nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-74
ISBN 87-7893-130-4

An analysis of errors of commission in the Nordic nuclear power plants based on plant operating experience

Pekka Pyy[1], Jean-Pierre Bento[2] and Yngve Flodin[3]

[1]VTT Automation, Finland
[2]JPB Consulting, Sweden
[3]SwedPower, Sweden

December 2001

Abstract

The report presents the methodology followed, the material used and conclusions drawn in a study of active human failures. First, the report discusses the concept of active human failures in the context of human errors. Then, a simplified methodology is presented applicable to analysis of operating experience and documenting all kinds of human failures. Also the material and analysis procedure used in the three parts of the study are discussed. Finally, some selected highlights of the results are presented with common conclusions and recommendations.

Key words

Human reliability, Operating experience, LERs, HRA, Errors of Commission

NKS-74
ISBN 87-7893-130-4

Pitney Bowes Management Services Denmark A/S, 2002

The report can be obtained from
NKS Secretariat
P.O. Box 30
DK – 4000 Roskilde
Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@catscience.dk

AN ANALYSIS OF ERRORS OF COMMISSION IN THE NORDIC NUCLEAR POWER PLANTS BASED ON PLANT OPERATING EXPERIENCE

Pekka Pyy
VTT Automation

Jean-Pierre Bento
JPB Consulting

Yngve Flodin
SwedPower

21.12.2001

FOREWORD

The study reported here formed a part of the Nordic nuclear safety research (NKS) programme 1998–2001. The research was sponsored by NKS, The Swedish Nuclear Power Inspectorate (SKI), Forsmarks Kraftgrupp (FKA) and TVO. This report has been prepared by Pekka Pyy (VTT Automation) with help from Jean-Pierre Bento (JPB Consulting), Per Evenéus and Yngve Flodin (SwedPower). Göran Hultqvist (FKA), Risto Himanen (TVO) and Anders Hallman (SKI) have provided guidance throughout the work, and the authors acknowledge their input. The participation of the personnel of the nuclear power plants Forsmark, Olkiluoto and Oskarshamn in the project work is also duly acknowledged.

Espoo, 21.12. 2001

CONTENTS

1 INTRODUCTION

The NKS/SOS-2 subproject AMF (aktiva mänskliga fel, in Swedish) concentrated upon studying the unforeseen effects of human actions on processes and components of nuclear power plants. Especially, the area of active human failures, sometimes called errors of commission, was studied. The classic definition for error of commission (EoC) is a somehow wrong human output i.e. selection error, error of sequence, time error (too early, too late) or qualitative error (too little, too much). This is sometimes called the phenotype of error. For comparison, errors of omission (EoOs) mean omitting an entire task or steps in a task. There are other definitions of commission errors. Some of them are presented in Appendix 1.

The need to complete PSAs with the analysis of errors of commission has been noticed world wide. Among others this topic is discussed within OECD Nuclear Energy Agency (NEA), CSNI/PWG5 task 97-2 (OECD, 2000). In addition, international nuclear power plant experience encompasses many significant events with human contribution. In the previous NKS-project RAK-1.3 (Andersson & Pyy, 1997), methods for the human reliability analysis were developed with the concept of integrated sequence analysis (ISA). ISA formed a basis for the NKS/SOS work presented here by highlighting the need for broader analysis of man-machine systems as a whole.

Human actions mostly lead to desirable consequences only. They complement from their part automated safety features of NPPs. Deviations from expected performance in human actions, such as EoCs or EoOs, may result either in a) active or b) passive equipment inoperability consequences in their target system (see Figure 2 in App. 1). Active consequences are different kinds of initiating events, including those making safety systems inoperable at the same time (CCIs), of PSAs and other unanticipated system / component functions. This is resource taking from the PSA point of view, since both the safety contribution and the physical consequences have to be further analysed for each case. In case of omission of equipment function the calculation of system response is much easier. Consequently, many PSAs only stick to simple EoOs in procedure based actions and their consequences, i.e. no start of a pump etc.

Significant nuclear events are often consequences of several human actions even including correct ones. Some of them form the kernel of the failure mechanism, and some other contribute to the strength of plant barriers, timing of the events and the final consequences of the case. Consequently, it was foreseen from the beginning that the search strategy of the NKS/SOS-2 subproject AMF needs to be broad to cover all human actions which may lead to active consequences.

2 SCOPE AND OBJECTIVES

The study scope was to cover control room activities, maintenance, surveillance testing and outage management, i.e., no human activities in nuclear power plants were restricted outside the scope. Although the working group saw the need to analyse operator activities in a detailed way, it was also identified that the used LER (licensee event report) material would probably also include a great deal of maintenance and testing activities.

The objectives of the project were to: 1) define the research area related to commission errors / active human failures, 2) perform a survey (identification and mapping) of them, 3) summarise Nordic views on the topic, and 4) recommend items and approaches for further development work.

From the PSA point of view, the primary goal was to identify failure modes that are not included in published PSA studies. Nevertheless, developing approaches for the analysis of active human failures and for the integration of this analysis into PSA is a large task. The authors are aware that this issue requires a more extensive research programme than was possible in one NKS period. In NKS/SOS-2, the priority was consequently put on scanning the problem area, and on forming a Nordic view on the subject.

3 USED METHODS AND MATERIAL

The phases of the study were:

1) Developing a methodology for the survey.
2) Mapping of commission errors.
3) Suggestion for an approach to analyse and manage commission errors.
4) Writing a project report.

The project phases are discussed in a more detailed way in the following chapters.

In addition, in-depth studies about specific topics were discussed at the outset of the project. These studies might have included, e.g. carrying out simulator runs, going through control room panels and such. The time and resources available did not allow for this kind of in-depth investigations. However, a brief review of potential design features mitigating deviations in human actions was carried out, and simulator instructors were interviewed in one subtask of the project.

3.1 Developing methodology for the survey

Developing methodology for the survey included a classification method and an approach for information retrieval. The work was based on prior experience and needs of the project so that a reasonable level of detail could be reached with optimal use of resources. Case histories were used to steer the development work.

The chosen approach begins by selecting a key human action. For each event, this means defining a primary (key) human action that brought a failure mechanism into the system. If there are other human failure events related to the event, they need to be considered as failed barriers. The primary action needs preferably to be found as close to the technical systems as possible. Thereafter, broken and effective barriers are investigated before and after the key action. Thus, the result became a barrier model depicted in Figure 1.

The next step was to fill in more detailed information about the key action. After that, causes and contributing factors of the event were considered. The decision was taken to use the classes presented in Appendix 2. Thereafter, various consequences, representing a variety of classes, were studied. The effect on systems, plant operation, safety (PSA / other) and economy (production loss) were considered as consequences.

