functions and categories of staff. Given the nature of outages, it is reasonable to expect that the differences will be even more marked then, and that for instance work organisation will be particularly important. In that respect it is interesting to note that the recommendations made at the end of the report were:

- To reinforce more stringent work organization end administrative routines;

- To encourage the operating staff to show a more rigorous respect of procedures;

- To improve work place ergonomics; and

- To maintain high morale, motivation and enthusiasm among the staff.

The same recommendations seem relevant for outage and ORV work, due, perhaps, to their general nature.

3.2 Identification Of Human Originated Test And Maintenance Errors

This reports a method developed under the Nordic RAS-50 project (Pyy & Saarenpää, 1988). Despite the title, the method does not deal specifically with human or organisational causes of maintenance errors. Instead, the method purports to identify human related common cause (CC) failures by structured interviews with plant experts, based on a list of maintenance tasks (specifically tests). The aim of the method was to assign possible failures into three CC classes (risk classes), using the simple formula:

$$R = (f / i) * c$$

Where:

R = Risk,

f = task frequency

i = inspection frequency

c = consequences.

Although the method represents an interest in human-related maintenance errors, it is of limited interest from a psychological or organisational perspective, and therefore only of limited value for the study of ORV.

3.3 Studies on Human Errors Related To NPP Maintenance Activities

This paper reports on an explicit study of human errors related to NPP maintenance (Pyy et al., 1997; Pyy, *in press*). The study was motivated by the finding that NPP equipment sometimes could be declared operable, even though it would not be capable of fulfilling all its functions. This can be seen as a kind of latent unavailability that may have many different causes, including forgetting to restore a function combined with incomplete testing. The objective of the study was to identify and give examples of common cause failure mechanisms and generate numerical safety indicators that could be used to predict the effectiveness of maintenance performance.

The raw data were 4407 records of maintenance and repair from the Olkiluoto BWR in Finland for the period 1992-94. After an initial screening, about 500 cases remained. These were further analysed with the assistance of utility personnel, to reveal cases where human induced common cause failures (HCCF), human induced non-critical faults (HCCN) and human shared equipment failures (HSEF), i.e., cases where single human actions had consequences because of latent conditions in the technical systems.

Altogether this reduced the data material to 334 cases, which yielded statistics of 206 single errors, and 126 cases that were subjected to a more detailed root cause analysis.

For the ORV project, the interesting finding from the Pyy et al. study concerns the time when the errors were detected. Here it was found that while 94 % of the designated human failures that originated from power operation were also detected during power operation, about 49 % of the designated human failures that originated from outage remained latent until the plant start-up or even until the power operation. Of those that remained, 17% were detected by preventive actions (presumably some kind of operational readiness verification), 10% were detected during start-up, 7% were detected by preventive actions during power operation, and a full 32% during power operation. (The paper unfortunately does not clearly define the nature of all the operational regimes.) The failures were also analysed with respect to the equipment category involved, and it was found that although the detection of failures in mechanical components was larger during outages, there was no statistically significant differences among the various groups (Pyy, *in press*).

Figure 4 shows the result from a more detailed analysis of the detection mode for 12 dependent human errors that had their origin during the outage period. The bars show the number of errors that were detected at each of the states defined above, and the graph shows the cumulated percentage of detections.

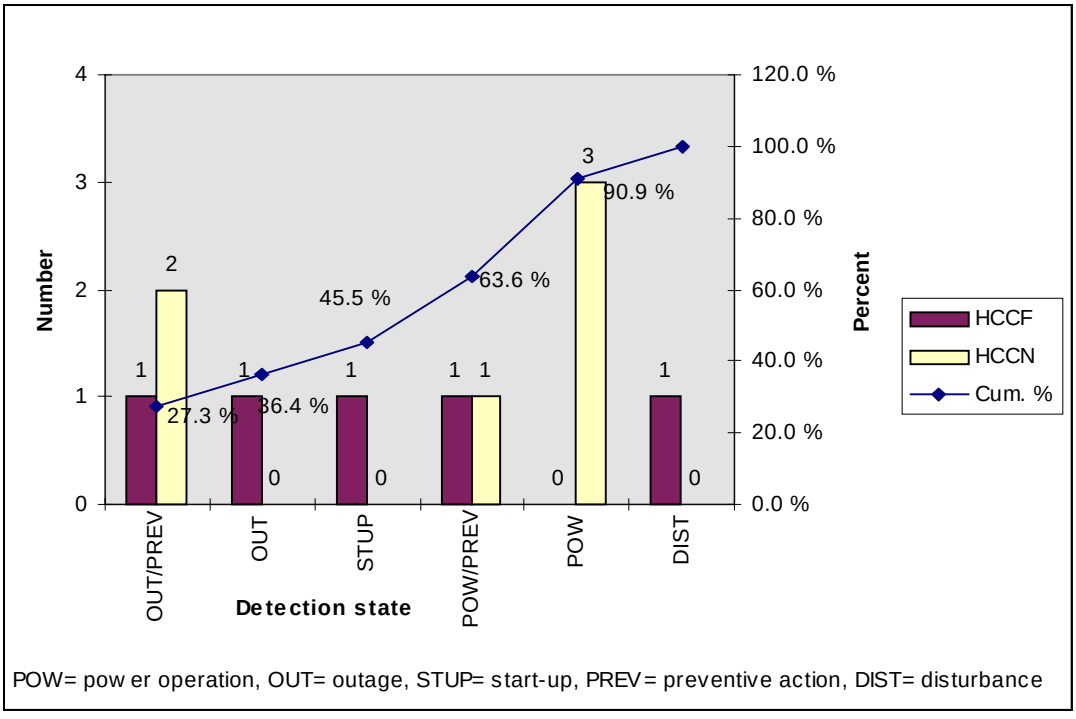

Figure 4: Distribution of detection modes of for 11 cases of human induced dependent faults introduced during an outage (after Pyy, in press).

These results are quite discouraging, since they mean that only a small part of the failures (around 27%) were detected by means of preventive actions during outage, such as readiness verification. About one third of the failures were only detected during actual power operation! A further analysis of the data revealed that while periodic

testing and alarms altogether detected about 50% of the cases, the preventive actions themselves were the designated cause of five of the cases. If these numbers are correct, it actually means that the preventive actions introduce almost as many failures as they detect!

3.4 Maintenance Errors

Two surveys in the context of NPP found that errors in maintenance activities mainly were errors of omission (Reason, 1990; 1997). Another more recent survey realised in the UK nuclear industry (Reiersen & Gibson, 1995) disagreed with these findings. It actually emphasised that "step incorrect" and "domino – step incorrect" explained 31.7% of direct causes ("domino –step incorrect" describes the condition when a task is carried out on a correct object but that during this task the operator interferes with another unrelated equipment).

Reiersen & Gibson (1995), who reviewed a number of studies of factors influencing maintenance errors in the nuclear power industry, summarised the findings in the four following points:

- Maintenance activities take place throughout the plant. Problem of access, constraining work environment are commonly faced problems. The working environment considerably impairs communication in the work place.

- Organisational settings should be considered, especially during maintenance outage.

- Time pressure to reduce duration of outages has a direct influence on personnel.

- Maintenance training is central.

From the study of 172 reports, Reiersen & Gibson (1995) identified several underlying causes for maintenance errors. Procedural deficiencies represented 30.3% of these causes, while 71% were generated by incorrect or insufficient procedure content. The failure to use procedures was found to represent only 14.5% of procedural deficiencies, thus contrasting with other studies. However, as exemplified in Bourrier (1999), cf. below, the influence of cultural settings is crucial and any attempt to generalise should be taken very carefully.

3.5 A Case Study Of Outage Management

This work referred to a case study performed at a two-unit commercial PWR, when one unit was in a refuelling outage and the other unit was at full power operation (Haber et al., 1992). The background for the study was an increased concern at the NRC regarding the safety of NPPs during shutdown, specifically loss of shutdown cooling at Diablo Canyon (U.S. NRC, 1987), loss of all vital AC power at the Alvin W. Vogtle plant (U.S. NRC, 1990) and loss of shutdown cooling at Prairie Island (U. S. NRC, 1992). Based on their evaluations the NRC concluded that outage management should be seen as the most important issue related to shutdown risk. This is a little different from ORV issues, since the focus is on safety during the outage rather than the readiness of the plant when it is started again. It is nevertheless reasonable to assume that problems during outage in

many cases also are the source of problems during restart, and the report has therefore been included in the survey.

Data were collected over a period of approximately four months in a field study conducted by teams from Brookhaven National Laboratory (BNL) and the University of California at Berkeley (UCB). The primary purpose of the study was to collect data for part of the NRC's organisational factors research program. The data collection made use of interviews and observations of plant personnel and organizational activities, as well as a paper and pencil survey regarding organisational culture and work environment issues and administered across the plant.

One conclusions was that:

> "the management of a scheduled refuelling outage … serves as a primary means of enhancing safety during shutdown. Managing risks and maintaining safety functions during a multitude of outage activities requires a clear understanding of the plants' safety philosophy, appropriate involvement of organizational levels, planning and coordinating, communication, and the awareness of plant status by the personnel involved in those activities"
> (Haber et al., 1992, p. 134)

The effective management was described in terms of five organizational factors, namely:

1) communication – including interdepartmental communication, intradepartmental communication, and external communication,

2) management attention, involvement and oversight,

3) standardization of work and skills,

4) human resources, and

5) organization culture.

Each factor of these factors was discussed in terms of the dimensions relevant to what was observed during the field research. The conclusions were, however, short on specifics, and merely pointed out that these factors are pervasive during an outage (and presumably also during other operational regimes). The study did not report specific failures or near misses that might have been observed during the data collection, and it is therefore not possible from this study to suggest more concrete relationships that should be kept in mind.

3.6 Plant Functional Modelling

Rasmussen & Petersen (1999) reported on the development of a method to assess the impact of management on plant safety. The method was developed as part of a CEC STEP project named TOMHID (An Overall Knowledge-based Methodology for Hazard Identification). The proposed area of application was chemical process plants, but since

the method was generic it can presumably be also applied to nuclear power plants and to operation as well as maintenance.

The purpose of the method was to provide means for representing a process plant as a socio-technical system and to allow hazard identification on a high level in order to identify major targets for safety development. This was achieved through a methodology with the following steps:

1. Preparation of a plant functional model where a set of plant functions coherently describes hardware, software, operations, work organization and other safety related aspects. The basic principle is that any aspect of the plant can be represented by an object based upon an *Intent* (Sic!), associated *Methods* by which the *Intent* is realized, and *Constraints, which* may limit the Intent.

2. Plant level hazard identification based on keywords/checklists and the functional model.

3. Development of incident scenarios and selection of hazardous situation with different safety characteristics.

4. Evaluation of the impact of management on plant safety through interviews.

5. Identification of safety critical ways of action in the management system, i.e. identification of possible error- and violation-producing conditions.

In relation to the present project, the most interesting part of the proposed method is the plant functional model, as shown in Figure 5. For the issue of ORV, the important part of the model is the set of constraint, which may lead to an unintended output. The modelling processes is described as follows:

> "The modelling principle is a top-down approach, which ensures a logical functional model of the process plant. The usual starting point will be a process flow sheet and from this the analyst will have information on all the chemical substances (new materials, products, waste products, residues, solvents etc.) and the characteristics of the main process streams. From this starting point, the functional decomposition is performed, ensuring that all relevant activities are considered (processing, maintenance, controls, emergency systems etc.). For a particular plant, there will be one plant object, one or more unit objects, and a number of objects of the lower levels corresponding to systems and subsystems in the plant."
> (Rasmussen & Petersen, 1999, p. 202).

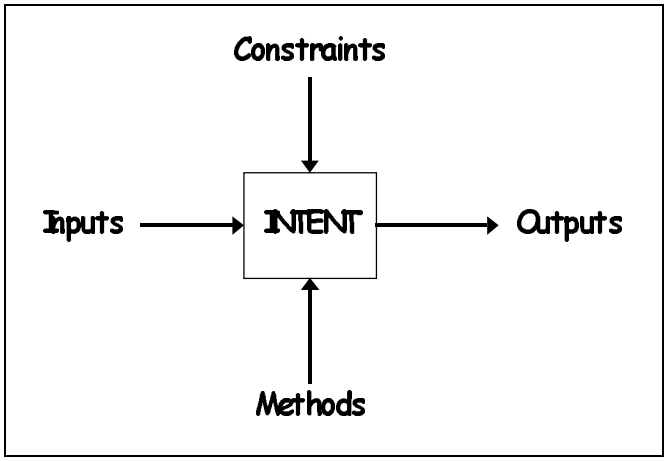

Figure 5: Diagrammatical functional model (TOMHID project).

In the model, Intents represent the functional goals of the specific plant activities in question, and methods represent items (hardware, procedures, software, etc.) that are used to carry out the Intent or operations that are carried out using those items. Likewise, inputs are the necessary conditions to perform the Intent and the link to the previous Intent, and outputs show the outcome produced by the Intent and the link to the subsequent Intent. Finally, constraints describe items (physical laws, work organization, control and protective systems etc.) that exist to supervise or restrict the Intent.

