NEA/CSNI/R (97)5 - Part 1

Restricted

LATENT FAILURES OF SAFETY SYSTEMS

A generic study performed by the Principal Working Group 1 on Operating Experience and Human Factors

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY

Le Seine Saint-Germain - 12, boulevard des îles
F-92130 Issy-les-Moulineaux - France
Fax: 33 (1) 45 24 11 10 - Telex: 640048 - Electronic mail: NEA@nea.fr
UNDETECTED FAILURES OF SAFETY SYSTEMS

A Generic Study Performed by the Principal Working Group 1 of the Committee on the Safety of Nuclear Installations
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995) and Hungary (7th May 1996). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of all European Member countries of OECD as well as Australia, Canada, Japan, Republic of Korea, Mexico and the United States. The Commission of the European Communities takes part in the work of the Agency.

The primary objective of NEA is to promote co-operation among the governments of its participating countries in furthering the development of nuclear power as a safe, environmentally acceptable and economic energy source.

This is achieved by:

- encouraging harmonization of national regulatory policies and practices, with particular reference to the safety of nuclear installations, protection of man against ionising radiation and preservation of the environment, radioactive waste management, and nuclear third party liability and insurance;
- assessing the contribution of nuclear power to the overall energy supply by keeping under review the technical and economic aspects of nuclear power growth and forecasting demand and supply for the different phases of the nuclear fuel cycle;
- developing exchanges of scientific and technical information particularly through participation in common services;
- setting up international research and development programmes and joint undertakings.

In these and related tasks, NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has concluded a Co-operation Agreement, as well as with other international organisations in the nuclear field.

 Publié en français sous le titre :

© OECD 1996
Applications for permission to reproduce or translate all or part of this publication should be made to:
Head of Publications Service, OECD
2, rue André-Pascal, 75775 PARIS CEDEX 16, France.
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

***********

The opinions expressed and the arguments employed in this document are the responsibility of the authors and do not necessarily represent those of the OECD.

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France
TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. INTRODUCTION

2. ORGANISATION OF THE REPORT

3. EVALUATION OF SIGNIFICANT EVENTS INVOLVING UNDETECTED FAILURES OF SAFETY SYSTEMS
   3.1 definition of undetected failures
   3.2 information sources
      3.2.1 IRS reporting categories
      3.2.2 Criteria used in the ASP Programme
   3.3 description and discussion of events
   3.4 design deficiencies
      3.4.1 re-analysis of design basis accidents
         3.4.1.1 steam generator tube re-analysis at North Anna
         3.4.1.2 main steam line break re-analysis at Millestone-2
      3.4.2 emergency electrical power sources
         3.4.2.1 overloading and sequence logic deficiencies
         3.4.2.2 inadequate cooling
      3.4.3 auxiliary feedwater system
         3.4.3.1 failure to meet the single failure criteria
         3.4.3.2 inadequate net positive section head
         3.4.3.3 deficiency in the containment penetration isolation valve
         3.4.3.4 venting problems in the nuclear service water discharge piping supplying the safety grade auxiliary water
      3.4.4 flooding, seismic, fire, and environmental protection
      3.4.5 component cooling water system
         3.4.5.1 deficiencies in the line connected to the thermal barrier of the reactor coolant pumps
         3.4.5.2 deficiencies in post-accident containment cooling conditions
      3.4.6 residual heat removal system
      3.4.7 containment integrity
      3.4.8 service water system
      3.4.9 emergency core cooling system
3.4.9.1 low pressure coolant injection valve single failure valve reliability
3.4.9.2 high pressure injection pump inoperability
3.4.9.3 hydrogen gas hindering of low pressure and high pressure coolant injection pumps
3.4.9.4 failure of low pressure safety injection pumps and containment pumps for recirculation mode as a result of air entrainment
3.4.9.5 inadequate relief set points of the high pressure safety injection system
3.4.9.6 emergency core cooling system minimum - flow lined deficiencies
3.4.9.7 design deficiency in installation of instrumentation taps on emergency core cooling system lines
3.4.9.8 emergency core cooling system switching deficiency from injection to recirculation mode
3.4.9.9 plugging of emergency core cooling suction strainers