The barrier model in Figure 1 shows how causal factors lead to failed human activities and from them to consequences due to the fact that barriers fail. Finally, the progression of the event is stopped by a barrier function, which may be physical, engineered design or organisational. Logically, if no barrier stops the event progression, an accident is born. The methodology is described comprehensively in a separate report (Holmberg et al. 2001) in Swedish.

The classification was transferred to columns in MS Excel software to form tables. Each case is represented by one row in the tables, so that the classification procedure described earlier could be followed. The tables were then distributed among the project participants. An example record from the tables is shown in Appendix 2 (Table Appendix 2-2).

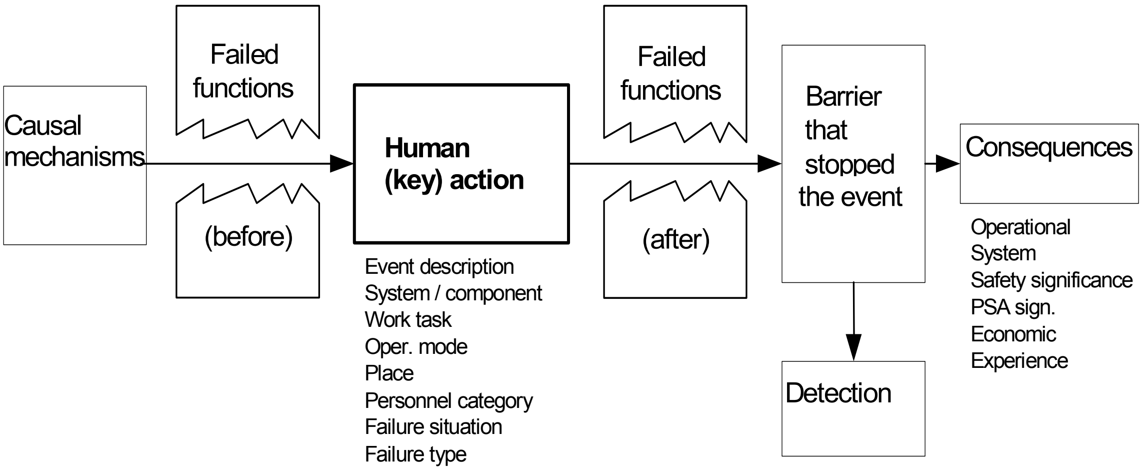


Figure 1. A schematic representation of the classification used in the AMF-study and the location of various categories in a barrier model.

3.2 Mapping of commission errors

The information about the incidents was based on operating experience from the years 1997-1999. It was aimed at establishing a database of events with human contribution for future uses.

For example, the following types of material were used to collect information:

1 Scram and disturbance reports
2 Other types of licensee event reports (LERs)
3 Yearly, quarterly and monthly reports
4 The yearly reports of the operating experience group and their appendices
5 MTO analyses
6 Operator and other personnel interviews
7 Interviews with persons involved in early plant design (about design principles against man machine problems)

Mostly, the mapping was based on scram reports and other LERs. It was performed in three separate studies for material from the years 1997-1999. VTT Automation studied the material from Olkiluoto NPP with the financing by TVO, JPB Consulting studied the material from Oskarshamn with a financing by SKI and SwedPower studied the material from Forsmark with financing by FKA.

Despite that the agreed analysis approach was mainly followed, there also were differences in the analysis scope. For example, SwedPower used operator and instructor interviews as complementary data sources. Furthermore, JPB Consulting utilised existing MTO analyses for the work, and completed them with additional information e.g. for PSA importance. The amount of LER cases for Forsmark was 29, and the material also included one scram. For Olkiluoto, 31 significant events, discussed in this report, were identified. Also 41 cases with a rather small safety and economic significance were found for Olkiluoto, but they were not analysed in a detailed way. The approach of JPB Consulting led to a significantly greater amount of events (151). The VTT study was the only one studying the events also from economical point of view.

4 SUMMARY AND CONCLUSIONS

4.1 Role of human activities in significant NPP events

In this section, the share of significant human actions in scrams and other types of LERs is discussed. The summary table of the related three studies is presented in Table 1. The amounts are events with human contribution and, e.g. the total amount of scrams for Olkiluoto through 1997-1999 was thus 10 (7 with human contribution corresponding 70 %).

Table 1. Human contribution in scram reports and in other LERs through 1997-1999.

Report type	**Number of cases (Percentage of all cases, %)**		
	Olkiluoto	**Forsmark**	**Oskarshamn**
Scrams	7 (70 %)	1 (10 %)	15 (70 %)
LERs	14 (48 %)	28 (15 %)	136 (40 %)
Sum	21 (68 %)*	29 (100 %)	151 (100 %)

* for Olkiluoto, significant faults are not automatically classified as LERs

As noticed, both the Oskarshamn and Olkiluoto report consistently quite high contributions of human actions, whereas the Forsmark study came up with a significantly lower share. The reasons for this low share are to some extent unknown, but JPB Consulting and VTT have used a considerable amount of work to go through plant documentation related to the events, including documents of the ERF-group, MTO-analyses and interviews of the involved people. SwedPower, on the other hand, concentrated more on interviewing operators, designers and training instructors.

Despite some inconsistency, the results point to the direction that human actions play a significant role in nuclear events. When looking at results one must also remember that the definition of a LER differs between Finland and Sweden – in Finland the definition is much stricter and not all the faults causing limiting condition to operation according to TechSpecs are classified as LERs.

In the next Chapters, the figures refer to all human failure events for Olkiluoto and Forsmark, whereas they mean EoCs for Oskarshamn. Using also only EoCs for the first two plants would not mean a significant change in the presented results, but the material would be smaller. This would have induced some more uncertainty in the results.

4.2 Consequences to systems and plant

Both in Olkiluoto and Forsmark events, the auxiliary systems of the reactor plant (300-systems) and electrical systems are well represented. The same finding applies to that part of events that was found to have a significant impact on safety (see section 0). Especially, system 321 was often the target of failed human actions, but these did not clearly represent a homogenous population. No direct conclusions may be based on that finding. The reason for this is that these systems play an important role for NPPs, generally, and any event in them often leads to LER reporting.

From **Oskarshamn** events, about 83% of the commission errors did not affect the operation of the units, meanwhile 10% resulted in automatic scrams. The finding is almost similar for the **Forsmark** events (89 % / 8 % correspondingly). The **Olkiluoto** data for the 31 identified significant events also included 18 events (58 %) with no significant impact on the plant output (scrams, reduction of power etc.). These high numbers show that not all the safety significant events have to cause a plant level disturbance (e.g. scram) immediately. This discussion will be expanded under section 0.