In the functional model, the Intent may represent a maintenance activity, and the constraints may represent the conditions that affect the implementation of the maintenance activity, specifically whether it is successfully accomplished. Since the output of one Intent "unit" may become the input of another, the model includes the basic elements for describing the interaction and dependency between specific actions, hence the propagation of side effects from constraints at previous steps. In the TOMHID project, neither the model nor the methodology was developed to look specifically at maintenance issues. The proposed use of functional modelling is, however, an interesting pointer for further ORV work.

3.7 Sociological Analysis Of Outages In France And The USA

Bourrier (1999) studied maintenance work in four NPPs, two in France and two in the USA. Her work, which looked at other issues in addition to ORV, provides a good introduction to the context in which ORV should be considered and pointed to relevant criteria for the literature survey. Her organisational analyses of four sites lead to the definition of four different states of organisational reliability. However as the fourth example described an organisation in a transient state, it has not been included here.

3.7.1 Deviations at Bugey

The management of outage at Bugey was based on adaptation and improvisation activities. Deviation from procedures occurred through interpretation, adaptation to the context, and also through violation, which usually found its bases in convenience and routine. Improvisation, however, also lead to deviations. On the procedural level,

improvisation served to fill up “holes” and deficiencies in procedures. On an organisational level, improvisation occurred in order to replace or create missing roles.

The situation at Bugey was due to the organisational practices and climate. The technicians never took part in the creation of procedures, which were imposed from the outside. Operators did not participate in the updating of procedures either. Because of the limited possibility for operators to have a say in the improvement of procedures, they progressively stopped reporting deviations between procedures and the reality they were applied to. Bourrier also identified political factors that led to this deviation strategy.

The deviations from the written prescriptions were, however, not totally uncontrolled. As the development of deviations took place in the context of a group, deviations became known and accepted within a group. These new “accepted deviations” constituted new tacit rules that should not be transgressed. These factors increased the importance of the socialisation process of new technicians who needed to learn these tacit rules and also needed to be aware of their informal / illegal values. The autonomy of operators thus presents a paradox as it included both positive and negative attributes. In that context, the increasing use of external contractors during outage threatened the established system. Since contractors did not belong to the community of station technicians, contractors tended to act differently.

3.7.2 Compliance At Diablo-Canyon NPP

At the Diablo-Canyon NPP work was entirely formalised and there were procedures for everything. The operators strictly complied with procedures, and if some information was lacking they reported it to their managers and did not act until further information was provided. In this environment there was absolutely no place for improvisation to take place. However, such a system is not theoretically viable. Due to the inevitable individual and organisational variability, a formal system that lacks a modicum of flexibility is doomed to fail. Yet despite that some factors seemed to render the system viable.

One factor was that the time devoted to planning was significant so that unexpected events were less likely to occur. This meant that there would be few cases where a procedure did not exist. A second factor was that the resources delegated to assist technicians were significant. This assistance provided the possibility for unplanned events to be reviewed quickly and consequently for solutions to be proposed. It seems then that Diablo-Canyon embraced two traditionally opposed strategies: the allocation of important resources for planning without neglecting the importance of the unexpected.

3.7.3 Exceptions At North-Anna NPP

Actors at North-Anna were found both to comply with and to transgress procedures. Specifically, they both complied with procedures and secretly changed the planning of the tasks. Bourrier actually observed an application of the general rule, which states that the degree of implication in the creation of the rule, and the recognised capacity to change it, are determining factors in the level of compliance. In fact, as maintenance operators had explicit means of modifying the procedures, they complied with them. By

the same token, as they lacked control over the establishment of the planning, they usually did not comply with it but instead tried to take into account other constraints.

Compliance to procedures at North-Anna differed from Diablo-Canyon where compliance was used as a self-protecting strategy. In fact, at North-Anna, operators participated in the elaboration of the procedures, which were therefore not seen as forced, but as chosen. The autonomy of the operator at North-Anna must nevertheless be distinguished from the autonomy of the operators as Bugey. In both case the autonomy was real, but in contrast to the case at Bugey, the autonomy at North-Anna was recognised, hence legal.

3.8 Inter-Project Learning

Since each outage can be considered as a unique project, the concept of inter-project learning can be of value. Although every project in some way is unique, it is often possible to distinguish different degrees of uniqueness since some aspects or elements will be common to many projects. This is certainly the case for NPP outages where there are a considerable number of routine elements, but where each outage period also has its particularities, is uniqueness.

Inter-project learning is understood as an "approach to reduce future uncertainty by exploiting experience gained in previous or concurrent projects" (Antoni, 2000). Inter-project learning takes place in two different ways, called codification, and personalisation (see Figure 6). These two concepts describe whether knowledge is transferred in a codified manner (hence de-personalised) or whether it is the members of the organisations who are the carriers of experience (Antoni, 2000; Hansen, 1999).

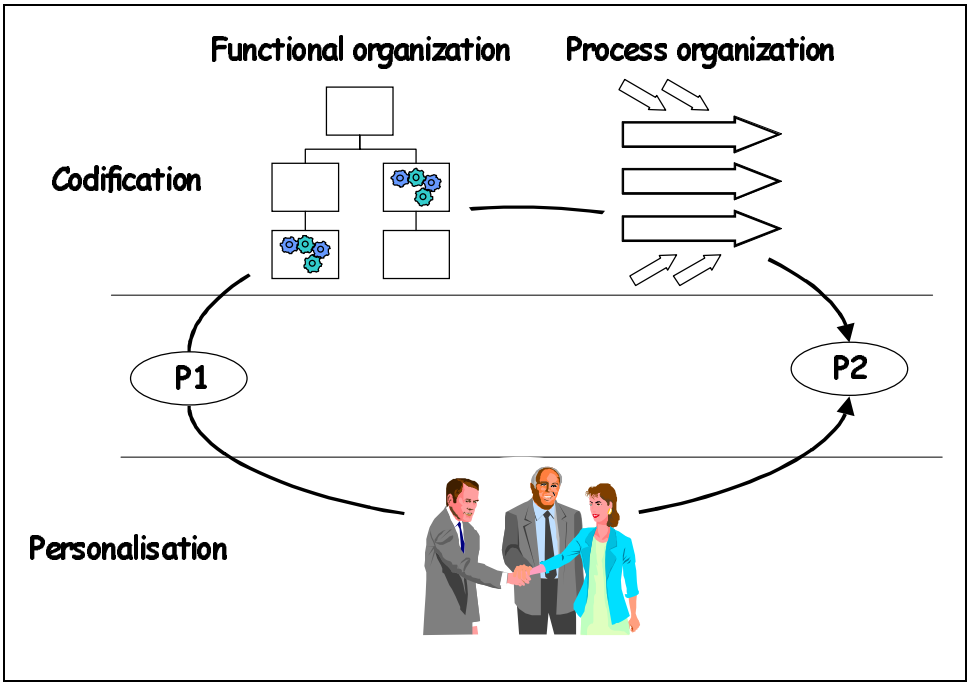

Figure 6: Inter-Project Learning Model (source: Antoni, 2000).

It is obviously not desirable if inter-project learning is based only on personalisation, since this leaves little record of what is learned, and since it is difficult to monitor and control. Conversely, inter-project learning based exclusively on codification may be rigid and stale, since formal rules and classifications by their nature are better at capturing what is general than what is unique. A formal procedure usually also requires some time to be developed and updated, and may therefore represent the problems and experiences of yesterday rather than of today. While a proper balance between codification and personalisation clearly is attractive, this is easier said than done since achieving the balance cannot itself be codified. It is nevertheless important to understand the properties of inter-project learning and to consider it as a part of the longer-term organisation and management of outages.

3.9 Aviation Experiences

One field that is especially prone to the effects of failures during maintenance is aviation. The reason for this is simple: aircraft are extensively maintained and checked, from the routine check after each landing and before each take-off, to more extensive periods of maintenance and overhaul according to strict schedules agreed upon between aircraft manufacturers and airlines. The event reporting system in aviation is extensive, and currently available data indicate that 12% of major aviation accidents can be attributed to maintenance and inspection (sic!) deficiencies. Furthermore about 23% of the mechanical discrepancies in flight are caused by errors in a previous maintenance task. Indeed, the aviation industry has a common definition of maintenance error, as follows:

> "Any action by a person or people that results in an unintended aircraft discrepancy. May include, but is not limited to, non-compliance with a maintenance program, a civil aviation authority regulation, or a company procedure."

The difference between aviation and NPP is the occurrence of many relatively brief and highly regulated maintenance periods, instead of a few long outage periods. This means that the activities during aircraft maintenance can be better planned than work during NPP outages, that people can be specifically trained, and that the planning and organisation of work falls within the sphere of normal rather than exceptional operations. Another difference is that aviation only has a limited involvement of external contractors, at least in the sense of people who are not familiar with the "plant" and the work environment.

Due to these differences it is to be expected that the way in which maintenance errors occur in aviation (the "failure mechanism" so to speak) is different from how they occur in nuclear power. Indeed, a common finding is that the cause of maintenance errors often is a deviation from the normal conditions, for instance because some person or component is missing, because there is an unusual need or high time pressure, or because the work is disturbed by an external event in some way. A classical example of that is the case of the missing O-Rings on an Eastern L-1011 flight, as described in Appendix A. (Note, by the way, the rather terse account given by the investigation official report.) In this case a component was installed incorrectly because the routinely used supply was empty. Since there had been a habitual deviation from procedures, the maintenance workers failed to check that the component they used was complete and in good working order. Adding to that, the procedure for the post-condition testing was

ambiguous and underspecified, which meant that the test was carried out in a perfunctory manner, thereby opening the way for the incident to happen.

According to the Flight Safety Occurrence Digest from 1992, the four most important maintenance errors were:

- Incorrect installation of components;
- Fitting of wrong parts;
- Electrical wiring discrepancies; and
- Loose objects left in the aircraft.

It does not take much imagination to translate these into similar failures in an NPP. Furthermore, they all are a type of failures that in principle could be detected by a thorough post-condition ORV. In other words, they are failures that are characteristic of specific subsystems or components, rather than the (aircraft) system as a whole.

Since aircraft maintenance is highly regular and highly regulated, there is considerable emphasis on the use of procedures as a way to reduce or avoid maintenance errors. One of the two main aircraft manufacturers promotes the following analogy between a procedure and a musical score: (1) they both specify performance; (2) different "orchestras" produce different performance; and (3) everyone must respect the composer's intentions. The analogy is less frivolous than it may seem, which becomes clear when a detailed comparison is made, cf. Table 1.

Table 1: Similarity between a musical score and procedures.

Musical score	Maintenance procedure
Play the instrument you can play	Match your objectives to your skills and abilities
Play the right score	Make sure you are using an applicable procedure; if in doubt, ask.
Play the score by reading it	Read the procedure and follow it **step-by-step** (no shortcuts)
Make sure you play the right note	Check if you are not sure; monitor the consequences of your actions; report any problems.
Stay in tempo with the orchestra	Synchronise your actions with the rest of the group.

The relevance of this analogy becomes obvious if it is compared to the use of procedures at Bugey, Diablo-Canyon, and North-Anna, as described above. At Bugey the operators would freely improvise, at Diablo-Canyon they would play the score as an unimaginative machine, and at North-Anna they would generally follow the score, but introduce some improvisation. As we shall discuss later, procedures can be seen as representing a specific type of barrier system, with specific advantages and disadvantages.

3.10 Summary

The findings from the literature survey reported above contain a number of common pointers or indicators, although they do not provide a complete picture. One reason for this is possibly that the majority of research relating to NPP operation has considered

the risks associated with power operation and work in the main control room. This goes for the human factors related work as well as risk and reliability analyses. The same situation is found in other domains, possibly because the effects of maintenance errors are found mostly during power operation and are difficult to trace back.

By way of summary, the findings presented above show the following important points:

- The diversity of causes related to human performance issues is much larger for LERs than for scrams. Considering the nature of outage work, there is every reason to believe that the diversity will be no less for this kind of work.

- The analysis of human errors related to maintenance showed a gradual reduction as the NPP went through consecutive stages of test and verification. However, the reduction was far from satisfactory, and about 2/3 of the errors remained in the system after the maintenance work had been completed. The Pyy et al. (1997) study also suggested that a description of consecutive barriers or defences was a useful conceptual vehicle.

- A study of maintenance errors showed that incorrect execution of steps (sequence errors) probably was more important than simple omissions. It was also found that a large contribution (in the order of 30%) came from procedures. The organisational setting, the occurrence of time pressure, and the quality of training were identified as important issues.

- A study of outage management identified five organisational type factors. It was also pointed out that the efficiency by which outage work was managed was an important issue.

- One study proposed the use of functional modelling to describe how performance constraints may affect outcomes. This model could also be applicable to show the couplings and dependencies between separate, but interlinked, tasks.

