SKI Report 98:11

UNDETECTED LATENT FAILURES OF SAFETY-RELATED SYSTEMS

Preliminary Survey of Events in Nuclear Power Plants 1980-1997

OUPPTÄCKTA LATENTA FEL I SÄKERHETSSYSTEM

Bengt Lydell

March 1998

ISSN 1104-1374
ISRN SKI-R-98/11--SE

SKI Report 98:11

UNDETECTED LATENT FAILURES OF SAFETY-RELATED SYSTEMS

Preliminary Survey of Events in Nuclear Power Plants 1980-1997

OUPPTÄCKTA LATENTA FEL I SÄKERHETSSYSTEM

Bengt Lydell [1]

[1] **RSA Technologies,**
1736 Promenade Circle, Vista, CA 92083-6172, USA

March 1998

SKI Project number 97257

This report concerns a study which has been conducted for the Swedish Nuclear Power Inspectorate (SKI). The conclusions and viewpoints presented in the report are thos of the authors and do not necessarily coincide with those of the SKI.

SKI/RA-009/98
RSA-R-98-02
Rev. 0
SKI Ref. No.: 14.2-980179

UNDETECTED LATENT FAILURES OF SAFETY-RELATED SYSTEMS

Preliminary Survey of Events in Nuclear Power Plants 1980-1997

Prepared for

Swedish Nuclear Power Inspectorate
Department of Plant Safety Assessment
SE-106 58 Stockholm, Sweden

REMARK

IN THIS COPY OF THE REPORT, THE PLANT IDENTIFICATIONS ARE REMOVED IN THOSE CASES WHEN THE SOURCE OF DATA IS AN INDIVIDUAL IRS-REPORT. *THE SOURCE DOCUMENT - SKI/RA-009/98*, WILL BE UPDATED IN NEAR FUTURE WITH MORE INFORMATION.

NOTICE

This report on latent errors includes restricted information on plant events. Except for U.S. LERs (public domain information available from the NRC Public Document Room) and Swedish 'Reportable Occurrences' (ROs), the information in Table 2-2 (pp 8-15) is restricted. This report must not to be distributed to third party without written permission from the Swedish Nuclear Power Inspectorate.

ATT OBSERVERA

I bifogad rapport refereras till ett relativt stort antal IRS rapporter, som är klassade av OECD/NEA och IAEA som ”restricted”. Detta innebär att användning av rapporten utanför SKIs och de svenska kärnkraftverkens domäner inte får ske om inte anläggningsnamnen avidentifieras från de tabeller dessa förekommer i. Ni som vill sprida rapporten till sådana externa användare bör därför maska bort uppgifterna om dessa identiteter. IRS rapportnummer skall i sådana fall användas som händelseidentitet.

SUMMARY

This report summarizes results and insights from a *preliminary* survey of events involving undetected, latent failures of safety-related systems. The survey was limited to events where mispositioned equipment (e.g., valves, switches) remained undetected, thus rendering standby equipment or systems unavailable for short or long time periods. Typically, these events were symptoms of underlying latent errors (e.g., design errors, procedure errors, unanalyzed safety conditions) and programmatic errors.

The preliminary survey identified well over 300 events. Of these, 95 events are documented in this report. Events involving mispositioned equipment are commonplace. Most events are discovered soon after occurrence, however. But as evidenced by the survey results, some events remained undetected beyond several shift changes. The recommendations developed by the survey emphasize the importance of applying modern root cause analysis techniques to the event analysis to ensure that the causes and implications of occurred events are fully understood.

Key words: Latent failures; detection; safety-systems; human factors/organizational factors; human reliability analysis (HRA); probabilistic safety assessment (PSA); error trends; plant operating experience.

SUMMERING

I rapporten redovisas en undersökning som SKI/RA initierat av händelser med anknytning på oupptäckta latenta fel i säkerhetsrelaterade system. I rapporten sammanställs intressanta amerikanska händelser, som inträffat under tiden 1980-1997. Urvalet som plockats fram är begränsat till händelser som berör felaktigt baslagda komponenter (ex. ventiler, pumpar, brytare) och som förblivit oupptäckta och därmed också förorsakta otillgänglighet på standby utrsutning och säkerhetssystem en kortare eller längre tid. Det typiska i dessa händelser är de underliggande symptomen för latenta fel (designfel & -svagheter, procedurfel, ej utförligt analyserade säkerhetsrisker).

I den preliminära undersökningen identifierades ca 300 amerikanska händelser. Utav dessa , har vi valt att presentera 95 st. Händelser som berör felaktig basläggning är relativt frekventa händelser. I de allra flesta fallen upptäcks basläggningsfelen inom en relativt kort tid efter att dessa initierats. I sammanställningen framgår det dock att så inte behöver vara fallet alla gånger. Otillgängligheten har varit så lång som 8760 timmar eller mer i ett antal fall. Vid noggrann läsning av de inträffade händelserna ser man också att flera av dessa händelser är solklara beroendefel av typen CCF.

I rekommendationerna poängteras viktigheten av att tillämpa modern och effektiv rotfelsanalys teknik som ett komplement till händelseanalyserna för att försäkra sig om att orsaker och influenser av inträffade fel är fullt ut omhändertagna.

TABLE OF CONTENTS

1

INTRODUCTION

This report documents the results of a preliminary survey of nuclear power plant events involving undetected, latent errors of engineered safeguards systems. Prompted by recent events[1] in Swedish nuclear power plants, the survey concentrates on events where safety systems were rendered inoperable due to the mispositioning of equipment. Trends and patterns in occurred events involving latent errors are developed from reviews of mainly Swedish and U.S. selected operational experience during 1980-1997.

1.1 Issue Summary & Work Scope Definition

As formulated in Rasmussen (1984), Reason (1990), and Embrey, Kontogiannis and Green (1994), adverse consequences of latent (or hidden) errors are revealed when they combine with other factors to breach a system's safety barrier(s). The different categories of latent error are identified in Figure 1-1 and Table 1-1, and discussed below.