3.5 inadequate or incomplete testing
   3.5.1 motor-operated valves
   3.5.2 tests never performed
   3.5.3 unforeseen interactions and incorrect initial configuration
      3.5.3.1 procedural deficiencies resulting in incomplete testing
      3.5.3.2 procedural deficiencies masking deficiencies
   3.5.4 tests not simulating actual conditions
   3.5.5 inappropriate prerequisites
   3.5.6 incomplete testing
      3.5.6.1 failure to verify testing overlap in logic testing of safety related circuits
      3.5.6.2 failure to verify the operability of a check valve on the reactor coolant pump fire protection system
   3.5.7 inability of routine test measurements to identify certain failure modes
   3.5.8 inadequate calibration and evaluation of instrumentation set-points

3.6 inadequate control of modifications to safety-related systems
   3.6.1 incomplete post-modification testing
   3.6.2 inadequate design control and post-modification testing
   3.6.3 deficiencies in the quality organisation

3.7 improper installation
   3.7.1 deficient electrical terminations in safety-related components
   3.7.2 multiple grounds in direct current distribution systems
   3.7.3 inadequate configuration control
   3.7.4 quality organisation deficiencies
   3.7.5 erroneous installation of instrumentation

3.8 inadequate maintenance
   3.8.1 lack of maintenance and imprecise guidance in maintenance procedures
   3.8.2 deficiencies in the quality organisation
   3.8.3 inadequate or incomplete post-maintenance requalification testing
   3.8.4 incidents caused by the installation of temporary devices
3.9 ineffective experience feedback
3.10 results and conclusions

4. CORRECTIVE AND PREVENTIVE ACTIONS CONDUCTED BY LICENSEES AND REGULATORY ORGANISATIONS

4.1 regulatory requirements
   4.1.1 periodic safety reassessments
   4.1.2 decennial inspections and tests
   4.1.3 probabilistic risk assessments
   4.1.4 individual plant examinations

4.2 specific corrective and preventive actions conducted by licensees and regulatory organisations
   4.2.1 United States
      4.2.1.1 findings and insights gained from operating experience feedback for specific issues
      4.2.1.1.1 reliability of safety-related steam turbine-driven standby pumps
      4.2.1.1.2 solenoid-operated valve problems
      4.2.1.1.3 high pressure coolant injection system at US Commercial BWR plants during 1987-1993
      4.2.1.2 insights on licensee’s corrective actions related to undetected failures of safety systems
   4.2.2 Spain
   4.2.3 Belgium
   4.2.4 Finland
   4.2.5 Sweden
   4.2.6 France
      4.2.6.1 in-service test programme
      4.2.6.2 requalification tests
      4.2.6.3 modification implementation
      4.2.6.4 installation of temporary devices
      4.2.6.5 restarting operations
      4.2.6.6 site endurance tests

4.3 Conclusions
EXECUTIVE SUMMARY

Undetected failures of safety systems in nuclear power plants are of a great concern, especially when the failures remain undetected for a long time. Survey of operating experience through the incident reporting system (IRS) and licensee event reports (LERs) revealed that a significant number of latent failures remained undetected during many years of commercial operations sometimes since initial start-up. Also, plants operated under unaanalysed conditions, outside their design basis condition, or with long-term unavailabilities associated with high conditional core damage probabilities.

Deficiencies affecting safety related systems and their support systems have been discovered in all nuclear activities from initial fabrication, design and installation or commissioning tests, in-service testing, maintenance, inadequate review and testing of safety system modifications.

Though a downtrend should normally be observed as a result of the increased integrated operating experience of the nuclear industry, recent events indicate that deficiencies in initial design are still being discovered. Moreover, latent failures have been introduced in the course of inappropriate or ineffective maintenance activities, as well as through incompletely reviewed and tested design changes or modifications. In other cases, deficiencies in the quality organisation as well as failure to implement corrective actions in time have also contributed to maintain these failures during an extended period.

This inability to detect problems in a timely manner indicates that existing means to demonstrate the functional capability of equipment to comply with regulatory requirements need to be used more efficiently or upgraded.