- A comprehensive study of outage work in France and the USA showed important differences in the way procedures were used, and in the balance between decentralisation and centralisation. Since humans never can be expected to follow procedures to the letter, it is better to acknowledge this from the start and ensure that the organisational structures and functions are able to manage a flexible type of conformity. Rigid conformity requires that procedures are complete and comprehensive in all respects, and this goal can never be achieved in practice. This is true for procedures for design-base activities, and therefore even more so for maintenance and outage work.

- A description of the learning that takes place between different projects (outages) point to two main mechanisms: codification and personalisation. Effective learning and improvement require a judicious combination of both.

- The lessons learned form aviation point to the disruption of otherwise routine maintenance work as a significant cause of errors, and also emphasised the role of procedures to ensure efficient performance.

4. Operational Readiness Verification and Maintenance

As discussed already, ORV – or requalification, which is the term preferred by the CSNI – can be realised on different levels, ranging from individual components to entire systems. On the component levels ORV can consist of mechanical test (whether a part can move as it is supposed to), a functional test (whether a pump can be started), a static check (whether a valve is in the desired position), etc. These tests are realised by the work-leader after an intervention has taken place and have been characterised as post-condition ORV tests.

In contrast to that tests on the level of the whole system will be more complex and are often performed from the control room. Once maintenance work has been performed on one subsystem, the whole function must be tested before work is begun on another subsystem and/or before restart. The first case corresponds to a kind of systemic post-condition test, the latter to a pre-condition ORV test. A comprehensive or integral test, during which all safety systems are considered, is in any case necessary run before restart.

In terms of the current project, a focus on ORV alone, as the practice of test and evaluation, would be too narrow. ORV is an integral part of maintenance and should be seen as such. In fact, a lack of ORV can in some sense be understood as an "error of omission" in performing the maintenance task. ORV incidents may therefore be seen as a case of maintenance errors not discovered in time.

4.1 Conditions Favouring Maintenance Errors

The kinds of incorrect actions that can occur during maintenance and ORV are not different in kind from incorrect actions made under other conditions. This means, that there are no **specific** errors that are unique to maintenance / ORV and which do not occur otherwise. Indeed, there are only a very limited number of possible error modes (action error modes), which are common to all domains and types of human activity. On the other hand, it must be expected that the **distributions** of error modes differ from one type of work to another, hence that there is a characteristic distribution or profile for maintenance and ORV work. This was amply illustrated in the study by Bento (1988).

The literature survey as such has not gone into a detailed analysis of maintenance or ORV errors. Based on the general experience and the findings that commonly are reported in the literature, it is nevertheless reasonable to assume that sequence errors and omissions are highly characteristic for maintenance and ORV activities. In accordance with the discussion above, the sequence errors and omissions are not just those that occur in the ORV activities, but also in the maintenance work as such. Two sources that address this issue are Hollnagel (1998a) and Reason (1997).

Table 2: Detailed classifications for sequence errors and omissions.

Specific antecedents for error mode "Sequence" (Hollnagel, 1998a)	10 feature that increase the probability of occurrence of errors of omission (Reason, 1997)
Interface, temporary **::** Access limitations	
Communication **::** Communication failure	
Interpretation **::** Faulty diagnosis	
Planning **::** Inadequate plan	The step occurs close to the end a the task
	Steps recently introduced /change from previous practice)
	Steps involving the installation of multiple items
	A step is functionally isolated from preceding actions
Procedures **::** Inadequate procedure	The goal of the task is achieved before the task itself is completed
	Steps not always required in the performance of the particular task
Person, temporary **::** Inattention	
Person, temporary **::** Memory failure	Steps involving recursions of previous actions
	Steps are not required in other very similar task
	Steps dependent upon some former action, condition or state
Observation **::** Observation missed	The object concerned with the step is out-of-sight

Although the two sources treat the subject quite differently, it is possible to relate them to each other, as shown by Table 2. The description by Reason focuses on psychological "mechanisms" or mental traps that may lead to a step being omitted, whether it is related to maintenance work or ORV testing. The description by Hollnagel reflects the lessons learned from risk and hazard studies, and points to the commonly recognised factors that may result in the incorrect performance of a sequence of actions – specifically the omission of an action.

Looking at the combination of factors in Table 2, the two main groups relate to inadequate planning and inadequate procedures, with individual performance variability (memory failures) as a third important group. These findings are in good agreement with the conclusions from the literature survey, and are therefore an important indication for the direction of work in the remaining part of Phase I of this project.

5. ORV As A Barrier System

A common analogy or image for accident prevention is the notion of barriers or defences, which has been made popular by the notion of the "Swiss cheese model" (Reason, 1997). Indeed, within the nuclear community the concept of defences has been institutionalised via the notion of defence-in-depth as defined in a report from the International Nuclear Safety Advisory Group (INSAG). The primary aim of these guidelines is NPP safety during operation (IAEA, 1996), which includes "all activities performed to achieve the purpose for which a facility was constructed" (IAEA, 2000, p. 94), hence also maintenance.[1] It is therefore highly relevant to apply the defence-in-

[1] The definition of operations specifically includes maintenance, refueling, in-service inspection and other associated activities.

depth principle to the ORV problem. One only has to look at the objectives for defence-in-depth listed by the INSAG report to realise that. The first and the second objectives mentioned by the report are:

- To compensate for potential human and component failures.

- To maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves.

A third objective, which has less immediate relevance for the ORV issue, is "to protect the public and the environment from harm in the event that these barriers are not fully effective".

The very purpose of ORV is to "compensate for potential human and component failures" by ensuring that such failures are detected and corrected in time. This is done by a series of defences or barriers that are distributed throughout the outage activities. In the normal defence-in-depth system the barriers are mainly of the physical or material type, such as the containment, or of the functional type, such as the safety injection systems. This is because the primary objective is to avoid the uncontrolled transportation of mass or energy in the system. For maintenance and ORV, the barriers must be of a different type, since the possible risks are in the form of activities that are not carried out. Whereas the barriers for the normal operating situation can be described in relation to the physical topology of the plant and focus on defences aimed at specific sources (reactor vessel, steam generators), barriers for maintenance and ORV must be described in relation to the flow of work, i.e., a temporal rather than a physical structure.

One suggestion for that structure can be found in the work by Pyy et al. (1997), and can be seen in Figure 4 above. This figure lists five different detection states, which correspond to different phases of the maintenance work. The five detections states are: preventive actions during outage, outage, start-up, preventive actions during power operation, and power operation. (The sixth state mentioned in Figure 4 is not considered here, since a disturbance clearly is not a part of the normal progression of work.)

If we consider work during an outage, there is an obvious logic to the temporal ordering of tasks, which in the main coincides with the five detection states suggested by Pyy et al. Referring to the basis for the representation in Figure 1 and Figure 2, we will propose the following sequence of events:

- The maintenance work itself. This is carried out subject to procedures and job descriptions of various types, which are followed to a larger or smaller extent by the operators. The procedures are in principle a kind of barrier, since they among other things serve to prevent incorrect actions from taking place.

- ORV as post-condition. These are the tests that are carried out when the maintenance work on a specific subsystem or component has been completed. Such tests are often prescribed by the procedures, but are in this context considered to be conceptually separate.

- ORV as pre-condition. In accordance with the distinction proposed above, the use of ORV as a pre-condition test aims to ensure that the reconnected system is in a ready state before the start-up is begun.

- The start-up sequence itself. This is regulated by procedures, which include various checks and tests. It is assumed that some of the checks are carried out automatically, i.e., by the technological systems themselves. Such tests are normally defined as operational pre-conditions and are part of the I&C logic.

- Power operation. This is an extended phase of steady-state operation, but regular checks are a part of that.

- Finally, the automatic safety systems also constitute a barrier. They serve to catch the effects of unexpected internal and external events before they turn into disturbances as such. An NPP is constantly monitored in different ways to ensure that it stays within the envelope of normal performance. This monitoring constitutes a barrier against incidents and accidents.

Putting all these together, we propose a view of a set of barriers as shown in Figure 7. The reader may find it is interesting to compare this with the requalification strategy described in Section 8.2.2 below. As the arrows illustrate, the barriers are intended to capture and "reject" errors, so that in the end nothing is left that can lead to incidents or accidents. Practical experience shows that these principles do not always work as planned, although the data provided by Pyy et al. hopefully overstates the problem.

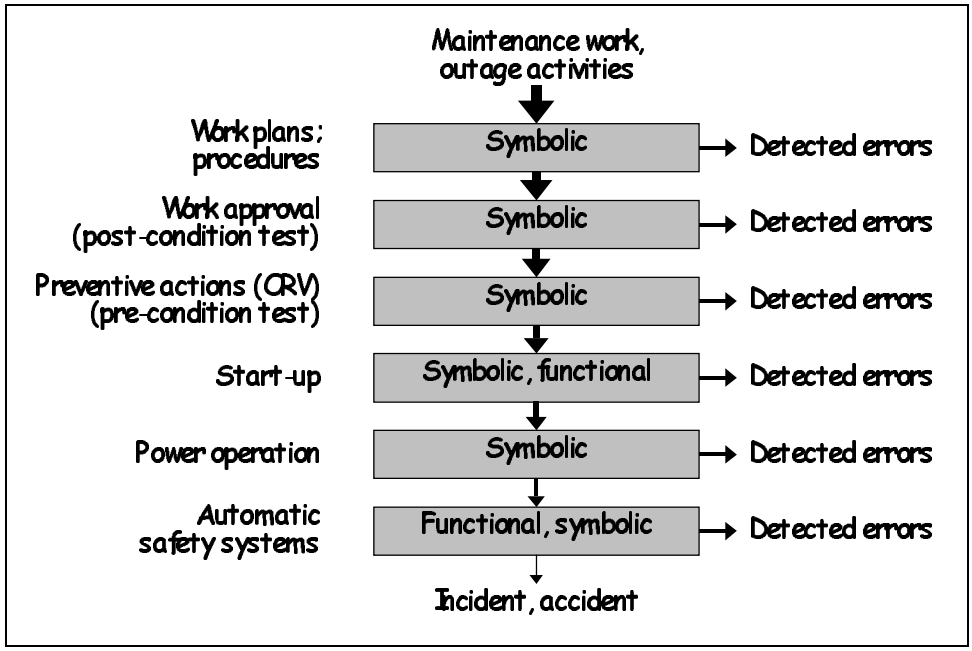

Figure 7: Layers of barriers related to ORV.

The various barriers in Figure 7 are described as either symbolic or functional, and these terms have also been used occasionally in the preceding. The terms refer to a classification of barrier system and barrier functions proposed by Hollnagel (1999). From an analytical point of view a distinction must be made between a **barrier function** as the specific manner by which a barrier achieves its purpose, and a **barrier system** as the substratum or foundation for the barrier function, i.e., the organisational and/or physical structure without which the barrier function could not be accomplished. For example, a valve provides the barrier function of preventing a flow (when it is closed), and is an example of a functional barrier system because it can be in different

states (closed-open). From this starting point it is possible to define four basic barrier systems, as follows:

- **Material barrier systems,** which physically prevent an action from being carried out or the consequences from spreading. Common examples are buildings, walls, fences, railings, bars, cages, gates, etc., and specifically the containment. A material barrier system is an actual physical hindrance that prevents certain actions and outcomes, and although it may not be effective under all circumstances, it will at least slow it down or delay it.

- **Functional barrier systems** impede an action or function, for instance by establishing a logical or temporal interlock. A functional barrier system effectively sets up one or more pre-conditions that must be met before something can happen. A valve, for instance, prevents flow when it is closed, but not when it is open.

- **Symbolic barrier systems** require an act of interpretation to work, hence an "intelligent" agent that can react or respond to them. Whereas a functional barrier works by establishing an actual pre-condition that must be met by a system before further actions can be carried out, a symbolic barrier indicates a limitation on performance that may be disregarded or neglected. All kinds of signs and signals are symbolic barriers, specifically visual and auditory signals. The same goes for warnings (texts, symbols, sounds), interface layout, information presented on the interface, visual demarcations, and procedures (because they require interpretation).

- **Immaterial barrier systems** are not physically present but depend on the user's knowledge to achieve their purpose. Typical immaterial barrier systems are rules, restrictions, and laws. In industrial contexts, immaterial barriers are largely synonymous with the so-called "organisational barriers" which are rules for actions that are imposed by the organisation, rather than being physically, functionally or symbolically present in the system.

Since ORV is based on the use of procedures and tests (checklists), it is essentially a symbolic barrier system using this terminology. This is evident from Table 3, which shows an analysis of the nine incidents according which type of barrier failed. (The nine incidents are reported in IEAE (1999) and described further in Section 7.1 below.) In all cases the barrier systems were of the symbolic type, specifically instructions or procedures. Unlike a functional barrier system, such as an automatic limit checker, there is a need to interpret the instructions before they are acted on. As Figure 7 indicates, there may in addition be functional barrier systems involved, in the sense of technological safeguards, alarm and monitoring functions, etc., but none of these were involved in the nine incidents.