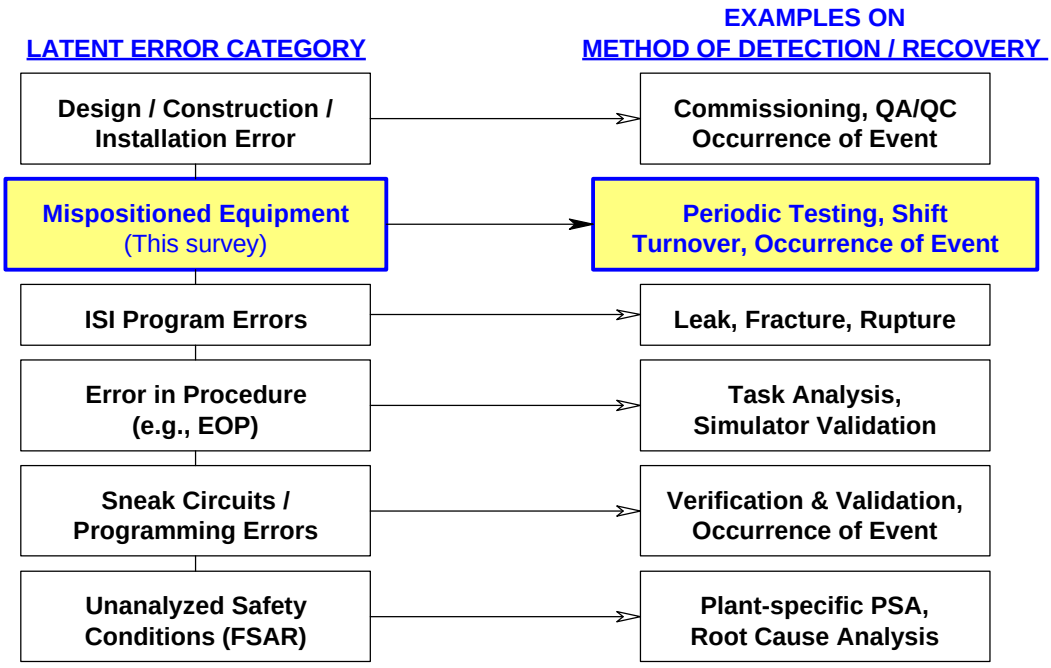

Figure 1-1: *Some Examples of Different Types of Latent Error*.

[1] For example, Oskarshamn-2 on November 13, 1996 and Ringhals-4 on September 28, 1997; *c.f.* Table 2-1 in Section 2 of this report.

Table 1-1: *Latent Errors and Their Detection.*

Latent Error Category	Method(s) of Detection (Examples)
Design / construction / installation error	Fortuitously as a result of plant transients; QA/QC; commissioning of newly constructed plant; PSA
Mispositioned equipment	Alarm/indication in control room; fortuitously as a result of plant transient (restoration per EOP-guidance); system walk-downs; shift turnover.
ISI program errors	Fortuitously as a result of leak/rupture; ISI program reevaluation based on feedback of service experience.
Error in Procedure	Simulator training; walk-through/talk-through; job performance measures; fortuitously as a result of plant transient with safety system actuation and implementation of EOP.
Programming errors	Verification & validation; fortuitously as a result of unexpected/unusual/off-normal system response.
Unanalyzed safety conditions	Fortuitously as a result of plant transient; PSA; root cause analysis.

(a) **Design/construction/installation error**. An early study by Risø National Laboratory concluded that "… design and other human errors are responsible for a significant number of failures and abnormal occurrences …" (Taylor, 1974). One would expect that the role of design errors diminishes as the plants grow older, and a common notion has been that the errors are revealed and corrected during the commissioning of newly constructed plants. Actual experience shows that design errors remain important during mature plant life; *c.f.* (NRC, 1994a). One reason could be the inadequacy of traditional reliability analysis and root cause analysis methods in revealing and accounting for design/construction/installation errors. Therefore, independent event and safety analysis approaches tend to be quite effective in unraveling previously unidentified design deficiencies. Mostly, these types of latent errors are identified fortuitously as a result of plant transients (NEA, 1996), however.

(b) **Mispositioned equipment** (the topic of this report). Latent errors due to mispositioning of equipment could occur upon completion of test & maintenance activities. The combination of failure to restore valve and/or switch positions *and* failure to reveal the cause of the unavailability of standby equipment at the time it occurs results in a latent error condition. Summaries of recent U.S. operating experience is found in Kauffman (1995) and Pullani and Brown (1997). Typically, this type of latent error is a problem in connection with annual refueling outages. During the outages the role of the operations staffs changes considerably compared with full power operation. The operating circumstances during outages are more demanding, the work more intensive, and shift turnovers more difficult (Barriere et al, 1994). Mostly, these types of latent errors are identified fortuitously as a result of routine system walk-downs or special inspections.

(c) **ISI program errors**. Numerous piping failures (cracks/fractures, leaks, ruptures) have occurred due to omissions or inadequacies in inservice inspection (ISI) programs. That is, without these omissions or inadequacies, the effects of degradation mechanisms could have been controlled/arrested. As an example, the rupture at Sequoyah-2 in 1993 of a DN250 steam extraction pipe (NRC, 1993a) was the result of an ineffective erosion/corrosion control program. Similarly, the significant steam generator tube degradations reported at Main Yankee in 1994 were attributed to inadequate eddy current test procedures (NRC, 1994b).

(d) **Error in procedure**. Errors or omissions in modern symptom-based emergency operating procedures (EOPs) could lead to the implementation of less-than optimal recovery strategies. Using current HRA terminology, latent errors due to procedural weaknesses could lead to error forcing contexts (EFCs). The steam generator tube rupture event at Palo Verde-2 in March 1993 revealed a weakness in the EOPs (NRC, 1993b). After the reactor trip, the operators used the EOP diagnostic logic tree to diagnose and mitigate the event. However, the operators twice failed to diagnose the tube rupture because the radiation monitors that would have led to that diagnosis were not in alarm status when the applicable step in the logic tree was reached. As a result, the logic tree directed the operators to use the procedure for a reactor trip without complications to begin recovery actions. The operators could not enter that procedure because the pressurizer level was below 10%. Therefore, the control room supervisor directed the operators to begin the functional recovery procedure. The operators isolated the ruptured steam generator 2 hours and 53 minutes after the rupture had occurred. Additional examples on EOP deficiencies are included in (Kauffman, 1995).

(e) **Programming errors**. Analog instrumentation and control (I&C) systems are being replaced with digital I&C systems. These new systems come with increased vulnerabilities to software failures and certain types of hardware failures. In a review by NRC (1994c) of digital system failures from 1990 through 1993, poor software verification and validation, and poor plant procedures were listed among the root causes of these failures. While most of these failures did not cause a significant safety event, they could potentially cause common cause failure.