In the light of the events reviewed in this report which entails a widespread field of failures involving a broad class of systems and a great variety of failures, it appears that some of these failures could have been detected earlier by more complete surveillance tests or prevented by better monitoring and more effective post-maintenance testing. Moreover, as nuclear plants get older, increasing attention should be given to maintenance and modification activities. Therefore efforts should be directed to:

1. Improve existing test programmes and procedures in order to render them more comprehensive.

2. Assess modifications implementation and subsequent requalification.

3. Establish post-maintenance testing requirements in order to verify the performance of repaired or replaced component and the functional requirements of the whole system.

4. Implement appropriate instrumentation, monitoring or diagnostic techniques, for trending component performances.

The report gives an overview of the specific findings, insights, and actions as reported in the individual contributions of the participating countries. It provides some
guidance and insights gained from generic studies that could be useful in implementing corrective and preventive actions.
1. INTRODUCTION

In September 1994, Principal Working Group Number 1 (PWG-1) of the Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) decided to conduct a generic study on undetected failures of safety systems in nuclear power plants (NPPs). These failures are of great concern especially when they remained undetected for a long time.

The scope of the study was to review them with respect to the discovery methods and the corrective and preventive actions by the licensees and the regulatory organisations in order to gain insights which could be useful in preventing or reducing the likelihood of such failures.

Representatives from Belgium, Finland, France, Germany, Spain, and the United States agreed to participate in the study, and the representative of France volunteered to coordinate it. Sweden joined the Working Group later. Participating countries contributed to the study by submitting reports documenting the most representative examples of deficiencies discovered in their respective countries, along with general comments underlying the specific findings and insights resulting from their respective evaluations.

2. ORGANISATION OF THE REPORT

The first part of the report (sections 1 to 3) deals with the categorisation and evaluation of latent failures according to the type of deficiency, method of discovery, failure causes, corrective and preventive actions, with the purpose to gain insights from failures which could be useful in preventing or reducing the likelihood of such failures. This evaluation was performed independently of where the failures occurred.

The second part (section 4) deals with the specific corrective and preventive actions undertaken in each participating country by licensees or regulatory organisations as result of the findings and insights gained during their respective operational experience.

Copies of the reports submitted by the participating countries are gathered in a separate volume.

3. EVALUATION OF SIGNIFICANT EVENTS INVOLVING UNDETECTED FAILURES OF SAFETY SYSTEMS

3.1 Definition of Undetected Failures

For the purpose of this study, undetected failures of safety systems include significant events in which equipment (system, component, logic circuitry, or structure) remained inoperable or would have been unable to correctly fulfil its intended function for an extended period of time until its condition was discovered.
In this definition, an extended period of time is a period of at least one refuelling cycle duration or several test intervals.

Failure of non safety systems were also considered when such failures prevented safety systems from fulfilling their intended functions.

Failures concerning the integrity of the primary circuit and steam generator tubes were not considered in the scope of this study. In addition PWG-1 placed little emphasis on items like motor-operated-valves (MOVs), clogged strainers, and ageing, since these problems were recently reviewed in the course of PWG1 generic studies.

3.2 Information Sources

Information sources are issued from IRS reports and contributions of participating countries including IRS reports as well as events reported in the national data bases, US events included in the Accident Sequence Precursor (ASP) programme and reported in the ASP NUREG status reports as part of IRS reports, Information Notices (INs), Generic Letters (GLs), and Bulletins (BLs) issued by the US Nuclear Regulatory Commission (NRC), and three NUREG operating experience feedback reports on specific issues.

3.2.1 IRS Reporting Categories

Because the IRS coding system does not directly allow for retrieval of events related to latent failures of extended duration, PWG-1 initially scanned for the system and then scanned following reporting categories through careful reading of reports:

- deficiencies in design
- deficiencies in safety evaluation
- discovery of major conditions not previously considered or analysed
- unforeseen or significant interaction between systems
- generic problem of safety interest
- events of potential safety significance
- common cause failure

3.2.2 Criteria used in the ASP Programme

Several countries use quantitative measures to estimate the risk significance of precursor events. In systematically and extensively performing such studies since 1985 the NRC coined the term “accident sequence precursor” (ASP). For the purpose of this study, only were considered precursors involving latent failures that existed for an extended period.