Table 3: Type of barrier failure in the nine Swedish ORV incidents

	Incident								
	F2 / 95	B2 / 96	F1 / 96	O2 / 96	R2 / 97	R4 / 97	O1 / 97	O2 / 98	O1 / 98
Work plans, procedures									
Work approval (post condition test)							X	X	X
Preventive actions (pre-condition test)	X		X	X		X			
Start-up		X			X				
Power operation									
Automatic safety system									

6. Conclusions

As a result of the literature survey, it is proposed that a useful characterisation of the ORV issues found in ORV can be based on a systematic description in terms of barrier systems and barrier functions with specific characteristics, and in particular specific strengths and weaknesses. This characterisation should be combined with some way of accounting for the dependencies within activities and barriers as well as between activities and barriers, for instance using the type of functional modelling suggested by Rasmussen & Petersen (1999). It is clear that a major weakness of ORV activities when considered as a system of barriers is that their order cannot be guaranteed. In other words, operators and maintenance workers may – deliberately or inadvertently – deviate from the prescribed order, for instance to accommodate an immediate demand or to avoid slowing down the work of others.

The proposed conceptual framework could be used to evaluate the effects of the recommendations from SKI to the Swedish NPPs concerning routines for verification of operational readiness after interventions affecting safety systems ("Rutiner för säkerställande av driftklarhet efter ingrepp i säkerhetssystem" [Dnr 8.25/961657]). These recommendations listed five precautionary actions that should be implemented to improve safety during a transition from a shutdown state to a full production stage:

1. Review and evaluate existing procedures related to the handling, verification and reporting of readiness issues in connection with interventions in already verified safety systems.

2. Overview and analyse the need for improvement in routines and procedures for managing and planning of work during ongoing outages, in particular re-planning (rescheduling) of work. Special attention shall be given to routines relating to the scheduling of STF-related tests. The order of occurrence of tests specified by the STF shall be examined and routines and instructions shall be approved.

3. Overview and analyse routines for handling potential deviations from procedures, with particular emphasis on situations that may occur during the change from an operation to a shut-down operational regime, as described by the rules and regulations of the STF.

4. Overview and analyse possible improvements of the operators' work practices and the feasibility of supports that may be provided track of ongoing and completed tasks and tests.

5. Overview and analyse possible improvements to safety related indicators and routine rounds in the control room, with the aim of achieving increased clarity and usability, as well as verification that safety systems are tested and ready.

The framework could further be used as a basis for systematically evaluating past incidents and current practice and to describe the following in more detail:

- The existing structure of multiple barriers / defences in Swedish NPPs, i.e., the way in which ORV is practically organised, both formally and informally. This might also look into the different management styles, as suggested by the Bourrier studies.

- Detection / verification "mechanisms" and procedures. This would provide an overview of the actual and potential approaches that could be used to ensure ORV, and further characterise each in terms of its advantages and disadvantages as seen from a systematic description of barrier systems and barrier functions.

- Dependencies that may exist between particular instances of detection / verification "mechanisms" and procedures. These dependencies should include both those that are derived from the theoretical point of view (e.g. by using functional models), and by studying actual practice, and in particular the constraints on work that arise during outages. It is, in fact, these constraints, which turn potential dependencies into actual ones, and thereby make the ORV system vulnerable.

- Finally, it would be useful to attempt an analysis of the distribution of action error modes, i.e., the kinds of performance failures that are characteristically seen in outages as documented by the cases that have been reported in Sweden. Specific emphasis should be given to the types of performance deviations that may defeat existing ORV procedures and approaches.

7. Description and Analysis of the Current Situation in Sweden

As described in the introduction, this report presents the findings from the two parts of Phase 1 of a study on safety during outage and restart of nuclear power plants. The preceding sections have described the literature survey. The remaining sections will describe the results of a field survey of the present situation with respect to ORV/DKV. This field survey looked specifically at current organisational and MTO aspects at the Swedish NPPs. The field survey is based on visits to most of the Swedish NPP and interviews with representatives from the technical staff who are or have been involved with or responsible for ORV. The visits and interviews took place between the months of November, 2000 and March, 2001.

One purpose of the interview-based field survey was to find out which solutions the various NPPs had developed to cope with the problem, and which steps had been taken specifically to improve the efficiency of ORV. However, as soon as the interviews started it became clear that it was contentious to separate ORV from the rest of the work done in a NPP during outages since in practice many of the proposed solutions have a broader scope than the ORV problems they were meant to address. For instance, solutions such as a **better** organisation of the outage period, **better** processes in order to learn from experience and a **better** "safety culture" are features, which benefit ORV as well as other aspects of work in the plant.

Finally a number of research questions are identified. While some questions are of generic value; like inferences with safety culture issues, or the influence of technical solutions on operators' work, others are more specifically linked to ORV.

7.1 The Incidents

Nine events involving issues related to re-qualification have been reported in Sweden between 1995 and 1998. All of these involved safety components / systems that were left inoperable when the plants were restarted after outages. The nine events happened in seven of the twelve Swedish NPPs (Table 4). Each event has been the object of extended reporting and analysis of root causes, which were distributed among four different classes being: (1) weaknesses of administration processes, (2) weaknesses in management, (3) weaknesses in human performance and (4) weaknesses in the control room layout (Committee on the Safety of Nuclear Installations; IAEA / NEA, 1999). In addition, at least one other event happened that has not been the subject of an official report (in the Forsmark NPP).

Table 4: Operational Readiness Verification Incidents in Swedish NPP

Date	Plant	Type	Power (MW)	Start of operation	Incident	Time before discovery
JUL 1995	F-2	BWR	1006	1981	Valves in the Containment Pressure Relief systems erroneously closed	2 days after start-up
JUN 1996	B-2	BWR	615	1977	Erroneously left open valve caused degraded containment pressure suppression function	Unknown
JUL 1996	F-1	BWR	1006	1980	Valves in the Containment Pressure Relief systems erroneously closed	Power ascension
NOV 1996	O-2	BWR	630	1975	Erroneously left open Disconnecting Switch caused inoperability in the Low Pressure Core Spray System	8 days after start-up
AUG 1997	R-2	PWR	917	1975	Steady State Protection System erroneously left inoperable	16 hours
SEP 1997	R-4	PWR	960	1983	Valves in the Containment Spray System erroneously closed	Unknown
OCT 1997	O-1	BWR	465	1972	Valves in the Containment Pressure Relief systems erroneously closed	7 months
AUG 1998	O-2	BWR	630	1975	Valves in the Residual Heat Removal System erroneously left inoperable	1 year (previous outage)
OCT 1998	O-1	BWR	465	1972	Valves in the Standby Liquid Control system erroneously left inoperable	12 days

Each of the four general classes of root causes mentioned above can be described in further detail. In the descriptions, *italics* are used to highlight qualifiers that require interpretation by end users, hence are potentially ambiguous.

The first, general weaknesses regarding **administrative processes**, can be illustrated by the following examples:

1. Routines for how to act in case an unexpected situation arises were often "*too weak*", i.e., incompletely specified.

2. In some cases maintenance operations took place on systems that already had been declared operable.

3. The logistic of the operability test has shown itself to be too weak.

4. The routines for re-planning during outage have "*sometimes*" been "*significantly weaker*" than the original planning routine.

The second, **weaknesses in management,** can be illustrated by the following examples:

1. It seems that management "*sometimes*" has not been aware of the impact of poor procedural routines.

2. It seems that management was not able to maintain a (sufficiently) high level of safety culture, specifically to ensure that every employee fully understood the importance of maintaining a high number of safety barriers.

Of the third class, the main "**weakness in human performance**" was the tendency for operators to anticipate procedural steps without "*adequately*" checking preceding work. However, as this weakness was identified subsequent to finding that root causes related to general time pressure it can be seen as a specific instance of that. Lack of time is apparently a common condition, and it is stated in the incident reports that "*enough time is always a strict condition for success*". We shall therefore come back to this point later. The interviews with operation personnel seem to confirm time-pressure as a factor instigating the incidents (at least as perceived by the workforce). Moreover, time pressure itself can be identified as originating in poor scheduling of the outage, and/or in the economical context.

Finally the **weaknesses in the control room layout** can stem from the fact that control rooms are designed for operation and that they therefore may be ill fitted to represent the plant state during outage and / or during the transition period between outage and operation.

A concrete example of how the general weaknesses can manifest themselves is illustrated by Table 5, which shows the case for events at the OKG.

Table 5: Root Cause of ORVs as identified in OKG

Administrative Routines	Conflicting demands (ex STF)
	Unclear structure and goal
	Instructions' hierarchy
	Instructions are used in a way not intended
The Human Factor	Deviation caused by time-pressure
	Supervisory possibilities, indications are missing
	Many activities at a time, hard to keep an overview
	Many persons involved
	Different standards for how to do things
Organisational Weaknesses	Planning
	Unclear principles (aim of testing / configuration)
	Training / Education
	Availability of competence and resources

Re-qualification problems have mainly been found in relation to outage periods, and re-qualification is usually considered a task for operations personnel. The control room operators are, in fact, responsible for making specific systems available for maintenance as well as for re-qualifying these systems when maintenance has been completed. This obviously presumes that the maintenance has been carried out in an appropriate manner. The maintenance activities themselves may, however, require that some kind of checking is carried out by the maintenance personnel, for instance to ensure that a repaired object is not leaking. Since the first step of re-qualification is to check whether the maintenance task has been done, it is important for operations personnel to get the correct information. This communication is implemented via the work-orders management group (ABH – Arbets Besked Hantering) and does not seem to have shown weaknesses.

There are, however, a few exceptions to this strict division of responsibility. Thus, for systems that are quite "*far*" from reactor safety, re-qualification is usually part of the maintenance task. This raises the question of how clearly this separation is defined; in other words, when is a system "*far enough*" away from the reactor so that the re-qualification can be left in the hand of maintenance personnel?

Moreover, while it is necessary to re-qualify a system after maintenance, it can be done in a more or less formal manner. While a high level of formality is required by the STF for specific safety systems, the requirements are less strict for specific production systems. Yet for operators the latter may be just as important. While there is a need to be safe, there is also the need to produce electricity. This often leads to contrasting strategies for safety systems and production systems and raises the question of where the line should be drawn – or even whether such a line should be drawn at all?

Another problem underlying the incidents has been the organisation's incapacity to manage the unexpected. Whatever weight an organisation lays on planning, improvisation always occurs (Weick, 1998). Interactive complexity and tight-coupling are properties of NPP that render them subject to unforeseeable accidents (e.g. Perrow 1984; Reason 1988); it is impossible to plan everything, and it is therefore necessary to be able to improvise. How has this issue been taken care of?

In Table 1, we observed very different time to discovery of the erroneous action; from a few hours to almost one year. As shown on Figure 8, there seems to be fundamental

differences between the “weaknesses” of the different settings, which led to these incidents.

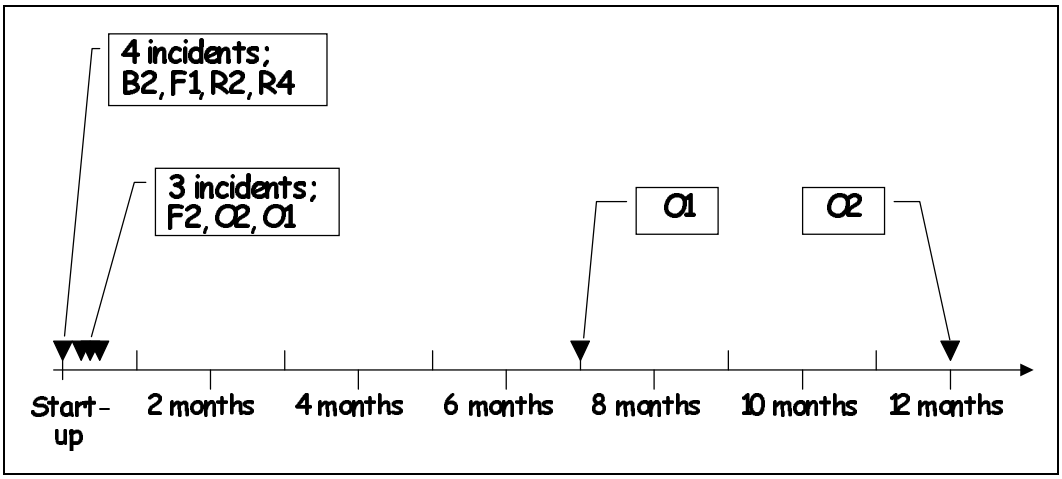

Figure 8: Time before discovery.

7.2 Important Changes in the Environment

It was earlier stated that time-pressure is seen as a root-cause of many incidents. Some of the solutions for coping with time pressure are in the hands of the NPP management, although much may be beyond their control. One factor is the general economical context, which is likely to have an important influence on time pressure; when plants are shut down for outage they do not produce electricity, and the outage period should therefore be kept as short as possible.