(f) **Unanalyzed Safety Conditions**. Related to the 'design error' category are the unanalyzed safety conditions. That is, safety conditions not considered in the original safety analyses that were part of the licensing requirements. A limited computer search[2] using the Sequence Coding and Search System (SCSS) for U.S. LERs during 1994-1996 yielded about 200 reports on unanalyzed safety conditions and procedural deficiencies that were revealed through independent safety evaluations (e.g., IPE/PSA) and root cause analyses of occurred events. Examples of unanalyzed safety conditions include safety systems not meeting functional requirements during certain accident conditions, technical specification limiting conditions for operation (LCO) that are inconsistent with safety analysis results, single failure mechanisms that could affect safety functions, etc.

[2] Copies (as electronic file or paper copy) of the computer search results are available on request.

A long standing argument against using PSA in safety-related decision making has been the perceived difficulty to account for latent errors in the analyses. A basic premise of the debates on PSA limitations has been the notion that latent errors are commonplace *and* difficult to predict. As expressed in a report by the Committee for Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency (Calvo et al, 1995, p 18), limitations of PSA include the following:

(a) Difficulty in ensuring completeness of sequence identification;
(b) Construction errors may not be represented;
(c) Management and safety culture issues are not represented;
(d) Quality of data (e.g., plant reliability);
(e) Engineering judgments are difficult to quantify;
(f) Human errors, particularly cognitive errors, are difficult to quantify;
(g) Common mode/cause failures are difficult to quantify.

Latent errors are known to play a role in issues (b), (c), (f) and (g). How important are these types of errors and to what extent are they accounted for by the PSA studies? Numerous surveys on operational events involving latent errors have been published in the past 25 years. The subject survey of latent errors due to mispositioned equipment included accessing materials from the U.S. NRC's Public Document Room via the Bibliographical Retrieval System (BRS). Human reliability analysis (HRA) and probabilistic safety assessment (PSA) perspectives on latent errors are addressed by this preliminary survey.

1.2 Outline of the Report

This report makes extensive use of previous summaries of operating experience involving latent errors. Especially U.S. NRC Generic Letters, Information Notices and Engineering Evaluations. Section 2 includes summaries of events in primarily Swedish and U.S. plants, and a presentation of trends and patterns. Section 3 includes a summary and recommendations for the systematic evaluations of latent errors by SKI.

1.3 References

Barriere, M. et al, 1994. *An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues*, NUREG/CR6093, U.S. Nuclear Regulatory Commission, Washington (DC).
Calvo, J. et al, 1995. *Regulatory Approaches to PSA. Report on the Survey of National Practices*, NEQ/CNRA/R(95)2, OECD Nuclear Energy Agency, Issy-les-Moulineaux (France).

Embrey, D., T. Kontogiannis and M. Green (1994). *Guidelines for Preventing Human Error in Process Safety*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York (NY), ISBN 0-8169-0461-8.

Operational Safety of Nuclear Power Plants, Vol. 1, International Atomic Energy Agency, Vienna (Austria).

Reason, J. (1990). *Human Error*, Cambridge University Press, Cambridge (UK), ISBN 0-521-31419-4.

Taylor, J.R., 1974. *Design Errors in Nuclear Power Plant*, Risø-M-1742, Research Establishment

2

REVIEW OF SELECTED EVENTS

With focus on latent error involving the mispositioning of equipment[3], this section summarizes insights from the review of selected events extracted from Swedish RO-reports, U.S. NRC Information Notices, U.S. NRC Licensee Event Reports (LERs), U.S. NRC reports on 'Systematic Assessment of Licensee Performance (SALP), and IRS reports[4].

2.1 Apparent Causes & Root Causes

The events selected for review are summarized in Table 2-2 and Table 2-3. This summary resulted from a limited review of selected operational events. All of these events involved multiple personnel errors in following procedures, inadequate procedures, and inadequate post maintenance and surveillance activities. The anatomy[5] of the events that occurred 10 or more years ago remains applicable to the recent events. This observation points to inadequacies of root cause analyses practices, and lack of feedback of operating experience. It also points to the complexity of unraveling the root causes of latent errors. Typically, the detection of unavailable standby systems was the fortuitous result of some control room or ex-control room activity soon after occurrence rather than a deficiency that was revealed via a planned or scheduled action; *c.f.* Figure 2-1.

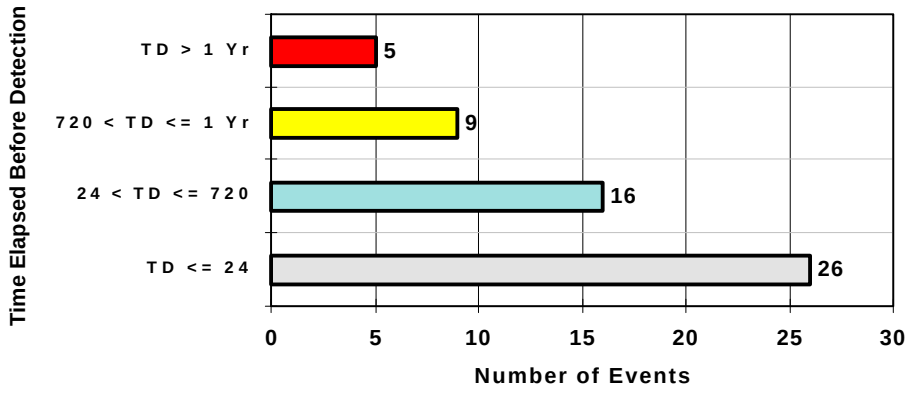

Figure 2-1: *Time to Detection of Latent Errors Summarized in Tables 2-2 & 2-3.*

[3] The Swedish term is 'basläggningsfel'.
[4] The IRS reports were made available by the Swedish Nuclear Power Inspectorate, Department RA (Plant Safety Assessment).
[5] In modern incident theory the term 'anatomy' refers to the systems-oriented models used in under-standing incident/event causation.

The mispositioning of equipment, and the consequential unavailability of standby equipment and systems, is the manifestation of some underlying cause(s); i.e., the root cause. Often, the mispositioning of equipment is the result of some other latent error in combination with programmatic or organizational deficiencies as shown in Figure 2-2.