The US ASP programme reviews operational events to identify, categorise, and evaluate precursors to potential severe core-damage accidents. Events are selected as precursors to potentially severe core damage accidents if the conditional probability of subsequent core damage is at least 10-6. ASPs can be either infrequent initiating events or equipment failures which, when coupled with one or more postulated events, could result in a plant condition with inadequate core cooling. Several of the recorded precursor events
involved equipment failures and unavailability caused by conditions that affected the ability of safety equipment to perform its intended function.

The result of ASP analyses indicate the level of risk associated with operating nuclear power plants based on direct assessment of actual operating experience. These analyses consider only significant events, and LERs are eliminated as precursors if they involve no more than the following conditions:

- a component failure with no loss of redundancy
- a loss of redundancy in only one system
- a seismic design or qualification error
- an environmental design or qualification error
- a structural degradation
- a design error and event discovered by re-analysis
- an event with no appreciable impact on safety systems
- an event involving only post-core damage impacts

The longest period of unavailability evaluated in ASP analyses is one year. A number of events identified as potentially significant in ASP studies but considered impractical to analyse are only briefly documented in the status reports, although such events are capable of initiating core damage sequences. Examples of such events include component degradation in which the extent of degradation could not be estimated or where a realistic estimate of plant response could not be determined or the impact of the degradation on plant response could not be ascertained (for example, high-energy line break concerns, cable routing not in accordance with requirements for fire protection, and inoperability of flood barriers). These events were not considered in this study, although a few are only mentioned as recurring events.

3.3 Description and discussion of events

In describing the events, PWG-1 considered the following aspects:

- type of deficiency
- method of discovery
- causes and contributing factors that delayed the discovery of the deficiency
- safety significance
- corrective actions

PWG-1 placed more or less emphasis on each of these aspects as appropriate to each event. As a result, events are described in various level of detail. Events are presented in chronological order in each category. In order to derive specific findings, PWG-1 categorised events according to the causes and factors that contributed to their discovery as follows:

- design deficiencies unrelated to the actions of the plant personnel, which are identified mainly in the course of the following activities and events:
  - re-analysis
– design basis reconstitution programmes
– engineering reviews
– probabilistic risk analysis (PRA)
– individual plant examinations (IPE)

• deficiencies related to human errors including:
  – inadequate or incomplete testing
  – inadequate control of modifications to safety-related systems
  – improper installation
  – inadequate maintenance

Many of these deficiencies occurred during implementation of modifications as result of inadequate testing in combination with design deficiencies. As a result, such deficiencies may be discussed in the context of inadequate testing or inadequate control of modifications.

In many cases, the risk significance is highlighted by the conditional probability of potentially severe core damage associated with a precursor event. In other cases, the risk significance of an event must be assessed according to the nature, extent, and duration of the problem, as follows:

• common mode failure of safety systems and degradation of components affecting multiple trains of multiple safety systems
• complete loss of a safety system
• potential off-site radioactive releases exceeding regulatory limits,
• situations assumed to be unrecoverable in the required period, either from the control room or at failed component
• generic aspect
• duration

Discussion of events are included in their associated categories and sub-categories. The distribution of the events selected for this study is as follows:

• design deficiencies
• inadequate or incomplete testing
• inadequate control of modifications
• improper installation
• inadequate maintenance

The following figure includes the main significant events related with latent failures classified according to their safety significance, with indication of the type of reactor and deficiency, and the delay of discovery.
<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>10-3</th>
<th>10-3</th>
<th>10-4</th>
<th>10-4</th>
<th>10-5</th>
<th>10-5</th>
<th>10-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1988</td>
<td></td>
<td>ZION 1-2(15) T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SHEARON HARRIS (1)D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td></td>
<td>ARKANSAS 1 (15) D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1990</td>
<td>CRUAS 4 (2) M (generic)</td>
<td>SEQUOYAH(8) D</td>
<td>FORT CALHOUN(16)D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HADDAM NECK (1)D</td>
<td>CALVERT CLIFFS 1(2) M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1991</td>
<td>SHEARON HARRIS (1)D</td>
<td>OCONEE 1-2-3 (20)D</td>
<td>COMANCHE PEAK (1)D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MILLSTONE 3 (5) D</td>
<td>PEACH BOTTOM 3 (2)M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NINE MILE POINT 2 (0)M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1992</td>
<td></td>
<td>OCONEE 1-2-3 (1)D</td>
<td>POINT BEACH 2 (1) M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1993</td>
<td>PERRY (1) M</td>
<td>QUAD CITIES (8) D</td>
<td>BEAVER VALLEY 2 (3) D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DAMPIERRE 12 units D</td>
<td>ARKANSAS (0.5) M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CATAWBA 1-2 (0.7) T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