The actual deregulation of the electricity market, seen in Sweden as well as in many other countries, has also led to stronger competition between electricity producers and to a general decrease in the price of electricity. The “obvious” conclusion is that deregulation means that the time-pressures increase. The reasoning is that as the price of electricity goes down there is a need to reduce non-productive costs, and therefore to reduce outage time. However, many operators have experienced the opposite effect; since the price of electricity has gone down, so has the pressure to reduce the duration of outages!

To understand this apparent paradox, we need to understand the shift that has occurred in measuring plant performance. Ten years ago the key number for measuring performance was the availability of the plant: “how many days per year are we producing electricity?” Since the deregulation of the electricity market, a new key number came into play and ultimately replaced the old one; the new question that had to be answered was “how much money do we earn?” Since outages usually take place during periods when electricity costs are low, the pressure to start producing again is not as high as it used to be. We thus observe a contradictory but at the same time fully rational scheme in which a higher emphasis on costs led to a lower time pressure for operators!

8. “Specific ORV Solutions”

This section discusses the different solutions that have been proposed to cope with the problems identified during the investigation mentioned in Section 7.1. The solutions have been assigned to two major categories: technical and organisational.

8.1 Technical Solutions

8.1.1 Overall Re-qualification Schema

The so-called ÖDS (“*Övergripande-Driftklarhets-Schema*”) provides operators in the control room with a general view of the plant situation regarding re-qualification. It consists of a hierarchically organised representation of the plant systems. As soon as a system is ready to operate (i.e.,. re-qualified) the ÖDS is marked by the operator in charge, to indicate that no further work should be done on that system.

8.1.2 “Blocked Safety Function”

This system, called *Blockerad Säkerhets Funktion*, is often called “*Röda Lampor*” (Red Lamps) because of its appearance in the control room. It consists of position indicators for a number of important valves, grouped logically (through a computerised algorithm) and visualising the availability of the different subs. Each sub is divided into five groups: reactivity, activity-barriers, hard-emergency cooling, cooling system and electricity system. It thus has the following appearance on the control room’s operating panel (Figure 9).

Each row represents a sub and clearly shows the availability of that, and thus the availability of the plant. The requirement is that at least three subs have to be operational.

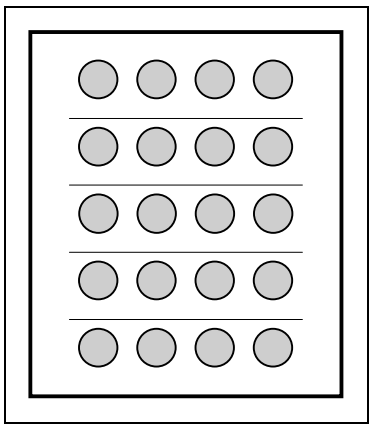

Figure 9: “Röda Lampor”.

In addition to providing the operators with an overview of the availability of the plants’ safety systems, the combination with a computer system makes it possible for operators to investigate further the reason behind a perceptible unavailability. In fact since each

lamp represents a number of different valves, the computer system is necessary for such an investigation to be possible.

8.1.3 "Computerised Operational Position Control"

Datoriserad Driftläges Kontroll (DDK) is a computerised system that makes it possible to compare the actual position of systems with their expected position (depending on the condition of the plant). The computer shows the deviations from the "normal situation". However, this system is not online, but it requires operators to interrogate the computer to find out whether divergences exist.

8.1.4 Central Indication in the Control Room

Some valves used to lack indication in the control room. For instance the position of some valves close to the reactor could not be checked directly; instead tests had to be performed to check their position. Some of these valves now have position indicators in the control room.

8.1.5 Comments to the Technical Solutions

Most of these technical solutions have been part of the design of the newer plants (e.g., Oskarshamn-3, Forsmark-3). To implement them in older plants requires essential changes both in the station and in the control room. Their implementation thus usually goes together with general reconstruction plans.

8.2 Organisational Solutions

8.2.1 Operational Readiness Plan

An organisational readiness plan ("*driftklarhetsplan*") describes the availability / operational readiness state of the different systems in parallel to the STF specifications and the maintenance plan (see Figure 10). It specifies the expected state of the different systems along the whole outage period.

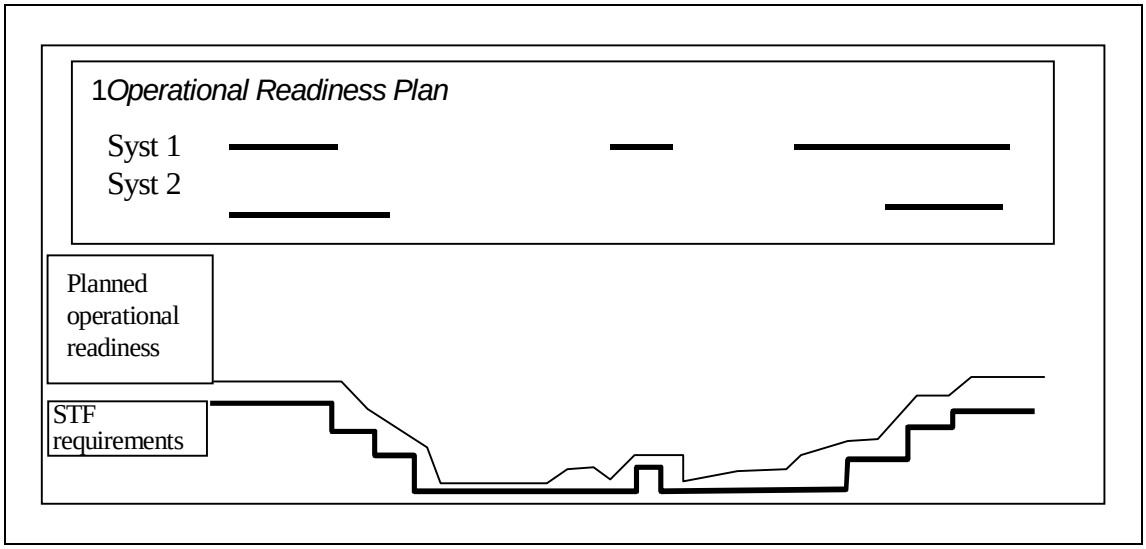

Figure 10: Operational Readiness Plan.

8.2.2 Systematic Way of Working

Following the observation that the logistic of operability tests was inadequate or missing (Committee on the Safety of Nuclear Installations), a systematic way of working has been defined which should apply to any system, though in a more or less formal manner. This logistic defines four steps in achieving operational readiness: (1) reinstating control ("återställningskontroll"), (2) "*basläggning*", (3) "*driftsättning*", and (4) testing (see Figure 11).

- Reinstating Control: Operations personnel controls that the maintenance work has been done. This is an administrative control but it provides an opportunity for operations personnel to "*sit back and think*" whether it is actually the right time to restore the system, whether all the maintenance work is done on that system, etc. The aim of this phase to prevent any further work once the system has been declared ready for operation.

- "*Basläggning*" and "*driftsättning*". First, all the valves are repositioned. Following that, the components (pumps, etc.) are tested functionally ("*driftsättning*") one by one.

- Testing. Finally, the whole system is tested, and then if the test is satisfactory the system is declared operationally ready!

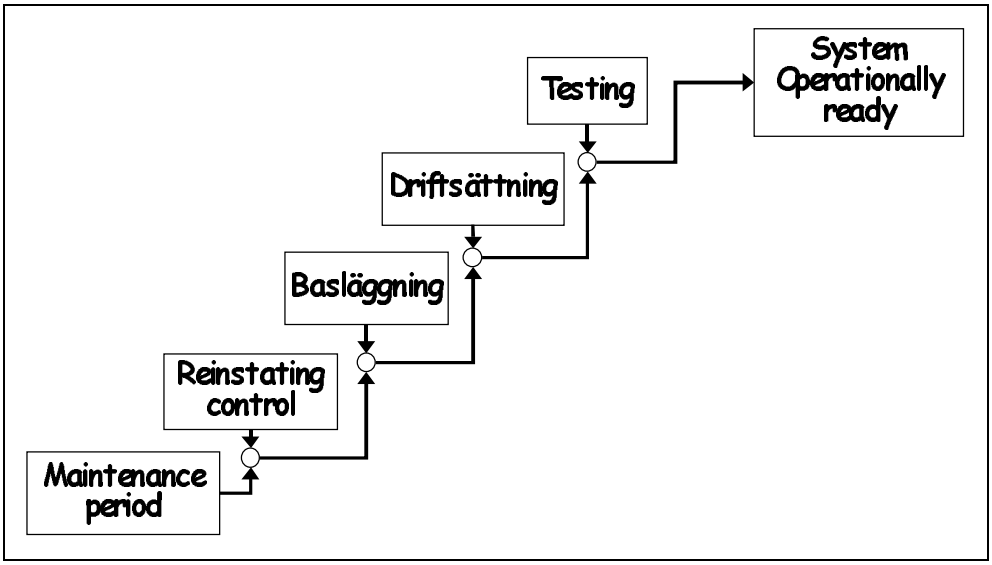

Figure 11: Re-qualification Strategy.

8.2.3 New Instructions

New instructions / procedures for re-qualification have been written for specific safety systems. Their structure is built according to the four steps of the work logistic described above: reinstating control, "*basläggning*", "*driftsättning*" and testing. Moreover, deviations from plans should be reported on the first page.

8.2.4 Co-ordination ("Samfunktions") Testing

This is a co-ordinated test of all the safety systems. However, this may introduce new risks since some systems have to be shut down before running this test, e.g., some valves have to be closed! Thus new re-qualifications tasks must be performed consecutive to this testing phase.

8.2.5 Redundant / Independent Control

At the very end of the outage period before the change from one level of operation to another one, an independent, physical control is performed on all the valves. The redundant control is often performed from a different point of view; for instance while the first control might have been done relative to systems, the second may be done relative to functions or even topographically. These different points of view are extracted from a database. In addition, the person who performs the check comes from the outside. This person may, of course, have been involved in the outage but has usually not been so active.

This redundant control is performed during a time-out at the end of the outage, but the plant operators do not experience the time-pressure on this time-out period as high. Yet even though none of the interviewees ever needed more time than initially planned, they all felt they could use more time whenever necessary.

8.3 What, Where?

In the following Table 6 we represent which solutions have been implemented at which NPP in Sweden (with the exception of Barsebäck). This should, however, not be used as a basis for a comparison between plants, since most of the "solutions" (especially the organisational ones) have to be anchored in the plant's culture and history as discussed later in this report. Moreover, there are fundamental differences between the different units in each plant, which can give rise to a number of objections to this table.

Table 6: Plants vs. Solutions

	Oskarshamn	**Forsmark**	**Ringhals**
Technical Solutions			
ÖDS	Yes	Yes	No?
Röda Lampor	Partially	Yes	No
DKK		Yes	
Organisational Solutions			
Operational Readiness Plan	Yes		
Systematic Way of working	Yes	Not explicit?	Not explicit?
New Procedures	Yes		
"Samfunktionsprov"	Yes	Yes	Yes?
Time-Out	Yes	Yes	Yes

9. Planning and Organisation of the Outage periods

Planning the outage can hardly qualify in itself as a solution to the ORV problems encountered. However, a well prepared and well planned outage period has a lower probability of encountering problems than a poorly prepared one. Thus we found it interesting to examine how the different plants organise themselves, both for planning the outage and during this period of extreme workload, which the outage is. We also tried to understand how deviations from the original plan are managed.

9.1 Planning the Outage

In Forsmark, the planning personnel used to be made up of four persons for each unit. Nowadays (since February, 2001), all the three units depend on the same division in which 10 persons are working all year around with planning the outages.

In Oskarshamn, on the other hand, a couple of persons per unit are centralising the planning work of the outage all year around, but the whole organisation is involved. The Operational Readiness plan is generated as well.

Here we saw an important difference between two plants; on the one hand planning is delegated to the different units, while on the other hand, planning is a centralised function of the plant. The impact of centralised and decentralised activities on safety has been discussed elsewhere. Both can be argued to positively and negatively affect safety. A proper balance between those two is often encouraged (Döös & Backström, 2000; Perrow, 1984; Weick, 1987).

9.2 Following the plan

As outside observers, it was important for us to understand how outage periods are organised: who are the participants? what is done? how are the tasks distributed? etc. While similarities can be observed on a general level, major differences between plants exist which go beyond simple difference in vocabulary. The difficulty we have had to get clear pictures of the organisation certainly originates in our lack of specific plant vocabulary, although this does not explain everything. Thus we found it interesting to underline the difficulties interviewed personnel had to describe the organisation they are involved in.

While Figure 12 to Figure 14 supposedly represents different organisations, it is our opinion that they actually represent different formal views of organisations that actually are very similar in the way they function.