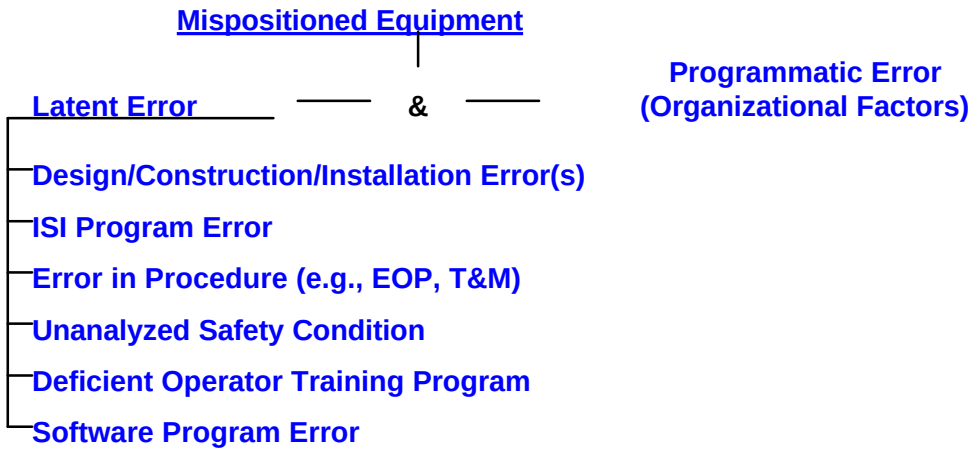

Figure 2-2: *An Example of Some Contributing Causes of Mispositioned Equipment*.

Recovery from all instances of mispositioned equipment included in this evaluation occurred without any serious safety consequences. It is likely that if equipment or systems had remained unavailable, the recovery guidance in the symptom-oriented emergency operating procedures (EOPs) would have prompted operators to attempt to restore the safety functions. Nevertheless, the events summarized in Table 2-2 and Table 2-3 are precursors to more severe events. Some perspectives on the potential implications of latent errors in general are provided by the U.S. NRC Information Notices that have been issued in response to occurred events; *c.f.* Table 2-1.

Table 2-1: *A Selection of U.S. NRC Information Notices on Latent Error.*

Information Notice	Title
IN 85-75 (August 30, 1985)	Improperly Installed Instrumentation, Inadequate Quality Control and Inadequate Postmodification Testing.
IN 87-01 (January 6, 1987)	RHR Valve Misalignment Causes Degradation of ECCS in PWRs.
IN 93-21 (March 25, 1993)	Summary of NRC Staff Observations Compiled During Engineering Audits or Inspections of Licensee Erosion/Corrosion Programs.
IN 93-56 (July 22, 1993)	Weakness in Emergency Operating Procedures Found as Result of Steam Generator Tube Rupture.
IN 94-20 (March 17, 1994)	Common Cause Failures Due to Inadequate Design Control and Dedication.
IN 94-88 (December 23, 1994)	Inservice Inspection Deficiencies Result in Severely Degraded Steam Generator Tubes.
IN97-78 (October 23, 1997)	Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times.

In next section tables 2-2 and 2-3 are presented.

Table 2-2 - *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (1-of-8).*

Table 2-3 - *Selected U.S. LERs on Mispositioned Equipment - Full Text LERs Not Yet Retrieved (1-of-4).*

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (1-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
3/23/81	XXX	ECCS	336		x	Deficient valve identification and valve line-up procedure	IRS 0058.00
6/6/81	XXX	ECCS	≥ 8		x	Possible sabotage; normally key-locked open valve found closed rendering all 3 train of HHIS unavailable. Possible deficient plant security procedure.	IRS 0147.00
3/2/82	XXX	Containment Spray + Charging pump	≥ 4	x		A containment spray pump and a charging pump, respectively, were left in 'pull-to-lock' upon completion of test. Cognitive error by operators.	IRS 0292.00
8/18/82	XXX	ECCS	44		x	Due to procedural deficiency, both ECCS trains were blocked while entering hot shutdown.	IRS 0328.G1
8/24/82	XXX	RHRS	5	x		A testing error in connection with plant startup rendered 1 train of the low-head SI unavailable. Caused by cognitive operator error.	IRS 0292.00
10/28/82	XXX	Containment Spray	ca. 8700		x	Procedural deficiency rendered both CS-trains unavailable since spray header isolation valves had been locked closed since before the plant achieved initial criticality. Also, the valve stems were not in accordance with design drawings leading to false position indications.	IRS 0287.00
12/6/82	XXX	ECCS	22.5		x	EOP deficiency; plant had been shutdown due to inadvertent SI. Both trains were blocked per EOP but not reset upon entering hot standby.	IRS 0328.G2

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (2-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
4/19/83	XXX	AFWS	120		x	Shared AFWS between Units 3 and 4. While Unit 4 was in shutdown, permission was given to close certain valves. However, the wrong valves were closed rendering the steam supply to the operable AFW pumps shut off. Lack of independent verification, deficient procedure.	IRS 0338.00
9/28/83	XXX	Containment Spray	5		x	Train B was declared inoperable due to equipment failure. However, train A was also inoperable due to a different equipment failure. This had remained undetected for 5 hours. The failure to detect the inoperability of train A was attributed to error of omission as well as a procedural deficiency.	IRS 0416.G2
11/16/83	XXX	Standby Gas Treatment Plant	1440	x		A separation jumper had been installed to prevent spurious starts of unit 1 & 2 shared safety related equipment. The jumper installation prevented auto-start of the SB gas treatment system. Error of omission.	IRS 0437.G4
11/29/83	XXX	Containment Spray	ca. 720		x	Two containment spray discharge valves were found closed with the CB:s locked open. Failure to perform valve position checks prior to startup. Work planning deficiencies.	IRS 416.G1
4/7/84	XXX	ECCS	14		x	Unit in hot shutdown. The BIT inlet and outlet valves were closed during recharging operations. Procedural deficiency.	IRS 0454.00
6/20/84	Cook-1	ESF Ventilation	ca. 12		x	Both trains of ESF equipment ventilation inoperable due to misinterpretation of test procedure.	LER 50-315/84-011 (IRS 0709.00)