conditional core damage probability
duration in years ( )
design deficiency D, testing deficiency T, maintenance deficiency M
PEACH BOTTOM BWR plant name, reactor type
DAMPIERRE PWR

### 3.4 Design Deficiencies

Design deficiencies are usually identified either during the course of studies or fortuitously as a result of plant transients. Events reported during studies typically involve design-basis events that were incorrectly assessed because of improper or nonconservative assumptions, design deficiencies associated to unanalysed conditions that placed the plants outside their design basis as defined in the final safety analysis report (FSAR). The main characteristics of these deficiencies are that they were outside of the control of plant personnel, and they were identified - before any malfunction or incident occurred - in the course of the following activities:

- re-analysis of design basis accidents
- design-basis reconstitution programmes
- probabilistic risk assessments
• engineering assurance programmes
• in-depth engineering studies or reviews performed by the licensees or the regulatory organisation or the nuclear steam supply system (NSSS) vendor
• reviews based on information provided by the NRC or the NSSS vendor.

For these deficiencies re-analysis were performed taking into account more stringent hypothesis than those considered in the initial design. Since most of these deficiencies only involved design errors discovered by re-analysis, they were not included in the criteria of the ASP analysis process. They include risk-significant events associated with single-failure vulnerabilities, and common-mode failures that rendered both redundant safety related trains inoperable. Most of these deficiencies affect plants of older design.

Licensee event reports (LERs) generally do not include any explicit statement of how and when an abnormal condition was discovered. The basic causes that originated these studies are identified only in a few reports such as the re-analysis of design-basis accidents (DBA) that were initiated after a steam generator tube rupture (SGTR) or fortuitously as the result of a steam generator (SG) replacement or when the NSSS vendor was asked to investigate a specific problem at the request of a licensee.

In-depth engineering design reviews of particular events led to evidence of design deficiencies concerning a few plants or generic problems relevant to a particular type or to all types of water-cooled reactors. These deficiencies existed from initial plant construction.

In many cases in-service testing contributed to the discovery of these deficiencies. Most of these events have been selected as precursors and included in the ASP analysis process.

Specifically, 10 precursor events associated with long duration unavailability had conditional core damage probabilities that ranged from 2.1.10^-6 to 6.3.10^-3. Six had probabilities of at least 10^-4, the value traditionally characterising significant events in the ASP programme, one involving the service water system (SWS) and the others the emergency core cooling system (ECCS). Design deficiencies identified concerned ECCS operability during direct and recirculation modes. The other precursors are related to inadequate emergency diesel generators (EDG) cooling problems and deficiencies in the power control logic following a loss of offsite power (LOOP).

Among all of these events, the incident in Barseback NPP (BWR), unit 2 on July 28, 1992, is certainly the most exemplary related to undetected latent failures. Until this incident, safety questions related to strainer clogging were considered to have been resolved. The spurious opening of a safety relief valve, which caused pipe insulation to be torn and discharged to the suppression pool, led to research and development revealing that essential parameters and physical phenomena involved in strainer clogging had not been adequately recognised.

Investigation of a minor event at the Trillo plant (PWR) also resulted in the discovery of significant design deficiencies which existed since initial start-up. This event and another later event, started a vast re-assessment programme, results of which are examined in section 4 of this report.
Since, the precise underlying causes which led to the analysis and design reviews were not specifically identified in the reviewed reports (except the two DBAs) it appeared most appropriate to group the design deficiencies according to affected systems.