The comparison of "effect on plant systems" was not possible for all the three studies, because their material and scope were slightly deviating. What is interesting is that spurious system functions were identified only for Olkiluoto events (4 cases). These are real human failures with active plant or system level consequences. Two of them were due to problems with documents rather than with deviations in the task itself. A potential explanation for the low amount of such events is that the current PSA analysis practices distinguish two groups of events: unavailability (basic events) and initiating events (which are in many cases spurious functions). This forces an analyst to think accordingly. It may also be difficult to distinguish between spurious and failed component / system functions.

4.3 Work tasks involved and detection of the event

4.3.1 Work tasks involved

In this section, the share of different organisational departments and work tasks is discussed. The summary table of the related three studies is presented in Table 2 for the personnel categories.

Table 2. Involvement of different personnel categories in events

Personnel involved	**Percentage of cases (%)**		
	Olkiluoto	**Forsmark**	**Oskarshamn***
Operating	33	59	32
External contractors	19	7	19
Maintenance, electrical	19	3	31
Maintenance, mech.	13	10	21
Maintenance, I&C and data	23	21	16

*of EoCs (for Olkiluoto and Forsmark about all important events)

Considering the above figures, it should be mentioned that several personnel categories were involved in many events. This is the reason for the finding that the Olkiluoto and Oskarshamn columns may sum up to more than 100 %. In cases where many persons are involved, the role of communication and work task management was often important. Although the role of the plant own personnel is important, the supervision of external subcontractors obviously needs to be enhanced, too.

The type of a work task involved was also studied. Here, a division into four categories was utilised: maintenance, testing & calibration, modification & installation and operation. The distribution of the EoCs in **Oskarshamn** in these work types was the following: maintenance / repair (44%), testing / calibration / configuration control (18%), modification / installation

(18%) and operation (16%). For Olkiluoto the distribution was almost even, but most (9) cases had to do with operating activities. No exact information was given for Forsmark, but the other results point to the direction that the role of modifications and testing should not be underestimated as contributing factor to deviations in human performance.

4.3.2 Type of deviation in human performance

The results obtained for contributions of the two human deviation types EoCs and EoOs in different studies are shown in Table 3.

Table 3**.** Share of errors of commission (EoC) compared to errors of omission (EoO) in scrams, LERs and other events.

Report type	**Percentage of EoC cases (%)**		
	Olkiluoto*	**Forsmark***	**Oskarshamn**
Scrams	3 (43 %)	1 (100 %)	8 (60 %)
LERs+other reports*	17 (81 %)	12 (52 %)	74 (54 %)

* notice that especially for Olkiluoto and Forsmark some cases could not be classified - the percentage refers to the classified cases (EoO or EoC) only and the amounts may thus not be compared to Table 1. For Olkiluoto, 10 events not classified as LERs were calculated with.

As clearly seen, the amount of EoCs for all plants is more than 50 % of all the failure modes (all events calculated). Although there are some differences in the results, the main conclusion is that EoCs represent an important group of deviations in human performance. This results confirms the one obtained by Pyy (2000), and suggests that more emphasis should be put on studying other deviations in human performance than just omitted actions (EoOs).

One needs to note, nevertheless, that the consequences, such as system inoperability or disturbance, do not have to depend on the type of deviation (see Appendix 1). Therefore, one needs to be broad-minded when studying potential human actions, and to start the study from the potential consequences of them rather than from psychological error mechanisms.

The amount of deviations "confusion in alternatives" was about half for Forsmark and Olkiluoto (46 and 45 % correspondingly), whereas the percentage for Oskarshamn some smaller (21%). This type of deviation takes place especially in instrument- and electrical systems including cables and wires. The reason for this difference is difficult to interpret. One possible reason is slightly different understanding of the concept of "confusion among alternatives" in different studies.

Next, we studied which phase in human behaviour, i.e. identification, decision making or manual activity failed (see e.g. Figure App. 1-2). The results are shown in Table 4.

Table 4. Phase of human action that failed

Report type	Number of cases (percentage, %)		
	Olkiluoto	Forsmark**	Oskarshamn
Manual actions	4 (13 %)	14 (47 %)	49 (66 %)
Decision making	2 (6 %)	6 (20 %)	14 (19 %)
Identification (diagnosis)	12 (39 %)	4 (13 %)	*
Other (preparation, communication etc.)	2 (6 %)	-	8 (11 %)
Not known	11 (35 %)	6 (20 %)	--

* reported together with the above class "decision making" for EoCs only

** also one case based on interviews calculated with in the figures

The results are somewhat inconclusive, here, but one has to take into account that the percentages would approach each other given that only surely classified were counted. What is important is that for Forsmark and Olkiluoto, the plant documentation did not always allow this kind of study of human performance. The MTO related LERs are classified, however, in a more detailed way for Oskarshamn. For the two former plants the technical problems are normally very well described whereas human and organisational aspects are discussed very briefly. Since even JPB Consulting reported some problems to analyse events, this is an area where improvement is required. It may require a major change in the analysis paradigm to become man-machine system centered instead of technical problem centered.

4.3.3 Timing of the human failed actions and their detection

Looking at the time of the key action and the detection of exact fault mechanisms, some problems arose. This is mostly due to the fact that the LERs register the time point of a disturbance, or the detection of the beginning of a TechSpecs related limiting condition. From the plant risk level point of view, more relevant question are: a) when was the fault of a technical system born or b) when was the fault mechanism transferred to a technical system. the time points a and b may be different, as the material shows.

For instance in the Olkiluoto data, 25 % of cases led to operational consequences only after some time (as a minimum some hours and maximum several years) after the key action had taken place. Relatively many faults remained latent from an outage to the power operation mode, which confirms the earlier findings by Laakso et al. (1998).

Table 5 shows the consistent findings of the three different studies with regard to the key action timing (action that transferred the fault mechanism into a technical system). In some cases this classification was difficult due to deficient information. Consequently, the table includes some judgement.

Table 5. Operating mode at the time of the key action.

Report type	Number of cases (percentage, %)*		
	Olkiluoto	Forsmark	Oskarshamn*
power operation	17 (55 %)	19 (65 %)	43 (52 %)
outages incl. start-up	14 (45 %)	10 (35 %)	39 (48 %)

* EoCs only - for Olkiluoto and Forsmark, the distribution of the EoCs was about similar.

Thus, when compared to the short time in other than power operation related operating modes (outage, other shutdowns, start-up), events stemming from them are well represented. Thus, tests and check-ups after an outage are in an important role in ensuring safety against human action related events.

4.4 Causal factors involved

4.4.1 (Direct) causes

The direct causes were based on J.P. Bento's classification used widely for MTO-analyses in Sweden and in Finland (see Appendix 2).