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (3-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
8/8/84	Cook-1	AFWS	ca. 8		x	Two MD AFW pumps inoperable due to failure to reset switches in auto. Procedural deficiency. Unit was in hot standby.	LER 500-315/84-016 (IRS 0709.02)
11/8/84	XXX	CCWS	> 8700		x	Blind flange installed on outlet side of the relief valve of the CCW surge tank. In this configuration the system was not adequately protected against over-pressure (e.g., water hammer). Probably an installation error that existed from the plant construction period.	IRS 0533.00
11/10/84	XXX	RPS	> 4000	x		The steam pressure density compensation line to each of the four flow transmitters was valved out. Procedural deficiency.	IRS 0536.00
12/18/84	Kewaunee	ECCS	≤ 360	x		Misaligned switch rendered auto-switchover from BAT to RWST upon low BAT level. The switch had been misaligned during a previous monthly surveillance. Communication problem + status display deficiency.	LER 50-305/84-021 (IRS 0589.00)
3/21/85	XXX	ESWS	unknown	x		Two open states link-terminal blocks in aux. control circuit rendered one loop of ESW inoperable. The states links had been opened by contract worker. Inspection/calibration error.	IRS 0590.00
2/1/86	XXX	SLCS	ca. 4000	x		Redundant explosive squib valves failed to actuate due to sneak circuit in the monitoring circuit. Not detected due to procedural deficiency.	IRS 0629.02
10/20/86	XXX	ECCS	≥ 4		x	Both LHSI & HHSI unavailable when bringing plant from CSD to hot shutdown. Procedural deficiency, poor communications.	IRS 0764.00

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (4-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
4/17/87	XXX	Emergency Containment Atmosphere Monitoring System	> 8700	x		Blind flange had been fitted to the discharge piping of the containment atmosphere monitoring system. The same fault also revealed in Unit-3. Error of omission.	IRS 0879.00
5/26/87	XXX	RPS	Not known		x	During preparatory phase for cold pre-critical testing, the RPS and monitoring system became totally unavailable. The alarm signals received in the control room did not alert the operators about the unavailability. Work planning deficiencies.	IRS 1086.00
6/28/87	Ringhals-3	ECCS	≥ 4		x	In connection with maintenance work on LHSI system during the annual refueling outage, two injection paths to RC cold legs were inadvertently disconnected. Work planning deficiency.	R3-RO-011/1987
11/1/87	XXX	Containment Spray System	500		x	During routine power operation, four manual isolation valves were found closed during a periodic check. The valves had been closed 3 weeks earlier during a periodic test. Error of omission, procedural deficiency.	IRS 0880.00
7/8/88	XXX	ECCS	ca. 8700	x		During a manual test of actuators, a regulating valve in a HPIS bypass line was found closed. It was not known if the valve had been closed since modification work during the 5th refueling outage, or if it was the result of maintenance during the 6th cycle. Procedural deficiency.	IRS 0982.00

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (5-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
9/14/88	Oskarshamn-1	ECCS	2.75		x	Two ECCS pumps (323 P1/P2) remained unavailable upon completion of maintenance work (pump breakers were not closed). Error of omission. Deficient work planning.	O1-RO-018/1988
2/19/90	XXX	ECCS	10		x	During the annual shutdown, an operator discovered a tagging error on the LPSI suction trains rendering the entire function unavailable. Deficient work planning. Error of omission.	IRS 1147.00
3/20/90	Catawba-1	RCS	ca. 672		x	Root valves for system pressure transmitters were valved out by I&E personnel. These pressure transmitters provided CR indication and PORV actuation as part of LOTP system. Tagging error during LP&S operations.	NRC Special Report DPC, 4/26/90
7/3/90	XXX	ECCS	72		x	During startup after refueling, the HPSI isolation valves were found closed on the 3 trains. This was discovered after reaching 180 C. Procedural deficiency. Error of omission. **INES = 2**.	IRS 1117.02
9/4/90	XXX	Scram System	3.5		x	Plant startup proceeded with discharged scram system accumulators. The deficiency was discovered during shift turnover. Procedural deficiency. EOO. Inadequate training.	IRS 1123.00
4/3/91	Harris-1	ECCS (HPI function)	ca. 8700		x	Tests conducted during refueling outage revealed that both relief valves in alternate miniflow lines had been inoperable due to a water hammer event caused by improper filling and venting in connection with installation of relief valves during the previous outage. Deficient procedure.	LER 50-400/91-008

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (6-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
4/10/91	Millstone-3	ECCS (HPI function)	ca. 5.2 yrs		x	Test revealed that the set pressure for HPSI-A/B relief valves was too close to system operating pressure. Design error, procedure and test error.	LER 50-423/91-011
9/1/91	Diablo Canyon-2	Containment spray + RHRS sump isol. Valves)	6		x	Plant in Mode 4 (hot shutdown). Both RHR pump suction valves inadvertently de-energized. Both containment spray pumps deenergized. Human error, procedural deficiency. Detected by system walkdowns.	LER 50-323/91-003
9/18/91	XXX	RPS	0.87	x		With the unit at full power, an operator found 1-of-2 control panels for RPS logic unavailable. Installation error and/or manufacturing/construction defect.	IRS 1268.00
7/17/92	Sequoyah-2	RHRS	17		x	Incorrectly terminated wire on flow switch. Deficiency in instrument preventive maintenance data package for RHR miniflow switches. Inadequate post-maintenance test.	LER 50-328/92-010
1/22/93	South Texas-1	EDG	ca. 600	x		EDG failed to start during a monthly surveillance test. Caused by paint applied to fuel injection pumps. The paint ran into fuel metering rod ports. Lack of proper work process control.	LER 50-498/93-005
1/26/93	Oconee-3	AFWS	5.5		x	Following the recovery from a reactor trip, involving transfer from AFW to MFW, both AFW control valves were not placed in auto mode. Operator error.	LER 50-287/93-001
1/29/93	Three Mile Island-1	RHRS	3		x	Personnel error caused both RHR heat exchangers to become unavailable. A licensed control room operator discovered the condition. Procedural deficiency.	LER 50-289/93-002

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (7-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
2/25/93	Catawba-1/2	ESW	ca. 1000		x	With Unit 1 at 100% power and Unit 2 in refueling, 3-of-4 ESW pump discharge valves failed to open (4 pumps serve both units). Discovered by surveillance testing. Deficient maintenance procedure caused the incorrect MOV torque settings.	LERs 50-413/93-002 & 50-414/93-002
11/6/93	Beaver Valley-2	EDG	ca 3 yrs		x	The auto loading capability of 2 EDGs failed during a test. The failure occurred when an SI signal was present coincident with a loss of normal power supply to the ESF bus. Caused by misoperation of a digital solid state timer. Inadequate engineering requirements guidelines.	LER 50-412/93-012
7/14/94	Paks-4	ECCS	10		x	During I&C maintenance, a short circuit resulted in interlocking operations and the subsequent inoperability of two HPI pumps. New system status not discovered until 10 hour later. Combination of design and procedural deficiency. **INES = 1**.	Paks Event Report B49406
9/28/94	Barsebäck-1	RPS	216	x		During restart after refueling, shift supervisor detected three blockages of end relays belonging to one condition chain in the RPS (reactor depress. function). Deficient work planning. Procedural deficiency.	IRS 1549.00 B1-RO-35/94
10/18/94	Catawba-2	AFWS	60		x	A reactor trip occurred during testing of solid state protection system. The AFWS auto started and 8 hours later the AFWS was secured & transfer made to MFW. The AFW flow controllers were set to zero. On 10/21/94 it was discovered that the valves were closed. Deficient EOP and shift turnover procedures. Three shift changes before mispositioned valves were detected.	LER 50-414/94-007