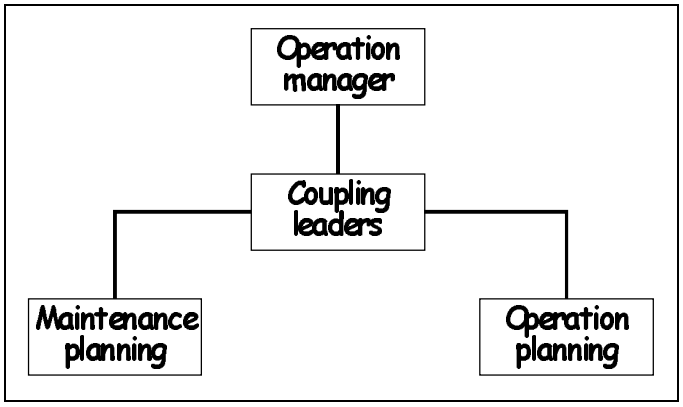

Figure 12: Outage Organisation at Forsmark.

9.2.1 Forsmark

Approximately one month before the start of the outage, control room personnel are attached to the planning division. These coupling leaders ("*kopplingsledare*") have the task to support the Operation Manager ("*driftvakt*"). These six persons are split into three pairs, one for each function: electricity, reactor, and turbine. They are working day-time; in fact, one of each pair starts at 5:00, while the other one comes later and leaves around 24:00. Their work is twofold: they are to deliver work permits, and they support continuity between the operational shifts.

Twice a day ("*morgonbön*", "*aftonbön*") all the parties meet, that is Operation Management ("*driftledning*"), Coupling Leader, Operation planning and Maintenance planning. Moreover, the operation manager meets the coupling leaders twice a day as well, one time before the morning meeting and a second time after the evening meeting.

As the coupling leaders' work is physically demanding, the coupling leaders are replaced when outages lasts longer than 20 days, even though this may be in middle of the outage.

9.2.2 Oskarshamn

During the outage, daily meetings take place between the concerned partners (operation, maintenance and outage planning). These approximately 10 persons meet to discuss the work plan for the next 24-36 hours. These meetings only take place on weekdays (i.e., from Monday to Friday).

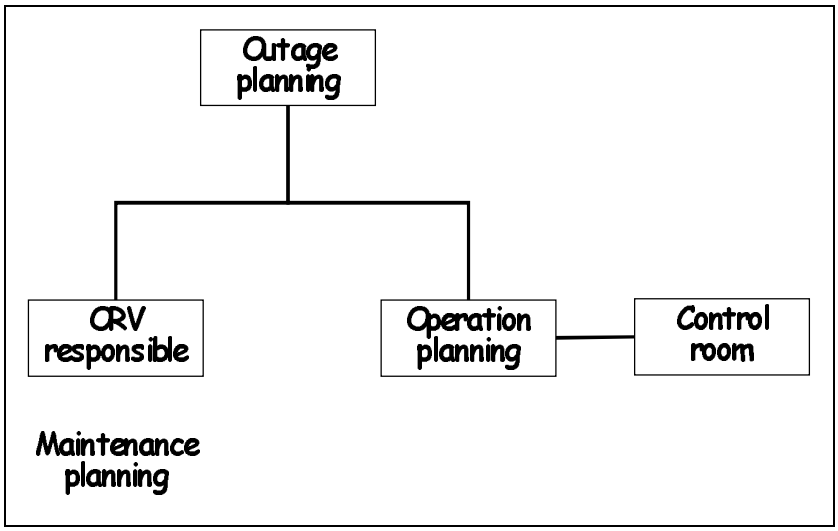

Figure 13: Organisation at OKG.

One person is responsible for ORV matters and works as a link between the maintenance division and the work-orders management (ABH) group.

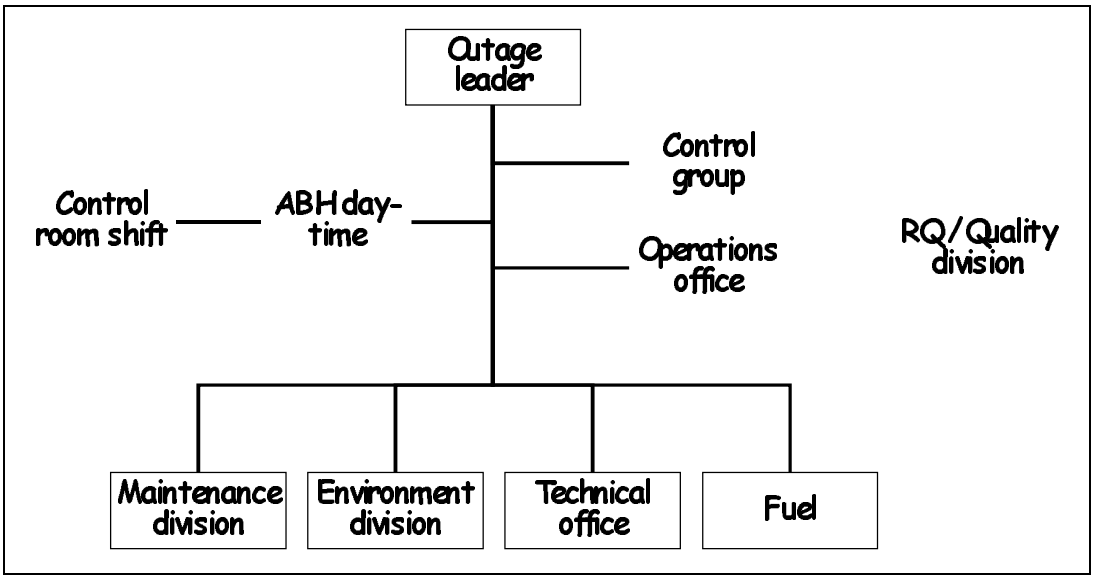

Figure 14: Outage Organisation at Ringhals.

9.3 Managing the Unexpected

In each plant, though the plan for the whole outage is ready before start, more specific plans for the coming 24-hour period are the one used by the operation manager. It does not cause further problem if the planning needs to be delayed because tasks take more time than originally planned. In case supplementary tasks need to be performed that were not initially planned, discussion is brought to the outage meetings.

This tendency to delay instead of changing the original plan has been observed in each plant. Although many interviewees have acknowledged this fact, it seems important to be aware of possible discrepancies between excepted official lines and actual practice, even on an unconscious level. The next section shows, however, how employees have perceived a certain improvement in the way outages are planned and thus in the organisation's ability to manage the unexpected. This part is as well to be related to the previous section, which discussed important changes in the environment that seemingly decreased time pressure on outages and thus decreased the need for re-planning.

9.4 Improvements?

Many of the interviewees have acknowledged a certain "*improvement*" in the way outages are planned.

> "*Jag tycker den fungerar bra .. den har utvecklats mycket de sista år, och den är nog också delvis en del av det här DKV .. den där med DKV plan. Man innan revisionen planerar systemsdriftklarhet under revisionen. … det är ett stöd .. i kontroll rummet… framför allt för driftingenjör*" [OKG2-26].

> "*Jag känner det var mer förut .. men idag i och med vi har logistiken så är det inte lika mycket. När vi går in i revisionen, upplever jag att vi är mer förberedda ... alltså alla arbeten är inplanerade under revisionen på ett mycket bättre sätt än det var för 5-10 år sen. Men visst sker det omplaneringar, men det är, vill jag säga, sällan sånna här stora omplaneringar där man ändrar driftklarheten på ett markant sätt. Då tar man näst hellre en revisionsförlängning idag .. för att några har insett, eller vi har insett tycker jag att det är så svårt att genomskåda allt som påverkas, och. blir det mycket ändringar i instruktioner, i driftordrar, och det ska då redovisas, det ska stämplas, och så granskas och godkännas. Så den administrationen… och sen finns det ändå en liten så där 'har vi glömt nånstans'. För att när skiftlaget jobbar aktivt med de dokumenten och de upptäcker att den här stämmer inte, då måste man kalla dit folk och reda ut den och den tar sin tid. Då är det bättre upplever jag några gånger, … vi resonerar så att det är bättre att ta den lilla förseningen i så fall.*" [OKG1-11].

This larger confidence in the organisation's ability to plan the outage in a more effective and safe manner is hard to analyse. Many different factors could lead to this increased confidence. Of course the main factor could actually be increased organisation's abilities, but this still is to be determined.

10. Learning from Experience

Another point, not directly linked to ORV but still of interest, is how learning occurs through the organisation. This includes learning from one outage period to the next,

learning from one unit to another, learning from one plant to another and finally learning from other fields. Although this issue is far too complex to be studied in details in this report, it nonetheless constitutes an important point to be considered.

Every plant seems to have developed processes to make improvements from one outage period to another one. The outage planning group usually meet all the different parties after each outage to discuss improvement points, usually leading to the writing of a report. In many plants a "black book" is also often available for comments. Informal discussions between operation personnel seem as well quite appreciated within the organisations. These different means toward improvement could easily be fitted into the inter-project learning model proposed in (Antoni, 2000) and presented in an earlier section of this report.

Learning from experience from one unit to another is not always that easy. However, between similar units the task seems attainable. Some plants have implemented systematic feedback processes. For instance, in Forsmark there are seven shift-teams working in each unit. Each of these is specifically responsible for certain systems. Contacts between corresponding teams of F1 and F2 are systematic; all changes in one unit lead to discussions with / information of the other unit. Moreover informal discussions are encouraged:

> "*Vi springer mellan varandra hela tiden när det är frågor… diskuterar hela tiden så att det blir en levande erfarenhetsåterföring hela tiden kontinuerligt, så fort det upstår nåt. …det blir en arbetsmetod man använder som jag tror fungerar mycket mycket bättre… det är samma mellan skiftlagen när det dyker upp frågor, diskuterar de med respektive författning…*" [FKG-18].

However, in other plants, like for instance in Oskarshamn, feedback is not systematic:

> "*vi har en sånt mötte för oss på 1:an. 2:an och på 3:an har sina mötten och sen byter vi inte; vi kunde lätt byta de där erfarenheterna mellan .. det kan vi inte säga vi gör så där mycket, eller sånt här formellt i alla fall.*" [OKG3-35].

Concerning learning possibilities from other fields, we can refer to the recent cooperation between the Forsmark group and the airline SAS. Since, as stated in the literature review, we find commonalties with the field of civil aviation regarding ORV issues, such an experience seems valuable and further investigation could be of interest for ORV issues.

11."Safety Culture"

Since incident investigations highlighted a certain lack of what is commonly referred to as "safety culture", some plants involved themselves in a formal work toward improvement (STARK-utbildning at OKG). Despite the interest of the question this work shall not be reviewed here.

Safety Culture is a complex and ill-defined concept. While some definitions see culture as a state or a goal by itself (Cheyne et al., 1998; Clarke, 1998; IAEA, 1991; Lee, 1998), others understand it as a process (Carroll, 1998; Hudson, 1999; Westrum, 1991). While some define it as a tool to measure an organisation's disposition for safe operation, i.e., safety culture is used as synonymous for safe operation (Reason, 1998; Reason, 1997),

others see it as a toolbox which enables safe operation (Weick, 1987). However, it is important to bear in mind the holistic and multi-faceted nature of the concept (Cooper, 2000; Döös & Backström, 2000).

From the High Reliability Organisations (HRO) research literature, an important aspect of safety culture seems to be the ability of organisational members to manage paradoxes (La Porte & Consolini, 1991; La Porte & Thomas, 1995; Rochlin, 1989; 1999), and particularly the following one. This paradox is closely linked to the search for continuous improvement in which HROs are engaged. Rochlin (1993) summarises this paradox under the three following points: (1) while HROs perform at very high levels, their personnel are never content, but search continually to improve their operation; (2) HROs set goals beyond the boundaries of present performance, while seeking actively to avoid testing the boundaries of errors; and (3) HROs search for performance and suspicion of quiet periods continually regenerates operational challenges even during times when things seem to be working quite well. On the individual level, we observe operators that reflect on how to carry out their work (Sanne, 1999). On an organisational level, "*continual reinvestments*" to improve safety are seen as the only way of maintaining the high level of reliability (Schulman, 1993). In fact, only very few activities are not subject to re-evaluation and critical assessment (Ibid.). Let us finally quote Rochlin once again:

"… the culture of safety that was observed is a dynamic, intersubjectively constructed belief in the possibility of continued operational safety, instantiated by experience with anticipation of events that could have led to serious errors, and complemented by the continuing expectation of future surprise. Rather than taking success as a basis for confidence, these operators, and their managers, maintain a self-conscious dialectic between collective learning from success and the deep belief that no learning can be taken to be exhaustive because the knowledge base for the complex and dangerous operations in question is inherently and permanently imperfect." (Rochlin, 1999).

Some of the interviews seemed to show evidence of such a culture among the interviewees. As we saw earlier, most of them are really confident in the organisation's ability to plan and carry out safe outage periods. They are even quite confident in the organisation's ability to learn, since they acknowledge a "*clear*" improvement during the last years of exercise. However, we also observed their uncertainty regarding the sufficiency of the actual organisational features; most of the interviewees stated that no solution is "*100 % safe*". Further work would however be needed in order to properly assess the organisations' safety culture.