For **Forsmark**, the most important cause categories were working practices (56 %), instructions (20 %), administrative routines (12 %), ergonomics (8 %) and communication (4 %). Problems with working practices often had to do with shortcomings in competence, training and safety culture. The top five cause categories for **Olkiluoto** were training and competence (35 %), working practice (35 %), work organisation & supervision (22 %), ergonomics (19 %) and communication (19 %). Notice that several cause categories may apply to one event, and the sum will thus be more than 100 %. Same categories dominate both in all events and in their EoC subcategory. Figure 2 presents the findings for Oskarshamn and also the share in four function classes: operation, maintenance, testing and modification discussed earlier under section 0.

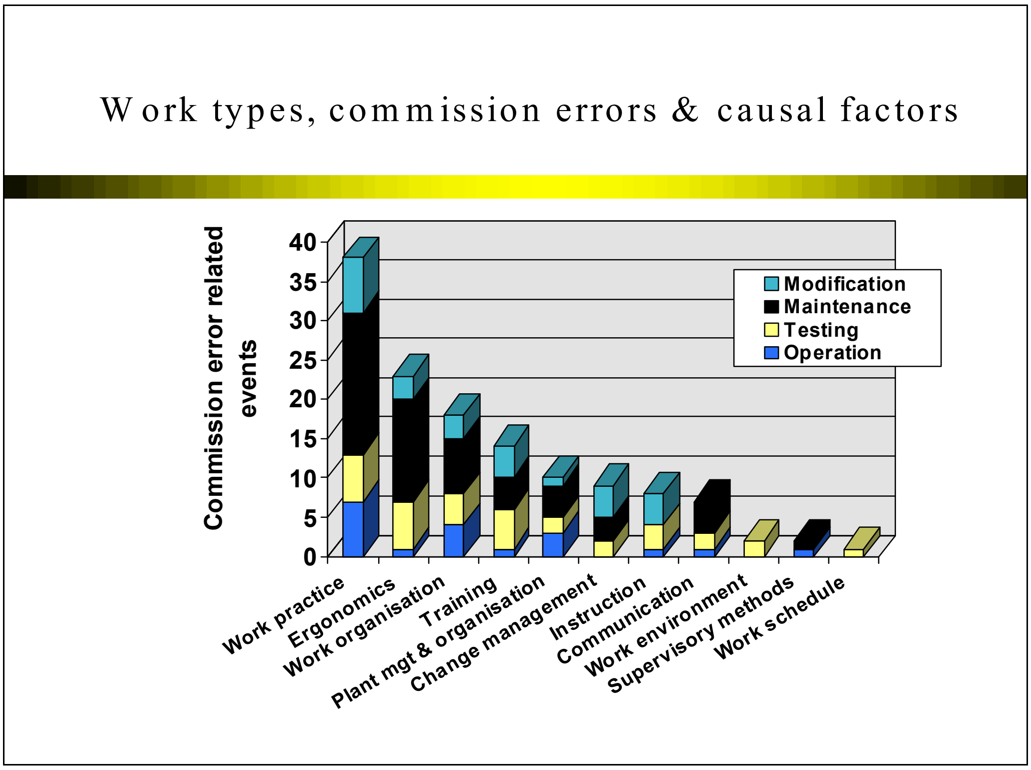


Figure 2. Cause categories for EoCs analysed for Oskarshamn.

As seen, the category “Deficient work practice” contributes to about half of the events, and many of such events were contributed by deficient self-checking. Other significant categories are “Deficient ergonomics/design” with the contribution of less than 30%, “Deficient work organisation” with slightly more than 20%, and finally “Deficient training/competence” with an average to about 17% of the EoC events. Thereafter, categories “Plant management & organisation”, “Change management”, “Instructions” and “Communication” follow.

Consequently, the results are quite similar in the three studies. Working practices, work organisation, competence & training play a very important role together with ergonomics and communication. This shows that safety culture has to be high at all levels of the organisation, behind the management desk as well as on the shop floor, in order to hinder significant events.

4.2.2 Broken organisational barriers

Deficiencies in organisational barriers before and after the key action were studied in all three studies. For **Oskarshamn**, all administrative and system functions were successful subsequent to the majority (about 80%) of the events. Deficient fault identification / repair / corrective action occurred only after about 6% of the events. In about 15% of the event reports, the identification of system / administrative deficiencies after those events was, however, some uncertain.

For Olkiluoto and Forsmark, we first discuss the **broken organisational barriers before a key action**. For **Forsmark**, design & planning was found to be somehow deficient in 31 % of the cases. Gaps in work order practices and restoration (operational safety) check-ups together had to do with 42 % of the cases. Tests or other check-ups were deficient in 18 % of events. For **Olkiluoto**, both a better safety check-up or a more accurate control could have helped to avoid problems in 18 cases (9+9=18), corresponding to 58 % of all MTO related significant events. It is important to notice that in many of those cases the people did not consider the situation to be risky, or there were faults in various documents guiding the activity (e.g. drawings). In 13 cases (42 %), it also was impossible to positively identify any organisational function that had failed, which is even much more than for Oskarshamn. This also shows that individual working practices and safety culture count in the results.

The situation was somewhat different for **failed organisational functions after the key action**. The results are quite consistent with those presented in the previous paragraph, since the share of cases with no clearly failed functions were identified was 84 % for **Forsmark** and about 50 % for **Olkiluoto**. The fact that many cases led to significant disturbances soon after a key action may give an explanation to this high amount. Also, one must remember that we aimed at choosing the key action as close to the process as possible (”front line action”).

The view about effective barriers was quite harmonious. For example, process control, design and independent check-ups were effective in 86 % for Forsmark and in 61 % of the cases for Olkiluoto. Still, they cannot be trusted blindly as the study shows.

4.5 Importance of the analysed events

4.5.1 Safety importance

PSA importance measures and the INES grade were used as indicators of safety significance. These two criteria are discussed separately in the following paragraphs.

Only 5 cases from **Olkiluoto** and one case from the **Forsmark** material were classified **INES** 1, whereas all the other either were classified 0 or "below scale". This result suggests that the material does not contain events very important from the safety point of view, although many of the cases with INES class 1 had revealed gaps in plant practices. Due to the low amount of events it is impossible to draw any further conclusions. INES classification was not assessed for **Oskarshamn** data.

Plant specific **PSA** models were used to verify safety significance. This was in some cases difficult, since for example some Swedish plants do not have a good enough quantitative PSA model for shutdown periods, and many events occurred in shutdown. Another difficulty was, in some cases, interpreting the consequences of human actions as events in the PSA model. Fortunately, very few events actually had active consequences other than causing an initiating event.

The amount of events that could be assessed by using a PSA model was 19 (out of 31 events) for Olkiluoto, 6 (out of 29) for Forsmark and 16 (out of 82 EoCs) for Oskarshamn. Thus, the coverage of Olkiluoto PSA including also the shutdown period is superior to other plants.