Table 2-2: *Summary of Events Involving Undetected Latent Failures of Safety-Related Systems (8-of-8).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
6/12/96	Barsebäck-2	Gas Treatment System for the Atmosphere (System 741)	226.5	x		During startup following annual refueling outage a valve between dry well and wet well was found open causing the containment PS-function to be unavailable. Deficient work planning. Procedural deficiency. **INES = 1**.	B2-RO-010/1996
11/13/96	Oskarshamn-2	ECCS	413		x	During a functional test of System 323 (Emergency Core Cooling System) the two pumps failed to start. The pump breakers were open; they had not been re-closed upon completion of the annual testing. Procedural deficiency. **INES = 2**.	O2-RO-043/1996
8/17/97	Ringhals-2	RPS	17		x	During startup, the end relays for the RPS auto SI function were found open. The end relays had been opened to prevent RC overpressurization. Deficient work planning. **INES = 1**.	R2-RO-026/1997
9/28/97	Ringhals-4	Containment Spray System	20		x	During startup after the annual refueling it was discovered that two MOVs in the containment spray system were closed. They had been closed in preparation for the Containment Air Test and not been restored. Deficient work planning. **INES = 2**.	R4-RO-043/1997
11/13/97	Nine Mile Point-2	RCIC	ca. 5000		x	During plant walkdown, an instrument root valve (pressure transmitter) was found shut. The closed valve rendered the RCIC inoperable. The root valve had not been opened following maintenance ca. 7 months earlier. Deficient work planning. Deficient procedure.	NRC Daily Event Report

Table 2-3: *Selected U.S. LERs on Mispositioned Equipment - Full Text LERs Not Yet Retrieved*[6] *(1-of-4).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
1990	Surry-1	MFW	--		x	All six main feedwater flow transmitters found isolated, equalized and drained.	LER 280/90-19
1990	Perry	RPS	ca. 170		x	CR RM isolated for more than 7 days.	LER 440/90-38
1990	Perry	Containment Spray System	--		x	Both loops of the CS inoperable because of mispositioned valve. Procedure problem.	LER 440/90-39
1990	San Onofre-2	AFWS	ca. 1320	x		Turbine-driven AFW pump inoperable for 55 days.	EA 90-115
1990	Perry	I&C	--	x		Mispositioned equalizing valve on reactor vessel water level instrumentation.	LER 440/90-34
1990	San Onofre-2	--	96	x		Violation for leaving sump valve open 4 days.	IR 361/90-37
1990	Catawba-1	--	--	x		Violation for not following a procedure that resulted in a mispositioned valve.	IR 413/90-29
1990	Fermi	ECCS	19	x		HPSI suction valve mispositioned for 19 hours after surveillance test.	IR 341/90-13
1990	Prairie Island-1	--	--		x	Inadvertent mispositioning of 11 heater controls.	LER 282/90-13
1990	Hatch-1	ECCS	--		x	Mispositioned valves in the core spray system.	IR 321/90-15
1990	Harris-1	--	--	x		Essential chiller inoperable due to mis-positioned valve.	IR 400/90-14
1990	Robinson-2	Fire Damper	--	x		Fire damper left in open position. Only damper to be closed to be operable.	LER 261/90-11
1990	Summer-1	CCWS	--	x		Two chiller system valves in wrong position. Failure to verify position.	IR 395/90-18
1990	Turkey Point-3	ECCS	--	x		One ECCS flow path left unavailable during reactor mode change.	IR 250/90-14

[6] Status as of 2/27/98.

Table 2-3: *Selected U.S. LERs on Mispositioned Equipment - Full Text LERs Not Yet Retrieved (2-of-4).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
1990	Millstone-3	ECCS	4	x		Accumulator isolated unknowingly when operator failed to reopen valve after fill.	LER 423/90-17
1990	Salem-2	Radwaste	--	x		Radwaste effluent line monitor left isolated by chemistry personnel.	LER 311/90-24
1990	Peach Bottom-2	--	--		x	Valves left closed after removal of blocking permit.	LER 277/90-12
1989	Calvert Cliffs-1	ECCS	--	x		HPSI discharge header valves not locked shut per LTOP requirements.	LER 317/89-19
1990	Harris-1	Radwaste	--	x		Misaligned valve caused unplanned release from waste gas system.	LER 400/90-13
1990	South Texas-1	Containment Ventilation	ca. 0.5		x	All three trains of containment vent. isolation in test mode and inoperable. Mode 6	LER 498/90-07
1990	Hatch-1	RV head vent	--		x	Two RV head vent valves found closed.	LER 321/90-08
1990	Seabrook	--	--		x	Numerous instrumentation valves found mispositioned.	LER 443/90-12
1990	Palisades	AFWS	--		x	AFW inoperable because backup nitrogen bottles isolated.	LER 255/90-05
1990	Sequoyah-1	AFWS	--	x		Handswitch controlling steam supply to AFW pump in manual.	LER 327/90-04
1990	Trojan	ECCS	--	x		Control switches for HPSI found in pull-to-lock position.	LER 344/90-29
1991	WNP-2	RHRS	--	x		RHR system differential pressure switch found isolated.	LER 413/91-20
1991	Palo Verde-3	AFWS	--	x		Equalizing valve on AFW flow transmitter found open.	LER 530/91-11
1991	Comanche Peak-1	AFWS	336	x		Recirc. test line had isolation valve ¼ -turn open even though independently verified.	LER 445/91-10
1991	Peach Bottom-2	EPS	--		x	Two diesels discovered inoperable because of mispositioned fuel oil valve.	LER 277/91-20
1991	McGuire-2	AFWS	--		x	TDAFW inoperable due to mispositioned sliding link on a pressure switch.	LER 370/91-02