3.4.1 Re-Analysis of Design Basis-Accidents

Two DBAs were re-analysed. In the first case, re-analysis was the result of a real SGTR accident which necessitated to implement a modification; in the other case a SG replacement revealed a non conservative assumption in the original analysis. This error could have been discovered otherwise and earlier.

3.4.1.1 Steam Generator Tube Rupture Re-Analysis at North Anna and Surry (PWR)

Following the SGTR accident at North Anna in July 1987, the flow resistance to the SG downcomers was modified by the addition of flow baffle plates. The SGTR event was reanalyzed using a revised containment related events Westinghouse method for calculating SG water mass, which indicated that during the event the water level on the secondary side could fall below the top of SG tubes for 10 minutes period at the beginning of the event.

This is significant because, if the break location becomes uncovered, a direct path might exist for fission products contained in the primary coolant to be released to the atmosphere without being scrubbed by the liquid phase. Offsite dose consequences could exceed those calculated in the FSAR.

The design-basis SGTR accident at Surry was also reanalyzed using the revised Westinghouse method. This analysis revealed that the SG tubes at Surry could also become uncovered even though the two Surry units were not modified by the addition of flow baffle plates. The updated Surry FSAR assumed that the break location is always covered with water.

At North Anna, the SGTR cause was a combination of the deficiency in the original analysis as well as design modification following the SGTR event. The cause at Surry was only the deficient analysis: no hardware changes were made. (IRS 905.G0)

3.4.1.2 Main Steam Line Break Re-Analysis at Millstone 2 (PWR)

In October 1991, the containment response to a MSLB was re-analysed in preparation for a planned SG replacement at Millstone unit 2. This re-analysis revealed that the assumptions made for the existing MSLB analysis (1979) were non-conservative with respect to power level, break size, and single active failure. Using more restrictive assumptions, design limits could be exceeded for containment pressure, and temperature.

The nonconservative assumptions were not discovered until the MSLB was reviewed to evaluate the impact of the planned SG replacement. That review revealed that the root cause of the event was an incorrect assumption, made in the FSAR analysis, that the limiting condition for the containment response associated with a MSLB, was not zero power. This assumption was based on the judgement that at hot zero power the steam generators
contain the largest inventory of hot water and thus resulted in the largest discharge to the containment. (IRS 1270).

3.4.2 Emergency Electrical Power Sources

Examination of the following events highlights that the numerous design deficiencies affecting EDGs operability and potential availability are shared by problems related to:

- overloading,
- EDGs cooling,
- failure of control logic to respond to sequences involving LOOP coincident with, safety injection (SI), seismic event or fire, or delayed LOCA.

Most of these deficiencies would have resulted in the loss of EDGs redundant trains. In one case EDGs power control supply did not meet the single failure criteria.

Among corrective actions, it is worthwhile to notice that Fort Calhoun instituted a System Engineering programme. One of the main function of the System Engineer assigned to the EDGs is to specifically ensure adequate testing and reliability of the units is maintained through trending and analysis of equipment history. Such initiative would deserve special attention from other NPPs.

3.4.2.1 Overloading and sequence logic deficiencies

In June 1986, at Turkey Point NPP (PWR), the licensee performed an analysis of failure modes and effects. This analysis performed by the licensee for units 3-4 identified multiple design deficiencies in the ac vital power system which could potentially result in overloading and a concomitant loss of both emergency diesel generators (EDGs) for a unit. In addition, the analysis revealed another deficiency that could result in the loss of all ac power to unit 4. (IRS 717.00).

On April 14, 1987, at Sequoyah NPP (PWR), the licensee prepared a report of an internal condition adverse to quality as a result of design reviews performed to ensure that adequate calculations existed to support the design basis of the plant. The report addressed calculations of voltage, current, and load for the class 1E electric power system. Before this report was prepared the effect of the fire pumps operation on safety-related equipment had not been considered. Fire pumps are powered by class 1E buses that automatically transfer to the EDGs in the event of a LOOP.

The fire protection heat sensors inside containment start the fire pumps upon detecting temperatures greater than 100°C. Because containment temperatures can be greater than 116°C during a LOCA, starting of the fire pumps would be expected to start; however starting the fire pumps concurrent with a LOCA could potentially degrade the voltage of the class 1E buses and prevent safety-related equipment from performing its intended function.