Risk achievement worth (RAW) measure and conditional core damage frequency (CCDF) were used as indicators of PSA significance. For **Forsmark**, the two most important events were: 1) a spurious disconnecting of the safety system room cooling on occasion of an auxiliary feedwater pump isolation (H-room, RAW < 1,65), and 2) a reduced PS-function of the containment in consequence of opening a valves for atmosphere change too early while shutting the plant down for the annual refuelling outage (RAW<1,6).

For **Olkiluoto**, three events led to considerable RAWs. Two of them led to an unavailability of a diesel generator: one due to using wrong lubricant for a centrifugal detector (RAW =1,36) and another one due to spurious fire extinguisher functioning (inaccurate human action) during a test (RAW =1,8). Furthermore, one case led to an unavailability of an auxiliary feedwater pump due to a slip in its test. The material also included a case, where lower equipment hatch was open during the maintenance of the main re-circulation pump during the annual refuelling outage. The RAW for that case is currently 1,02, but the analysis may need revisiting. Some events that could be interpreted as PSA initiating events and the four most significant of them led to loss of feedwater (CCDF=7,6 E-6). In addition, in one case the 400 kV grid, two 6 kV busbars and the residual heat removal system also became unavailable (CCDF=8,2 E-6). Two of the four cases happened in connection with tests and two other had to do with isolating or restoring equipment.

For **Oskarshamn** the most important events according to the PSA model were: 1) RO-O1-97/50 "Gas turbine generator not ready for start" (RAW =19 for transients), and 2) RO-O1-97/57 "Diesel generator DG112 not ready for start" (RAW =6 for transients). In both these events, poor ergonomics was a causal factor in relation to testing and calibration tasks.

The conclusion of the three studies is that most events are of a very low PSA importance. Different safety features in the different plants partly explain the high RAWs for Oskarshamn, i.e. all units in Forsmark & TVO are modern 4-redundant designs whereas Oskarhamn units 1 & 2 are 2-redundant. The finding is in line with previous ideas of that severe disturbances occur as a combined consequence of both human and technical causes. Many significant events had to do with front line safety systems and electrical equipment & busbars. Also testing played a role in many events, although it was difficult to identify other common traits in them.

4.5.2 Economic importance

The economic importance was only studied for Olkiluoto data, which does not allow any comparison. Man played a significant role in events leading to a 33 % loss in produced electrical output. Many events leading to considerable losses included actions outside the control room and were contributed by gaps in co-ordination and communication.

5 CONCLUSIONS AND RECOMMENDATIONS

Based on the analysis, human actions play a significant role in LERs. Despite this fact, human and organisational aspects are generally not analysed comprehensively unlike the technical issues. Related to this fact, human actions as causes and contributors to significant events may remain hidden in LERs. A follow-up analysis of deficient reports is very difficult and requires extensive interviews. Based on their salient role human actions deserve more attention in the analysis of operating experience.

Although the proportion of wrong human actions was high in the material, only few of them led to wrong system functions and disturbances (PSA initiating events) as their consequence. One should distinguish between the type of deviation in human actions and the consequences of the same actions when performing human reliability analysis. There is no generic law that would lead from an EoO to unavailability of equipment and from an EoC to a spurious system response. As noticed during this study, events often occur as a consequence of a combination of all kinds of human actions also including correct ones. This is the reason why the term “human error” should be used with extreme care.

Human reliability analyses have been concentrated upon omission (EoOs) of human actions prescribed in procedures. However, this study shows that significant events include at least as many wrong actions (EoCs). Due to the fact that events include many types of different human actions – correct and less correct - it is advisable to study consequences of all reasonable human actions and their contexts, rather than to restrict analysis to a specific subset like EoOs or EoCs only.

In this study, an extended concept of active human failures (AMF) was developed. AMF here means an event where individuals have affected technical systems in an unexpected way, which leads to other types of functional equipment consequences than unavailability of equipment only. Disturbances and spurious system actuations are examples of such consequences. The AMF concept is necessary in classifying deviations of human performance. This is because the concept “error of commission” is straightforward only if a deviation takes place in simple activities directly dealing with the process.

A significant amount of events were due to human actions outside the control room, which is another message to HRA. The control room is a focal point of operations and information exchange. Maintenance, testing and operating actions, however, take place all over an installation. Furthermore, many significant events had their roots in outages. This emphasises the need for even more profound safety control during and after a shutdown in preparation of a start-up.

Many important events were due to deficiencies in work practice. Also competence, training programme, work organisation and administration had to do with many events. It is important to maintain competence in a modern NPP subject to many types of both technical and organisational changes. Also improved communication, questioning attitude to the situation and simple self-control tools (e.g. STARC, Stop-Think-Act-Review-Communicate) would have possibly helped in many analysed events. These factors are safety culture related, which is a message for a more efficient safety management. Everybody’s attitude plays a role in safety work.

It was difficult to assess the risk significance of the faults / disturbances caused by human actions. Mostly, the analysed events did not play a significant role according to the PSAs. Only very few high Risk Achievement Factors (RAWs) due to the events were identified. Partly this was because of the shortcomings of the PSA models (e.g. no basic events exist for spurious system behaviour) and especially their HRA part. Also models for shutdown states were quite coarse except for Olkiluoto. However, one has to bear in mind that PSAs are intentionally based on simplified logical models.

No events aggravating the plant state during a disturbance (post IE) were identified in the material. To be able to make judgements about suitable ways to handle that kind of events in PSA, the modelling paradigm should be discussed as a whole and not only the HRA part. Simulator exercises may provide an analyst with data for such an effort, and their use is suggested for potential follow-up studies.

Development of approaches for the analysis of AMF and for integration of that analysis into PSA is a very demanding task. Another direction requiring, at least, equally great effort is the integration of the lessons learnt in the design process of new plants. In NKS/SOS-2, the priority was consequently put on scanning the problem area, and on forming a Nordic view on the subject. In our view no analysis or design principle should be based on humans acting only according to procedures, but on the goals and rational action alternatives that they are likely to have in real situations.

REFERENCES

Andersson, K., & Pyy, P., NKS/RAK-1 Subproject 3 - Integrated Sequence Analysis, Final Report, NKS/RAK-1(97)R11.

Barriere, M.T., Wrethall, J., Cooper, S.E., Bley, D.E., Luckas, Ramey-Smith, A.M. 1995. Multidisciplinary Framework for Human Reliability Analysis with an Application to errors of Commission and Dependencies. NUREG/CR-6265. U.S. Nuclear Regulatory Commission, August 1995.