12.Linking Theory and Practice

In the first part of this report, the literature survey presented different models related to human and organisational aspects of NPP safety, in relation to ORV issues. It was proposed that a systematic description in terms of barrier systems and barrier functions with specific characteristics, and in particular specific strengths and weaknesses, would be a useful way of characterising the issues that are found in ORV. This was tentatively formulated in Figure 7 as a model of the several layers of barriers. Based on the findings from the field survey, we are now in a position to describe further the characteristics of steps 1 to 5 as shown in Figure 7.

12.1.1 Step 1: Maintenance Work

As stated earlier, this study found that not much work has been done to involve maintenance personnel in ORV issues.

12.1.2 Step 2: ORV As Post-Condition

Different barriers have been added and/or improved. Mainly, the systematic way of working with its four phases (reinstating control, "basläggning", "Driftsättning" and testing) represents an important symbolic barrier when used together with a specific procedure, and an immaterial barrier when no specific procedure is required for a specific system. This systematic way of working strongly resembles the STARK-concept, and seems particularly promising. If fully internalised by all operators, the immaterial barrier it then provides is very appealing.

12.1.3 Step 3: ORV As Pre-Condition

The main barrier is the so-called *samfunktionsprov*, tests during which the functions (made of different systems) are tested. These tests however affect the operational readiness of some systems. In order to reduce such side effects, the position of some valves is now indicated in the control room, reducing the number of tests to be performed.

12.1.4 Step 4: Start-Up

Right before start-up the redundant / independent control constitutes an important barrier as well.

12.1.5 Step 5: Power Operation

Finally, under power operation such technical artefacts as Röda lampor, or DKK, constitute symbolic barriers as well.

12.2 Additional aspects

The previous analysis of ORV as a barrier system does not tell the whole story. In fact a major weakness of ORV when it is considered as a system of barriers is that their order cannot be guaranteed. In other words, operators and maintenance workers may, deliberately or unintentionally – deviate from the prescribed order, for instance to accommodate an immediate demand or to avoid slowing down the work of others. And at least three important aspects of safety in relation to ORV can only with difficulty be introduced in the previous analysis. The importance of safety culture and the importance of learning from experience have both been argued before and further discussion will not take place at the moment. However it seems important to focus on more time on a third aspect, namely the ability of the organisation to plan the outage in a right manner, together with its ability to improvise in case unexpected events occur.

Concerning the ability of the organisation to plan the outage period and to support operators in following the plan, work has been done in different directions, and it seems

that work planning has been improved. Moreover such tools as the operational readiness plan (driftklarhetsplan) and the overall re-qualification schema (ÖDS) were developed to support operators in following the plan.

Regarding the organisation's ability to improvise in order to cope with unplanned events not much work seems to have been conducted.

13. Conclusions And Some Research Questions

Even though we might be able to answer whether the above "solutions" are theoretically effective, it is much harder to judge how effective they are in the context of implementation. For instance, the new "ORV procedures" created in OKG might theoretically present many advantages (e.g., clear structure), but judging their effectiveness in settings cannot be done on the basis of today's study. Of course, some factors seem to demonstrate the ability to positively influence ORV safety. For instance, while some operators were hesitant to these procedures when they were first introduced, they seem to have become accepted in the operator community (OKG2-22, OKG3-34). Some factors for "*successful*" implementation could also be suggested (involvement of operators in the design of these procedures, positive outcomes of their use, etc.). However, despite confirmation from the literature (e.g., Bourrier, 1999), these are just hints for further research and cannot be considered as research findings. Thus, up to that point the following questions are unanswered.

13.1 Differences between plants

There seems to be important differences in the way in which plants look at ORV issues, and thus in the way they try to develop "solutions". It is clear for everyone that solutions have to be anchored in the plants' culture. There are no ideal solutions; they have to fit the context of implementation (Bourrier, 1999; Roberts, 1993). Some interviewees acknowledged that the process of improvement has not been a straightforward process; many solutions have been tried but few of them have been kept. For that reason it seems important to conduct further research at one plant only.

13.2 'Too Many Barriers?' Acceptance Of The "Solutions" Among Personnel… Relations To Safety Culture

It has been observed that the implementation of new procedures or new barriers is not a simple matter. Since one cannot "force" people to follow procedures, their usefulness has to be demonstrated to those who are involved. When a new preventive barrier is created (as for instance through the creation of a new control or check) it is important that everyone understand its utility. New barriers should not be seen as a lack of trust in the personnel in charge of previous stages in the process. Nor should people in charge of such previous stage release their attention and rely on later stages.

Closely linked to these issues is the concept of safety culture. As it has been observed previously in this report, safety culture is a complex and ill-defined concept. Without oversimplifying this "*holistic and multi-faceted*" concept, the definition we want to retain (at least until further notice) is Gene Rochlin's: "*the culture of safety that was observed is a dynamic, intersubjectively constructed belief in the possibility of continued operational safety, instantiated by experience with anticipation of events that could have led to serious errors, and complemented by the continuing expectation of future surprise.*" (Rochlin, 1999).

Understanding the foundations of such a culture is of interest. Especially we could try to answer the following questions:

- What creates such a belief?
- How can organisational factors support such a belief?
- How can this belief be used more efficiently by the organisation?
- etc.

13.3 Navigating Grey-Zones

We previously observed that ORV lies at the boundary between two very different worlds. ORV seems to be accepted as an operational issue, i.e., not of the concern of maintenance. However, maintenance personnel are involved at the first step of ORV; they are the ones who can answer the question whether a component is ready to be used. Tests on the systems' level should be able to answer this question as well but they are not always possible. This leads to an interesting paradox; while the literature survey made us focus on maintenance, practitioners clearly emphasised ORV as an issue for operational personnel.

Another ambiguity is whether ORV concerns all systems and if there should be fundamental differences between safety and production systems. Some plants decided not to differentiate between these two kinds of systems, even though a difference in the emphasis on formality exists. Other plants openly decided to focus on safety systems only. There are pros and cons for each decision. For instance, having the same work procedure for every system tends to increase clarity, while it might be time consuming. Differentiating between different systems pose the question of where to put the limit between safety and non-safety systems. And even though some techniques might be available to support this decision (PRA, Total Productive Maintenance, etc.) there will always be zones of uncertainty – Grey-Zones.

Management, and specially safety management, often focuses on planning. As we have seen a good planning of the outage seems to increase its chances of safe progress. Anyhow, regardless of the emphasis put on planning, unexpected situations will always occur, especially in complex systems. Organisations therefore have to be able to cope with unexpected, unplanned events (Weick, 1993). As we analysed the ORV related incidents we saw organisations which showed a weak ability to improvise when facing unexpected events. A group of organisational scientists assembled around Karl E. Weick found that the metaphor of jazz improvisation might be a good concept to help understand how organisations deal with the unplanned (e.g. Weick, 198). In fact central

to jazz improvisation is a balance between structure and freedom, autonomy and interdependence and surrender and control (Barrett, 1998), in other words the ability to navigate grey-zones.

Especially since ORV seems to be situated in different grey-zones, and because people do improvise whatever weight is put on planning, studying operators' work with ORV under an outage period might help us understanding the following points:

- How people deal with dualities (structure vs. autonomy, controlled vs. creative action, etc.) in their daily work.
- The relations between structure and improvisation; improvisation is not a chaotic process.
- How practising improvisation may improve safety.
- How organisation can support value-added improvisation.
- etc.

13.4 Technical Solutions: Complex Influences on operators' work

We saw in this report that different technical tools have been developed to support operators' work. Since people started to get interested in the use of tools, they realised that the relations between the users, the tools and the environment are complex (Ihde, 1979; Reason, 1988). The introduction of automation and its limitations has been abundantly discussed elsewhere with at least a recurrent conclusion; automation changes the task at hand (Bainbridge, 1983). It has been seen many times that the introduction of automation changes the task of operators into supervisory control tasks (Dekker & Hollnagel, 1999). However changes can also be more subtle, and in order to understand these subtle changes we first need to understand that the boundaries of the unit of analysis for cognition have to be extended and that the range of mechanisms assumed to participate in cognitive processes has to be extended as well (Hollan et al. 2000). Building on years of experience of studying cognition in real settings, "in the wild" (e.g. Hutchins, 1995), Hollan et al. (2000) proposed the four following tenets of a theory of distributed cognition:

– *Socially Distributed Cognition*: Put simply, this means that cognitive processes are socially distributed across the members of a group, but this also has the "odd" implication that the cognition of an individual is also distributed.

– *Embodied Cognition*: The organisation of mind is an emergent property of interactions among internal and external resources.

– *Culture and Cognition*: Because we live in complex cultural environments the study of cognition is inseparable from the study of culture.

– *Ethnography of Distributed Cognitive Systems*: A consequence of the previous three tenets is the need for a "new kind" of cognitive ethnography.

Let us look closer at the embodiment of cognition, as this is the domain where human-machine relations are in focus. During the recent years, the idea that minds are not representational engines whose primary function is to create mental model of the external world has found strong support. The modelling of human minds as information processing entities has lost interest. In fact "*the relations between internal processes and external ones are far more complex, involving coordination at many different time scales between internal resources-memory, attention, executive function- and external resources-the objects, artifacts, and at-hand materials constantly surrounding us. […] The organisation of mind is an emergent property of interactions among internal and external resources.*" (Hollan et al., 2000, 177). Cognition is always embedded in context, in situations (Hollnagel, 1998b). That is, work environments from time to time become elements of the cognitive systems; they do not only constitute of stimuli for a cognitive system. In other words, the introduction of new technology into a task world changes the task at hand.

Thus for a complete understanding of the effect of the technical solutions on ORV, more work would be required along, for instance, the tenets of the theory of distributed cognition as proposed by Hollan et al. (2000).

13.5 Quality of Testing

A distinction is usually made between three levels, or types, of tests: object test, system test and (safety) function test. The complexity of the NPP directly mirrors on the tests: while theoretically "simple", these tests in practice show themselves to be quite complex.

The aim of the present study is to analyse the different steps of testing in order to understand the impact on safety. Relation between tests and safety is not totally straightforward; while adding new tests increase the chance of discovering shortcomings, it also creates new risks: tests often require sub-systems to be shut down. It is thus necessary to adopt a fully holistic view when constructing tests.

As seen earlier, one plant tried to systematize its way of working with ORV issues, by implementing a four steps procedure to built up operational readiness. We also observed that this systematic way of working was especially noteworthy as creating an immaterial barrier (such as the concept STARK). Especially in the face of complexity, immaterial barriers seem to be of interest.

The study would take place at O3 during partial/sub-outages (subavställningar). These periods allow empirical work to be conducted in a more appropriate environment; personnel are of greater availability than during full outage period. Moreover, the occurrence several times a year would allow two periods of data gathering to take place over a shorter period of time.

14. References

Antoni, M. (2000). *Inter-Project Learning - A Quality Perspective. Division of Quality Technology and Management*. LiU-Tek-Lic-2000:35, Linköping, Linköping University.

Aufort, C. & Desmares, E. (1995). *Nuclear safety and the sub-contracting of maintenance operation*. Joint OECD/NEA-IAEA Symposium on Human Factors and organisation in NPP Maintenance Outages: Impact on Safety, Stockholm, Sweden.

Bainbridge, L. (1983). Ironies of automation. *Automatica, 19*, 775-779. Reprinted in: (1987) Rasmussen, J., Duncan, K. and Leplat, J. (eds.) *New Technology and Human Error*, Wiley, Chichester, pp. 276-283.

Bardot, A. (1995). *Improving the quality and safety of maintenance operations during unit outage*. Joint OECD/NEA-IAEA Symposium on Human Factors on organisation in NPP Maintenance Outages: Impact on Safety, Stockholm, Sweden.

Barrett, F. J. (1998). Creativity and improvisation in jazz and organizations: implications for organizational learning. *Organization Science, 9*(5), 605-622.

Baumont, G. (1995). *Ergonomic study of a French NPP outage unit*. Joint OECD/NEA-IAEA Symposium on Human Factors on organisation in NPP Maintenance Outages: Impact on Safety, Stockholm, Sweden.

Bento, J.-P. (1988). Analysis of human performance problems at the Swedish nuclear power plants. *IEEE Fourth Conference on Human Factors and Power Plants*, 55–60.

Bourrier, M. (1999). *Le nucléaire à l'épreuve de l'organisation.* Le Travail humain. Paris, France, Presses Universitaires de France.

Carroll, J. S. (1998). Safety culture as an ongoing process: culture surveys as opportunities for enquiry and change. *Work & Stress, 12*(3), 272-284.

Cheyne, A., Cox, S., Oliver, A. et al. (1998). Measuring safety climate in the prediction of levels of safety activity. *Work & Stress, 12*(3), 255-271.

Clarke, S. (1998). Safety culture on the UK railway network. *Work & Stress, 12*(3), 285-292.