The root cause of this problem was a design error. The design engineer realised that a fire concurrent with a LOCA was outside the design basis of the plant and that
containment isolation valves for the fire suppression system will close when a LOCA is detected. Therefore, the design engineer failed to recognize the possibility of inadvertent starting of the fire pumps during a LOCA and the effect of their operation on the normal and emergency power system. (GL 88-15)

On May 1, 1989, at Surry NPP (PWR), the licensee reported a deficiency in the EDG loading logic. This deficiency caused the EDGs to over-load if a LOOP occurred after a LOCA or other design-basis event. Such an overload would automatically start the safety system electrical loads. This sequence of events has not been considered in the design of the original EDG logic loading. Only simultaneous LOCA and LOOP conditions were used as the design basis for the EDGs.

During work on the improved technical specifications (TS) and through discussions with NSSS owners group, the NRC determined that other plants might have been designed to respond properly to simultaneous LOCA and LOOP conditions. However, those plants might not be capable of responding to other sequences which also result in a LOOP because of the characteristics of the particular design. A LOCA followed by a delayed LOOP, or a LOOP followed by a delayed LOCA may occur in various ways.

On May 25, 1989, a plant engineering design review of Unit 1 at Perry NPP (BWR), revealed a design anomaly in which ground faults on EDGs loads, coincident with a LOOP during a seismic event or fire could lead to the inoperability of more than one EDG.

At Perry Unit 1, each EDG was designed with a neutral ground circuit consisting of a high-impedance path from the neutral to ground, which limits ground fault current. The purpose of this ground path (in lieu of an ungrounded system) is to limit the build-up of high voltage stress during certain ground fault conditions that could ultimately result in the break down of the insulation of such components as motors and cables.

Ground faults are detected by sensing the voltage that is in the EDG grounding circuit whenever a ground fault exists in the electrical distribution system supplied by the EDG. In the Perry design, a voltage sensing relay would initiate a trip of the corresponding EDG whenever this voltage exceeds the relay's pick up value. This relay's contacts are bypassed in case of a LOCA. For non-LOCA events, however, a ground fault in any component, including non-class1E equipment, would have the undesirable result of shutting down the EDG.

This design raised the concern that a seismic event or fire could result in simultaneous ground faults in non-safety components supplied by all of the EDGs. Action by the protection circuitry at Perry could have shut down all of the EDGs, preventing them from performing their intended safety function. (IN 89-87)

In September 1991, at Doel NPP Unit 3 (PWR), as a result of a design review conducted during Decennial revision studies of the plant, the licensee realized that potential unavailability of EDGs existed in case of blackout following a safety injection associated with an improper temporation.
In this plant, a second protection level has since been designed in order to face to external accidents. The involved systems are contained inside a bunkered building. When a safety injection occurs, (first and second level) EDGs are started but remain uncoupled. The electrical boards keep their usual voltage, and the utilizers are not unloaded.

In case of a consequent LOOP, a black out signal is generated to ask for discharge of these electrical boards and their utilizers, which then coast down and build-up a residual voltage. After temporisation, the EDGs are coupled to the bunker electrical boards and the needed utilizers are sequentially switched on.

The EDG coupling temporisation corresponds to a 1-second delay introduced between the order of breaker opening for the offsite power supply to electrical board, and the order of EDG coupling to the electrical board. If the breaker opens slowly, EDGs may couple to an electrical board that is only minimally or not at all discharged electrical board resulting in a priority order of EDG shutdown. As a result, EDGs availability is not guaranteed following safety injection actuation in case of a LOOP. The EDG load increase, and in particular the risk of EDG shutdown under the conditions described above, had never been tested. To resolve this deficiency, the licensee implemented the following:

- addition of a 1-second delay for the EDG coupling after detection of effective breaker opening
- preoperational testing of the LOOP sequence following a safety injection signal scenario.