Gertman, D. I., Blackman, H.S., Haney, L.J., Seidler, K.S., Hahn. H.A. 1992. INTENT: A method for estimating human error probabilities for decision based errors**.** Reliability Engineering and System Safety, 35 (1992) 127 -136

Hollnagell, E. 1999. Looking For errors Of Omission And Commission Or The Hunting Of The Snark Revisited. Manuscript submitted for publication in reliability Engineering and System Safety.

Hollnagell, E. & Marsden, P. 1996. Further Development of the Phenotype - Genotype Scheme for the Analysis of Human Erroneous Actions. EUR 16463 EN. 88 p.

Holmberg, J., Evéneus, P., Pyy, P. 2001. Analys av aktiva mänskliga fel (commission errors) – Instruktion för kategorisering av händelser / identifierade felmöjligheter. SwedPower report T-SEA 00/052. 5 p + App.

Julius, J., Jorgenson, E., Parry, G.W., Mosleh, A.M. 1995. A procedure for the analysis of errors of commission in a probabilistic safety assessment of a nuclear power plant at full power. Reliability Engineering and System Safety 50(1995) PP. 189-201.

Laakso, K.,Pyy, P., Reiman, L. 1998. Human errors related to maintenance and modifications. STUK-YTO-TR 139. 42 p. January 1998.

Macwan, A. & Mosleh, A. 1994. A Methodology for Modelling Operator errors of Commission in Probabilistic Risk Assessment, Reliability. Engineering and Systems Safety, 45 (1994) 139 -157

Parry, G.W. 1995. Suggestions for an improved HRA method for use in Probabilistic Safety Assessment. Reliability Engineering & System Safety Volume 49, Issue 1. pp 1-12.

Pyy, P. 2000. Human reliability analysis methods for probabilistic safety assessment. VTT Publications 422, Espoo 2000. 63 p. + app.64 p.

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

Vuorio, U., Vaurio, J.K. 1987. Advanced human reliability analysis methodology and applications. Proc. PSA'87, Zurich, Aug.30 – Sept 4, 1987. Verlag TUV Rheinland, Köln 1987.

Williams, J. 1998. Identification of errors of Commission in UK nuclear utilities and formal methods. HSE, Nuclear Safety Directorate. March 1998. 18 p.

APPENDIX 1

Different definitions of error of commission (EoC)

There are many different definitions for commission errors in literature. The original definition comes from A. D. Swain & Guttmann (1983), who define the error of commission as a kind of wrong human output i.e. selection error, error of sequence, time error (too early, too late) or qualitative error (too little, too much). This is often called the phenotype of error (e.g. Hollnagel & Marsden, 1996). For comparison, errors of omission mean omitting an entire task or steps in a task. Macwan & Mosleh (1994) refine Swain's classification and define error of commission as an action not prescribed in the procedures (not required). In their classification, delayed actions are shown as a separate class. This may be proper since, in many cases, the delayed and omitted actions may have similar consequences.

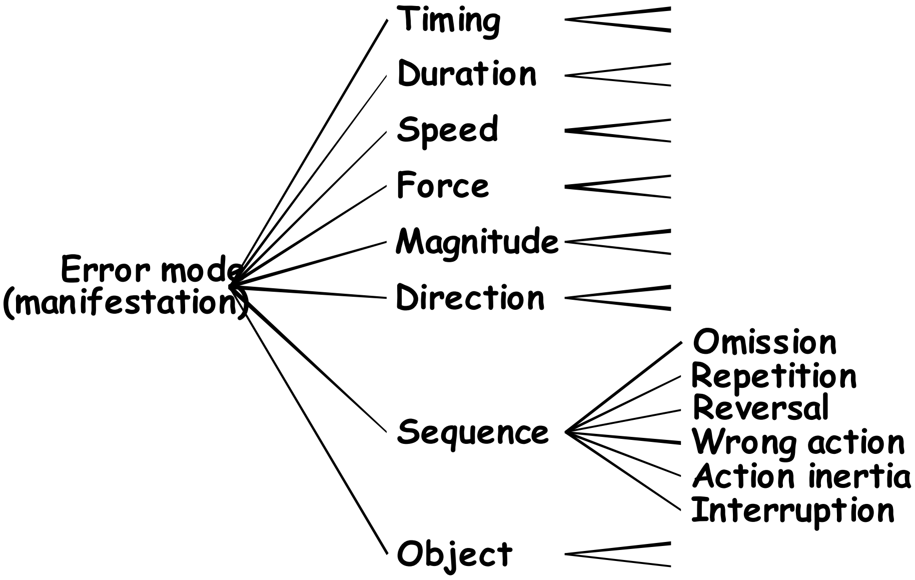
Parry (1995) expands the domain of commission error to premature actions and separates them from alternate actions (for which there are many possibilities). Both Macwan & Mosleh (1994) Gertman et al. (1992) distinguish between intentional and unintentional commission errors. The former are more related to the upper cognitive activities such as diagnosis and decision making, whereas the latter are more related to task execution.

Julius et al. (1995) draw attention to the fact that many commission errors both make unavailable one safety function and exacerbate the situation by failing other safety functions. Global and local misdiagnosis represent intentional commission error types whereas slip is an unintentional commission error on the action level. Global misdiagnosis means a total wrong identification of the situation with consequent procedural, whereas a local misdiagnosis refers to unsuited decision in the action programme.

ATHEANA classification (Barriere et al. 1995) makes a link to PSA by stating that an error of commission (EOC) is 'an overt, unsafe action that, when taken, leads to the change in plant configuration with the consequence of a degraded plant state'. Thus, not all human deviations in actions are seen as interesting but only those that lead to degraded plant conditions.

Williams (1998) divides errors of commission into two psychological subclasses. The first is compiled of 'errors of recognition, diagnosis or intention that leads to a series of acts formed with well-meaning intentions, but which are inappropriate for the technical scenario that pertains. The second is 'an isolated error introduced within an otherwise appropriate series of actions that may arise from a random aberration in behaviour or may be introduced by the inappropriate application of an habitual task behaviour'.