Committee on the Safety of Nuclear Installations (CSNI). *Requalification problems following outages***:** 38.

Cooper, M. D. (2000). Toward a model of safety culture. *Safety Science, 36*(2), 111-136.

Dekker, S. W. & Hollnagel, E. (1999). *Coping with computers in the cockpit,* Ashgate.

Döös, M. & Backström, T. (2000). *Control and learning - the necessary coexistence of incompatible cultures.* Social Construction of Risk and Safety, workshop on, Kolmården, Sweden.

Haber, S. B., Barriere, T. & Roberts, K. H. (1992). Outage management: A case study. In. E. W. Hagen (Ed.) *Proceedings of IEEE Fifth Conference on Human Factors and Power Plants.*

Hansen, M. T., Nohria, N. & Tierney, T. (1999). What's your strategy for managing knowledge? *Harvard Business Review, March-April*: 106-116.

Hollan, J., Hutchins, E. & Kirsh, D. (2000). Distributed cognition: Toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction, 7*(2), 174-196.

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

Hollnagel, E. (1998b). Context, cognition, and control. *Co-operation in process management - Cognition and information technology*. Y. Waern. London, Taylor & Francis.

Hollnagel, E. (1999). Accidents and barriers. In J.-M. Hoc, P. Millot, E. Hollnagel & P. C. Cacciabue (Eds.), Proceedings of. *Lez Valenciennes, 28,* 175-182. (Presses Universitaires de Valenciennes.)

Hudson, P. (1999). Safety culture - the way ahead? Theory and practical principles. *Profiting Through Safety: Proceedings of the International Aviation Safety Management Conference*. L. Hartley, E. Derricks, S. Nathan & D. McLeod. Perth, Australia, IASMC**,** 93-102.

Hutchins, E. (1995). *Cognition in the wild*. Cambridge, Mass., MIT Press.

IAEA (1991). *Safety culture* (Safety Series No.75-INSAG-4). Vienna, Austria: International Nuclear Safety Advisory Group.

IAEA (1996). *Defence in depth in nuclear safety* (INSAG-10). A report by the International Nuclear Safety Advisory Group. Vienna, Austria: International Atomic Energy Agency.

IAEA / NEA (1999). E*rroneous safety system status control after outage* (International Incident Reporting System IRS-7303). Vienna, Austria: International Atomic Energy Agency.

IAEA (2000). *IAEA safety glossary: Terminology used in nuclear, radiation, radioactive waste and transport safety.* Vienna, Austria: International Atomic Energy Agency.

Ihde, D. (1979). *Technics and Praxis*. Boston, D. Reidel.

La Porte, T. R. & Thomas, C. W. (1995). Regulatory compliance and the ethos of quality enhancement: Surprises in nuclear power plant operations. *Journal of Public Administration Research & Theory, 5*(1), 109-138.

La Porte, T. R. & Consolini, P. M. (1991). Working in Practice but Not in Theory: Theoretical Challenges of 'High-Reliability Organizations'. *Journal of Public Administration Research and Theory,* January, 19-47.

Lee, T. (1998). Assessment of safety culture at a nuclear reprocessing plant. *Work & Stress, 12*(3), 217-237.

Maqua, M. (1995). *Organizational Influences in NPP Outage Events*. Joint OECD/NEA-IAEA Symposium on Human Factors and organisation in NPP Maintenance Outages: Impact on Safety, Stockholm, Sweden.

Neau, E. & Lewkowitch-Orlandt, A. (1995). *Refueling Outages at EdF in NPP - A new Organization to ensure improved nuclear safety, industrial safety, working conditions and duration outages.* Joint OECD/NEA-IAEA Symposium on Human Factors and organisation in NPP Maintenance Outages: Impact on Safety, Stockholm, Sweden.

Perrow, C. (1984). *Normal Accidents: Living With High-Risk Technologies*. New-York, USA, Basic Books, Inc.

Pyy, P. & Saarenpää, T. (1988). A method for identification of human originated test and maintenance failures. In. E. W. Hagen (Ed.) *Proceedings of IEEE Fourth Conference on Human Factors and Power Plants*, 1988.

Pyy, P. Laakso, K. & Reiman, L. (1997). A study on human errors related to NPP maintenance activities. *IEEE Sixth Annual Human Factors Meeting*, Orlando, Florida, 12-23 – 12-28.

Rasmussen, B. & Petersen, K. E. (1999). Plant functional modelling as a basis for assessing the impact of management on plant safety. *Reliability Engineering and System Safety, 64*, 201-207.

Reason, J. T. (1988). Cognitive aids in process environments: prostheses or tools? *Cognitive engineering in complex dynamic worlds*. E. Hollnagel, G. Mancini and D. D. Woods. London, Academic Press.

Reason, J. T. (1998). Achieving a safe culture: theory and practice. *Work & Stress, 12*(3), 293-306.

Reason, J. T. (1990). *Human Error*. Cambridge, Cambridge University Press.

Reason, J. T. (1997). *Managing the risks of organizational accidents*. Aldershot, UK, Ashgate Publishing Limited.

Reiersen, C. S. & Gibson, W. H. (1995). *Identification of, and protection against, human error during maintenance.* Joint OECD/NEA-IAEA Symposium on Human Factors and organisation in NPP Maintenance Outages: Impact on Safety, Stockholm, Sweden.

Roberts, K. H., Ed. (1993). *New challenges to understanding organizations*. New York, Maxwell Macmillan International.

Rochlin, G. I. (1989). Informal organizational networking as a crisis-avoidance strategy: U.S. naval flight operations as a case study. *Industrial Crisis Quarterly, 3*(2), 159-176.

Rochlin, G. I. (1993). Defining "High Reliability" Organizations in Practice: A Taxonomic Prologue. *New challenges to understanding organizations*. K. H. Roberts. New York, Maxwell Macmillan International**,** 11-32.

Rochlin, G. I. (1999). Safe operation as a social construct. *Ergonomics, 42*(00).

Sanne, J. M. (1999). *Creating Safety in Air traffic Control*. Lund, Sweden, Arkiv förlag.

Schulman, P. R. (1993). The Analysis of High Reliability Organizations: A Comparative Framework. *New challenges to understanding organizations*. K. H. Roberts. New York, Maxwell Macmillan International**,** 33-53.

SKI (1996). *Säkerställande av driftklarhet efter ingrepp i säkerhetssystem - sammanfattning*. (SKI 8.25/961657). Stockholm, Sweden: Swedish Nuclear Power Inspectorate.

SKI (2000). *Ytterligare redovisning av åtgärder inom området verifiering av driftklarhet* (SKI 8.09-000879). Stockholm, Sweden: Swedish Nuclear Power Inspectorate.

U.S. Nuclear Regulatory Commission Inspection Report No. 50-306(92-005). *Prairie Island. Unit 2. Loss of RHR (February 20, 1992)*. Augmented Inspection Team Report, March 17, 1992.

U.S. Nuclear Regulatory Commission. *Loss of residual heat removal system* (Diablo Canyon). NUREG-1269, Washington, D.C., June 1987.

U.S. Nuclear Regulatory Commission. *Loss of vital ac power and the residual heat removal system during midloop operation at Vogtle unit I on march 20, 1990*. NUREG-1410, Washington, D.C., June 1990.

Weick, K. E. (1987). Organizational Culture as a Source of High Reliability. *California Management Review, 29*(2), 112-127.

Weick, K. E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. *Administrative Science Quarterly, 38* (December), 628-652.

Weick, K. E. (1998). Improvisation as a Mindset for Organizational Analysis. *Organization Science, 9*(5), 543-555.

Westrum, R. (1991). Cultures with requisite imagination. *Verification and validation in complex man-machine systems*. J. Wise, P. Stager & J. Hopkin. New-York, Springer.

APPENDIX A: Missing O-Rings on Eastern L-1011

The case is that of an Eastern L-1011 flying from Miami to Nassau in May of 1983. The aircraft lost oil pressure in all three of the engines in mid-flight. Two of the engines stopped, and the third gave out at about the time the crew safely landed the aircraft. It turned out that the O-rings, which normally should be attached to an engine part, were missing from all three engines.

One of the tasks of mechanics is to replace an engine part, called a master chip detector, at scheduled intervals. The master chip detector fits into the engine and is used to detect engine wear. O-rings are used to prevent oil leakage when the part is inserted. The two mechanics for the flight in question had always got replacement master chip detectors from their foreman's cabinet. These chip detectors were all ready to go, with new O-rings installed. The mechanics' work cards specified that new O-rings should be installed, and had a space next to this instruction for their initials when the task was completed. However, in their usual work situation this step was unnecessary, because someone else (apparently their supervisor) had already installed new O-rings on the chip detectors, but without initialling the work card.

The night before the incident, when the mechanics were ready to replace master chip detectors, they found there were no chip detectors in the foreman's cabinet. The mechanics had to get the parts from the stockroom. The chip detectors were wrapped in a "semi-transparent sealed plastic package with a serviceable parts tag". The mechanics took the packages to the aircraft and replaced the detectors in low light conditions. It turned out the chip detectors did not have O-rings attached. The mechanics did not check for them before installing them, but nevertheless did initial the work-card. There was a check procedure against improper seals; motoring the engines to see if oil leaked. The mechanics did this, but apparently not for a long enough time to detect oil leaks. The work card read "monitor engine and check chip detector for leaks" but it didn't specify how long. The mechanics had to fill in the gap, and it turned out the time they routinely used was too short to detect leaks.

Special training procedures concerning the importance of checking O-rings on the chip detectors were posted on bulletin boards and kept in a binder on the general foreman's desk. Theoretically, the foremen were supposed to ensure that their workers followed the guidance, but there was no follow-up to ensure that each mechanic had read these.

In this case, the airline had previous O-ring problems, but these were attributed to the mechanics. According to the NTSB report, the propulsion engineering director of the airline, after conferring with his counterparts, said that all the airlines were essentially using the same maintenance procedure but were not experiencing the same in-flight shut-down problems. Hence, it was concluded that the procedures used were valid, and that the problems in installation were due to personnel errors. Also, in reference to the eight incidents that occurred in which O-rings were defective or master chip detectors were improperly installed (prior to this case), the "FAA concluded that the individual mechanic and not Eastern Air Lines maintenance procedures was at fault".

NTSB Identification: **MIA83AA136** For details, refer to NTSB microfiche number **23663A**

Scheduled 14 CFR 121 operation of EASTERN AIRLINES, INC.

Incident occurred MAY-05-83 at MIAMI, FL
Aircraft: LOCKHEED L-1011, registration: N334EA
Injuries: 172 Uninjured.

DESCENDING THRU 15000 FT INTO NASSAU THE #2 ENG WAS SHUT DOWN DUE TO LOW OIL PRESS. AT 16000 FT RETURNING TO MIAMI THE #3 ENG FLAMED OUT, & 3 MIN LATER THE #1 ENG FLAMED OUT. THE ACFT BEGAN DESCENDING WITHOUT POWER FROM 13000 FT. AT ABOUT 10000 FT THE FLIGHT CREW ANNOUNCED THAT DITCHING WAS IMMINENT. THE #2 ENG WAS RESTARTED AT 4000 FT, & THE ACFT MADE A ONE-ENG LANDING AT MIAMI. ALL O-RING SEALS IN THE MASTER CHIP DETECTOR ASSY'S IN THE ENG LUBRICATION SYSTEM WERE MISSING CAUSING OIL LEAKS IN ALL ENGS. PROPER PROCEDURES TO REMOVE, REINSTALL & INSPECT THE DETECTORS FOR OIL LEAKS WERE AVAILABLE. THE FOREMAN KNEW THAT MECHANICS WERE NOT ROUTINELY REPLACING O-RING SEALS. ACCIDENT WAS 9TH CHIP DETECTOR OCCURRENCE SINCE PROCEDURES WERE REVISED 12/81. FAA AWARE OF PROBLEMS ON EAL ACFT BUT DID NOT ASSIGN SPECIAL SURVEILLANCE PRIORITY TO THEM. ATTENDANTS NOT AWARE OF TIME AVAILABLE TO PREPARE CABIN FOR DITCHING. PAX HAD DIFFICULTY LOCATING & DONNING LIFE VESTS.

Probable Cause

Lubricating system, oil magnetic plug .. Incorrect
Procedures/directives .. Not followed .. Company maintenance personnel
Maintenance, installation .. Improper .. Company maintenance personnel
Supervision .. Inadequate .. Company maintenance personnel
Unsafe/hazardous condition .. Not corrected .. Company/operator management
Lubricating system, oil magnetic plug .. Leak
Fluid, oil .. Starvation
Accessory drive assy, extension unit .. Overtemperature
Accessory drive assy, extension unit .. Failure, total
Accessory drive assy, ext shaft bearing .. Not engaged
Fuel system, pump .. Disabled
Fluid, fuel .. Starvation

Contributing Factors

Inadequate surveillance of operation .. FAA(organization)
Aircraft performance, two or more engines. Failure, total