Table 2-3: *Selected U.S. LERs on Mispositioned Equipment - Full Text LERs Not Yet Retrieved (3-of-4).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
1991	Salem-1	ECCS	--	x		ECCS suction valve not repositioned per tagging release work sheet.	IR 272/91-09
1991	Surry-1	EPS	--	x		Fuel oil transfer pump erroneously tagged-out / secured making one DG unavailable.	LER 280/91-04
1991	Catawba-1	ECCS	--		x	LPSI suction valve closed during power escalation.	LER 413/91-02
1990	Millstone-2	SWS	--		x	Service water cross-tie header valve found open.	LER 336/90-22
1992	Calvert Cliffs-1	ECCS	--		x	Violation for the isolation of the common miniflow line for all ECCS.	IR 317/92-27
1992	San Onofre-2	CCWS	--	x		Operator discovered emergency seal water isolation valve closed for salt water pump.	LER 361/92-09
1992	Zion-1	AFWS	--	x		AFW discharge valve locked closed. Previous event noted in a DVR in 1990.	LER 295/92-20
1992	Perry	SLCS	--		x	Valve positioning error disabled both SLCS trains.	LER 440/92-19
1992	Catawba-1	CVCS + ECCS	--		x	Violation for valve misalignments in CVCS, ECCS, and steam generator (SG) blowdown line. One deficiency was the operators incorrectly assumed that alignment was returned by fill and vent procedure. In another instance, the operators failed to close valves within block tag-out. These errors resulted in fluid discharge. The cause of the misalignment of the SG blowdown valves was not determined.	LER 413/92-22
1992	South Texas-1	AFWS	--		x	All 4 AFW control valves closed after recovering from reactor trip.	LER 498/92-06
1993	Quad Cities-1	ECCS	--		x	Failure to return valve positions in HPCI lines following test.	LER 254/93-17

Table 2-3: *Selected U.S. LERs on Mispositioned Equipment - Full Text LERs Not Yet Retrieved (4-of-4).*

Date	Plant	System(s)	Out of Service (OOS) Time [Hours]	Single Train OOS	Multiple Trains OOS	Apparent Cause + Root Cause	Reference
1993	Pilgrim	RCS	3	x		Two ATWS pressure transmitters valved out for 3 hours. These valves were closed during a backfilling procedure which was unclear about which of the two valves in series to close. As a result, the I&C personnel left the valve closest to the instrument rack closed.	LER 293/93-20
1993	Arkansas-1	AFWS	--	x		Mispositioned locked throttle valve in the AFW bearing cooling return line. The licensee identified several other cases of mispositioned valves.	IR 313/93-06
1993	Grand Gulf-1	RHRS	--		x	Mispositioned valves in the RHR system.	IR 416/93-07
1993	Brunswick-2	RHRS	> 8700		x	RHRS isolated when wrong fuse was removed. Incorrect labeling.	LER 324/93-04
1993	Millstone-2	ECCS	--	x		Mispositioned HPSI valve discovered by operator.	LER 336/93-03
1993	St. Lucie-2	ECCS	--	x		Safety injection tank isolation valve left open following test in Mode 5.	LER 389/93-05

2.2 HRA & PSA Perspectives

The mispositioning of equipment is covered in the typical system models of PSA. Deviations from the standard analysis practice should be supported by proper justification. Typical guidelines for system fault tree development include errors made in test & maintenance (e.g., components not returned to normal status and as identified by written procedure). Also included in the typical system fault tree is the manual backup to auto initiation failure, given that the system time-window is sufficiently long.

The completeness issues in PSA imply that systematic searches be made for unique situations that could challenge the plant safety barriers; e.g., unanalyzed plant condition that is beyond normal operator training and/or procedures. An *error forcing context* (EFC)[4] represents the combined effect of performance shaping factors and plant conditions that create a situation in which human error is likely. The plant conditions include plant configuration, system, component, instrumentation & control availability and reliability, process parameters, etc., which result in unusual plant configuration.

Looking at the events in Table 2-2 and Table 2-3, several of the latent errors remained undetected through two or more shift turnovers. This indicates that there is necessity in performing event analyses that go beyond finding the apparent causes of failure. Why did the errors remain undetected, and would the errors have been corrected in the case of a real plant transient. What-if analyses, root cause analyses and PSA-based event analyses should be used to evaluate the potential consequences of undetected errors in combination with other factors.

In the opinion of the author of this report, comprehensive and systematic evaluations of occurred events should be pursued to enable the development of experience-based databases on human error (Lydell, 1998). There is a need for calibrating human error probabilities that are derived using expert judgment techniques. Especially HEPs for mispositioned equipment affecting multiple safety trains.

2.3 Trends & Patterns

Are the undetected, latent failures of safety-related equipment or systems indicative of plant safety culture problems? A limited review of recent U.S. NRC reports on 'Systematic Assessment of Licensee Performance' (SALP) provides interesting insights. Four SALP reports were chosen at random. The SALP ratings of the four licensees ranged from 1 ('superior level of safety performance') to 3 ('acceptable level where the NRC will consider increased levels of inspection effort). In the four cases the performance analysis addressed recurring problems with undetected latent errors:

[4] NUREG/CR-6350 (1996): *A Technique for Human Error Analysis (ATHEANA). Technical Basis and Methodology Description.*

- SALP report on Callaway (NRC, 1997a). 'Operations' was rated a 2 ('good level of safety performance'). '… Plant operations during transient and nonroutine events continued to be superior; however, performance during normal, routine operations did not display the same degree of rigor and consistency. This was demonstrated by the numerous instances of procedural violations and inattention to detail and continuing problems with protective tagging and valve misalignments …"

- SALP Report on Clinton (NRC, 1997b). 'Operations' was rated a 3 ('acceptable level where the NRC will consider increased levels of inspection effort). "…Although conduct of operations in the control room was adequate, a number of errors were identified. Failure to track identified leakage during the RR pump seal failure event complicated the operating crew's ability to evaluate the proper emergency action level classification. An incorrectly performed valve line-up resulted in a large spill of feedwater which was not identified for two shifts despite repeated control room annunciator indications of high emergency core cooling system sump levels. NRC inspectors identified some instances of inadequate short term relief turnovers, incomplete operator logs and round sheets, and informal control room communications. Further, the inspectors identified one example of an operator leaving the 'at the controls' area without proper