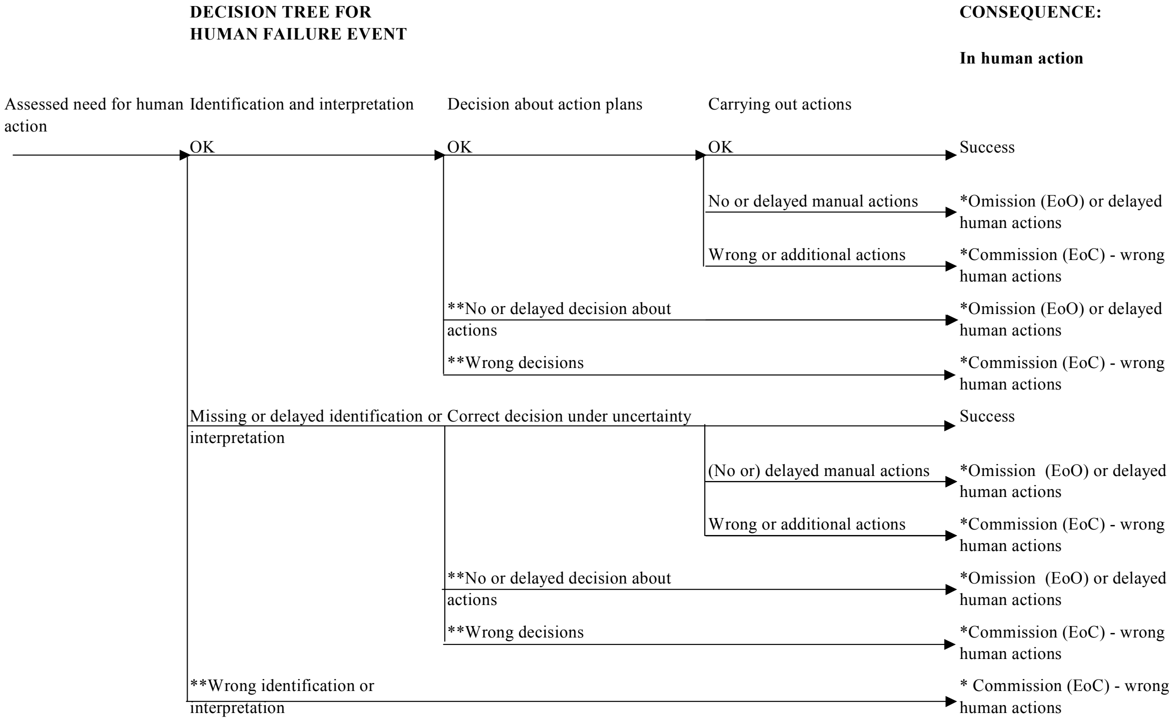
Hollnagel (1999) criticises the omission and commission error dualism due to the fact that it does not make a distinction between causes (genotypes) and manifestations (phenotypes). Rather, eight basic error modes should be used as manifested in the following picture App. 1-1. The error modes correspond to the limited number of ways in which something can be done incorrectly. Hollnagel also points out that the classes "omission" and "commission" are not mutually exclusive but lead to quite arbitrary situations. For example, there are two acts **I** and **II** that should be carried out in a sequence. If the task is performed so that **I** is delayed and then carried out in the place of **II**, both omission and commission errors can be regarded to have taken place.



Picture App. 1-1. Basic error modes according to Hollnagel (1999).

One may add the consequence point of view to Hollnagel's criticism. In PSA, what makes the spurious human actions interesting is their potential effect on systems. Thus, we are interested in the ways the systems function may become disturbed rather than in human errors per se. Risky events have to be studied with all the cause combinations leading to them rather than to stick into one or two potential causes. Thus, also some strictly speaking correct human actions in unfavourable context (triggering events) may result in system consequence. This property makes it sometimes utmost difficult to classify an event by using only one word (omission or commission). Rather, the whole causal and temporal network should be made visible to give a sufficient explanation to an event where human actions play a role. Building such a model would make it visible where e.g. the human beings had chances to recover the situation.

Moreover, the effect of HFEs on the process or equipment cannot normally be judged based on the human failure type (EoO or EoC) only. Even normal human actions can sometimes trigger unwanted consequences if other latent failures are present in the man machine system. Examples of such situations are errors in procedures that lead to a human failure although the operators follow the procedures correctly; and faulty calibration instruments that lead to multiple wrongly calibrated measurements (Pyy, 2000).


DECISION TREE FOR
HUMAN FAILURE EVENT
CONSEQUENCE:
In human action
Assessed need for human action
Identification and interpretation
Decision about action plans
Carrying out actions
OK
OK
OK
Success
No or delayed manual actions
*Omission (EoO) or delayed human actions
Wrong or additional actions
*Commission (EoC) - wrong human actions
**No or delayed decision about actions
*Omission (EoO) or delayed human actions
**Wrong decisions
*Commission (EoC) - wrong human actions
Missing or delayed identification or interpretation
Correct decision under uncertainty
Success
(No or) delayed manual actions
*Omission (EoO) or delayed human actions
Wrong or additional actions
*Commission (EoC) - wrong human actions
**No or delayed decision about actions
*Omission (EoO) or delayed human actions
**Wrong decisions
*Commission (EoC) - wrong human actions
**Wrong identification or interpretation
* Commission (EoC) - wrong human actions

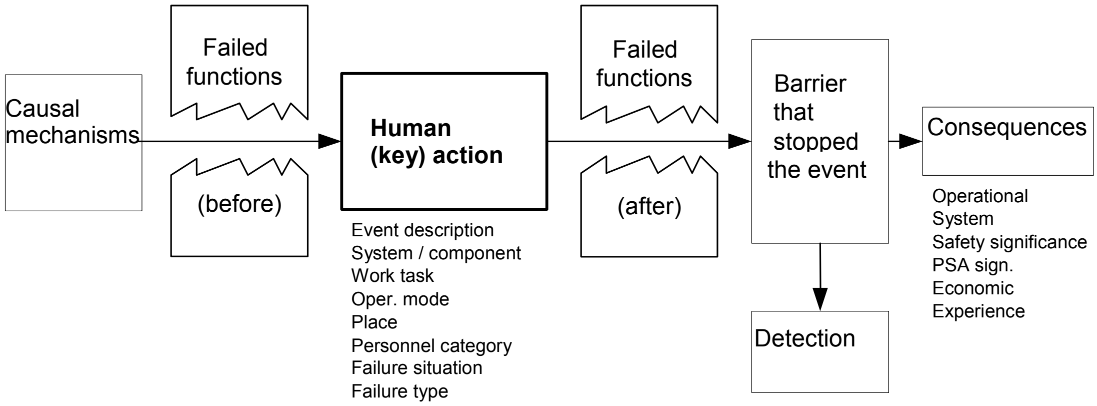
* In all cases, identification or decisions may be corrected given that the target system and time allow (recovery)

** No double failures included, e.g. no wrong identification and additional delayed manual actions

Figure App. 1-2. Decision tree for classifying human failure events. Unsuccessful recovery is implicitly included in the classes.

APPENDIX 2

Information used in the NKS/SOS-2 AMF classification



The following information and classes were used for the categories manifested in

Figure 1 in text (in Section 0). Some of them may have changed slightly from those presented in (Holmberg et al 2001) due to the needs observed during the analysis work.

Table Appendix-2-1. Explanation of the coding

Description	Explanation	Used classes	Comments
Plant unit	Administrative information	1, 2	
Date	Administrative information	None	Preferably both the time of the key human actions and the timing of the consequences (and their detection)
Event description	Event description by using one or two sentences	None	The role of the key action should become clear wrgt the sequence of events
System, component	System and its component type + number for identification	Plant systems and components	later on, this information was used for classification purposes, too
Work task	The characteristics of the work task related to which the key action took place. Operating mode:	Refuelling Cold shutdown Warm shutdown Nuclear warming Hot stand-by Power operation	Includes three kinds of information: the operating mode, the location of the task and the type of personnel that carried out the task
	Location:	Control room (incl. relay rooms) In field (normal environment) In field (controlled area) Workshop, storage Outside	See above
	Personnel category	Operator Field operator Mechanical maintenance Instrument maintenance Electrical maintenance Chemistry / Core group Fire, Data, Rad. protection Cleaning, Security Subcontractor	See above

Description	Explanation	Used classes	Comments
Failure situation	The phase of human information processing which failed	Identification, diagnosis Decision making Manual action Normal action, no failure Cannot be defined	If may be extracted based on the written material and/or interviews
Failure type	The type of deviation in the output of human actions	Omission (EoO) Confusion (EoC) Wrong action (EoC) Cannot be defined	If may be extracted based on the written material and/or interviews
Causes including root causes	The causes that led to the case (influencing the key action and the potential weakened barrier strength)	Working environment Work organisation, administrative routine Modification work routine Management/organisation Ergonomics / deficiencies in technique Work time factor Communication Instruction / documentation Work supervision Training / competence Working practice / individual reason	Based on the classification often in Sweden for incident analyses
Detection	The mechanism / function that led to the detection of the event (sequence)	Operational consequence (immediate) Operational consequence (delayed) Alarm, process control Abnormal indication Test, inspection Through another scheduled activity Basic state restoration control Control of panels Other type of control Walk-around-check Random	A user begins checking the conditions from the first one to the last
Failing functions (before)	The failed organisational functions in time/sequence before the key action which could have prevented the key action from transmitting a failure mechanism to the technical system	(Plant) Design Process control Testing, inspection Operability verification Other type of independent control Work permit handling Safety check-up Safety analysis	There may be other types of barriers, too, but here we concentrate upon the organisational functions dealing with safety
Failing functions (after)	The failed organisational functions in time/sequence after that could have prevented from / mitigated the consequences of the key action	(Plant) Design Process control Testing, inspection Operability verification Other type of independent control Work permit handling Safety check-up Safety analysis	There may be other types of barriers, too, but here we concentrate upon the organisational functions dealing with safety
Operational consequence	The consequences to the plant operating conditions	Hydraulic scram Other reactor trip (e.g. V) Turbine trip Lowered electrical output Shutdown (of MCPs etc.) Isolation sequence House turbine operation Increased testing Other operational consequence Other	Many of these conditions lead to, at least, economic consequences, too.
System consequence	The consequences to the target system of the key action (or sequence)	Total loss (of system function) Reduced system operability Seriously degraded redundancy	Cases with very small effect on the target system / plant were normally screened from the material during the

		Some degraded redundancy Spurious function CCF/CCI None	study
Safety significance	Non PSA-related safety significance (deterministic)	Highest allowed safety variable value exceeded Technical specifications LER written (type) INES class (number) Other None	Note that LERs and INEs reports have different classes
PSA significance	The importance of the event based on the PSA model	None Initiating event Basic event Event tree sequence Conditional risk influence Risk achievement worth (RAW)	In reality, only the conditional core damage frequency was calculated for those events corresponding the initiating events (IEs) in a PSA model and the RAW for the basic events
Economical consequence	The lost production in MWh	None (realised amount)	In some cases required further investigation
The function that stopped the evolution of the event	The function that finally put an end to the progression of the event	(Plant) Design Process control Testing, inspection Operability verification Other type of independent control Work permit handling Safety check-up Safety analysis	In many cases the plant design functioned e.g. in the form of a scram (completed later on by process control activities)
experience obtained, actions taken (MTO related)	Here, the emphasis was put to organisational activities focusing upon improving the reliability of human actions in future	Questioning attitude Training / Understanding safety / operating questions Documentation / instructions / Tagging Change of the working praxis Control of spare parts Control of performed installation Self control (stop-think-act-reflect-communicate) None	The classification was based on the Swedish example
References	The existing plant documents about the event	None	typically LERs etc.

Table Appendix 2-2: An example of the record in the AMF event database (the complete MS Excel table also included add-on comments and complementary LER-information)

Unit	Date	Event description	System, component	Work task (information)
OL1	27.5.1997	Reactor scram SS11(and SS5) just before the annual refuelling outage – a field operator got a mission to isolate TIP-actuators electrically but he erroneously isolated the switches of the whole electric cubicle	665D401-F2, 665B201-F2, 655A101-F2	Power operation, In field, Field operator

Failure situation	Failure type	Causes including root causes	Detection	Failing functions (before)	Failing functions (after)
(related to) Identification and diagnosis	Confusion	Ergonomics, working practice, communication, training / competence	Operational consequence (immediate)	None	Other type of independent control

Operational consequence	System consequence	Safety significance	PSA significance (conditioned cdf)	Economical consequence [MWh]
Hydraulic scram	Total loss of electricity supply, CCI	INES level 1	7,61E-06	3100

The function that stopped the evolution of the event	Experience obtained, actions taken (MTO related)	References
Design	Training, questioning attitude(communication), self control (STARC)	1-KK-R6-2/97, 0-TR-M-24/99 (reference 1)

Bibliographic Data Sheet NKS-74

Title	An analysis of errors of commission in the Nordic nuclear power plants based on plant operating experience
Author(s)	Pekka Pyy[1], Jean-Pierre Bento[2], Yngve Flodin[3]
Affiliation(s)	[1]VTT Automation, Finland, [2]JPB Consulting, Sweden [3]SwedPower, Sweden
ISBN	87-7893-130-4
Date	December 2001
Project	NKS/SOS-2.1
No. of pages	20 + 7 (app.)
No. of tables	5 + 2 (app.)
No. of illustrations	2 + 3 (app.)
No. of references	14

Abstract

The report presents the methodology followed, the material used and conclusions drawn in a study of active human failures. First, the report discusses the concept of active human failures in the context of human errors. Then, a simplified methodology is presented applicable to analysis of operating experience and documenting all kinds of human failures. Also the material and analysis procedure used in the three parts of the study are discussed. Finally, some selected highlights of the results are presented with common conclusions and recommendations.

Key words Human reliability, Operating experience, LERs, HRA, Errors of Commission

Available on request from the NKS Secretariat, P.O.Box 30, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@catscience.dk, www.nks.org.