- SALP Report on San Onofre 2 & 3 (NRC, 1997c). 'Operations' was rated a 2 ('good level of safety performance'). "… Programs for operations were generally excellent, including the programs for conduct of operations and minimizing operator work-arounds. However, procedure quality and usage problems were observed. Some procedures were very complex, containing transition and component identification errors, or were inconsistent with other guidance. Procedure changes continue to be numerous, indicating a need for improved procedures; although, the backlog of changes was being effectively managed. Weaknesses in procedure detail contributed to the failure to properly position a reactor vent valve …… Operators generally followed plant procedures during normal operations; however, operators occasionally exhibited weakness in attention to detail. Examples of this include setting the automatic boric acid flow rate low, the mispositioning of several valves, and not verifying offsite power sources when an emergency diesel generator was inoperable …"

- SALP Report on Oconee (NRC, 1997d). 'Operations' was rated a 2 ('good level of safety performance'). "… Procedure adherence and procedure quality issues provided challenges during this period. Operating procedure deficiencies and the failure to follow procedures by Operations personnel contributed to several operational events during the period …… Weaknesses identified during the previous assessment period regarding fuel handling and event report timeliness and quality have shown improvement during this period. Configuration control issues have also shown improvement with respect to the number of issues; however, there were several significant mispositioning events during this period that indicated continuing challenges in this area …"

Again, the four examples demonstrate the complex nature of latent errors. The mispositioning of equipment and non-detection is a universal problem affecting all plants. The root causes of these errors are found in all areas identified by Figure 2-2. Many industry studies have been performed since the 1980s; *c.f.* Tripathi (1986) and Israel (1994). In the U.S., the licensee corrective actions generally have not included tangible modifications such as status alarms and position markers, but rather, they have leaned toward employee discipline and counseling (Israel, 1994).

2.4 References

Israel, 1994. *Review of Mispositioned Equipment Events*, AEOD/T94-02, U.S. Nuclear Regulatory Commission, Washington (DC).

Lydell, B.O.Y., 1998. *Some Views on the Role of Human Factors Empirical Studies in Probabilistic Safety Assessment*, RSA-R-98-01, Presentation at the NUPEC Meeting, San Diego (CA), January 6-7, 1998.

U.S. NRC, 1997a. *SALP Report on Callaway*, Report No. 50-483/97-99, Washington (DC).

U.S. NRC, 1997b. *SALP Report on Clinton*, Report No. 50-461/97-001, Washington (DC).

U.S. NRC, 1997c. *SALP Report on San Onofre 2 & 3*, Report No. 50-361/97-99; 50-362/97-99, Washington (DC).

U.S. NRC, 1997d. *SALP Report on Oconee Nuclear Station*, Report No. 50-269/97-99; 50-270/97-99; 50-287/97-99, Washington (DC).

Tripathi, R., 1986. *Degradation of Safety Systems Due to Component Misalignment and/or Mispositioned Control/Selector Switches*, AEOD/T612, U.S. Nuclear Regulatory Commission, Washington (DC).

3

INTERIM CONCLUSIONS & RECOMMENDATIONS

Undetected failures of safety systems due to mispositioned equipment are commonplace. In most cases, the events involving mispositioned equipment are discovered soon after occurrence (e.g., several minutes to no more than a couple of hours), however. All events represent precursors to breaches of safety barriers, and systematic efforts should be implemented to ensure effective transfer of knowledge and insights from the event evaluations.

3.1 Interim Conclusions

The preliminary survey of events was limited to spot checks of information resources such as the U.S. NRC LER system, SKI's database on 'reportable occurrences', and the IRS database. The amount of information addressing undetected, mispositioned equipment is very extensive. On an annual basis, most, if not all, operating nuclear power plants experience one or more events where engineered safety features were rendered partially or completely unavailable for some time. Some of these events have generic implications, and the potential safety implications range from the benign to the serious. Modern, symptom-based emergency operating procedures (EOPs) have proven to be effective in supporting recoveries from latent errors. Among the interim conclusions are:

- Events that occurred ten or more years ago are repeated today. This indicates that the root cause analysis programs have not been fully effective, and event evaluations can be very complex.

- Based on the U.S. experience, a large number of reported events occurred in PWRs as compared to BWRs. One reason for this disparity could be that the BWRs have more automatic alignment features than the PWRs.

- There is no significant difference in event recurrence rates between the good and poor performers among the worldwide nuclear power plant population.

- The root cause(s) of undetected, mispositioned equipment quite often include such latent errors as design errors, deficient plant procedure, unanalyzed safety conditions, and human factors deficiencies. Significant improvements in the prevention of mispositioned equipment can be achieved through improvements in shift turnover practices, communications, and operator training.

- Introduction of new I&C technology (e.g., computer-based digital systems) could enhance the annunciation/indication of plant equipment status (e.g., valve, switch, breaker positions). As evidenced by some recent events, the added complexity for operation and maintenance of the digital systems increases the chance of human-machine interface errors, however.

3.2 Recommendations

SKI's monitoring of operating experience involving latent errors should continue. It is extremely important that event evaluations including root cause analysis efforts go beyond the identification of programmatic errors. A systematic program should be developed to analyze the potential implications of occurred events. Specific recommended action items include:

- Implement a comprehensive, modern root cause analysis program to more effectively address the full spectrum of latent errors. A program such as the U.S. NRC 'Human Performance Investigation Process', or its enhanced versions should be considered.

- Validation of human error probabilities (HEP) for valve/switch/breaker misalignments through a systematic review of the available operating experience. Sufficient operating experience does exist to extract human error data. Perform a review and comparison of analysis practices, including HEP estimates used in the Swedish PSAs.

- Improved consideration of conditioning events (or human error forcing contexts) in the HRAs through systematic reviews of the available operating experience.

- Perform reevaluations of the recent Swedish events to delineate the reasons (i.e., root causes) of delayed detection. Perform reviews of existing EOPs and simulator training programs to determine how the particular events involving mispositioned equipment would have been recovered during plant transient conditions.

A

ABBREVIATIONS & ACRONYMS

BRS	Bibliographical Retrieval System
ECCS	Emergency Core Cooling System
EFC	Error Forcing Context
EOP	Emergency Operating Procedure
ESF	Engineered Safeguards System
HRA	Human Reliability Analysis
IR	Incident Report
IRS	Incident Reporting System
IPE	Individual Plant Examination
LER	Licensee Event Report
PSA	Probabilistic Safety Assessment
RHR	Residual Heat Removal
RO	Reportable Occurrence
SALP	Systematic Assessment of Licensee Performance
SCSS	Sequence Coding and Search System
SLCS	Standby Liquid Control System
T&M	Test & Maintenance