On November 21, 1991, over-loading and subsequent lock-out of electrical buses during accident conditions were reported at Indian Point NPP (PWR) for Unit 3. The vital buses could become overloaded during a LOCA as a result of emergency operating procedures (EOPs) directing operators to restore non essential loads if off-site power is not lost. This procedure would result in both emergency and non-emergency loads being powered concurrently from the same bus. The licensee's calculations revealed that performing this procedure could overload the buses. The resulting over-current condition could lockout a bus (i.e., de-energise the bus and prevent it from being re-energised from any source including the associated EDG). The scenario could disable redundant trains of safety-related equipment. (IRS 1284.00 and IN 92-09)

In 1991, a functional inspection of the electrical distribution system of Unit 2 at Indian Point NPP (PWR), determined that two EDGs shared a normal 125-Vdc control power supply. The condition had existed for 10 years before being discovered. (LER 247/93-007)

On November 4, 1993, at Beaver Valley NPP (PWR), Unit 2, the automatic loading capability of the 2-1 EDG on a safety injection (SI) signal failed during a similar test. Two days later, the automatic loading capability of the 2-2 EDG also failed during a test. This failure would only occur when an SI signal was present coincident with a loss of the normal power supply to the engineered safety feature (ESF) buses.

Operator action would have been necessary to allow manual loading of equipment on the ESF buses. The cause of the test failures was the misoperation of a digital solid state timer associated with the load sequencer circuit during the reset of sequencer operation.
failure mechanism had existed since November 1990 and was identified by an AIT as an inadequate design control. Engineering requirements and guidelines have been developed for the use of digital solid state components as a replacement for electrochemical or non-solid state components. The conditional core damage probability estimated for this event is 2.1.10-6 (LER 412/-012)

3.4.2.2 Inadequate cooling

On December 24, 1986, an incident on unit 1 at Brunswick NPP (BWR), involved a common cause loss of all four EDGs at a site as a result of a LOOP. The isolation of the cooling air supply in the EDG room as a result LOOP might disable the EDGs when they are needed to mitigate the LOOP. The potential for common mode failure resulted from the interaction with instrument air, a non-safety system. (IRS 741.00)

On December 1989, during a refuelling outage of the Nine Mile Point NPP (BWR) unit 2, while reviewing the service water system (SWS) control logic, the licensee discovered that a LOOP with concurrent loss of one of the two operating EDGs, could lead to a loss of the operating EDG as a result of inadequate cooling water flow from the SWS.

Similar deficiency, which could result in inadequate SW flow to essential loads, was also discovered at Cooper NPP (BWR). The control logic design deficiency existed at Nine Mile Point Unit 2 since the plant was constructed and was not detected by the licensee's pre-operational routine surveillance and post-maintenance/modification testing.

At Cooper NPP, the problem was identified during the construction and licensing phase, but station procedures were not adequately modified to mitigate the concern over pump run-out with a potential for loss of flow. (IRS 1050.00)

On September 13, 1990, high air temperatures resulted in failure of an EDG during a performance test at Fort Calhoun NPP (PWR). The other EDG was not subject to a similar test, but was identically configured. An investigation into the failure revealed that components in the generator exciter circuit had overheated and failed because they were located in a non-vented cabinet. Similar incident had occurred on June 25, 1990, during a full load test on an EDG.

A root cause analysis of the exciter failure was initiated concurrent with a design engineering assessment of the high temperature capabilities of the EDG cabinets. The EDG vendor designed and subcontracted the cabinet construction, and apparently did not incorporate the appropriate ventilation requirements into the design. This analysis revealed that the root cause of this condition was improper design of the exciter cabinets. A contributing factor to the duration of this condition was the failure in previous years to identify the cabinet overheating as the probable cause of a history of static exciter component failures at Fort Calhoun NPP.

The cabinet design deficiency created a common mode failure potential that could have prevented both EDGs from performing their safety function following a DBA. This condition was outside the plant design basis and had likely existed since initial plant start-up.
The conditional probability of core damage associated with this event is 6.5 10-5. (LER 285/90-025)

Among the corrective actions, the licensee instituted a System Engineering programme at the plant. One of the main functions of the System Engineer assigned to the EDGs is specifically to ensure that adequate testing and reliability of the units is maintained through trending and analysis of equipment history.

On April 22, 1993, during a surveillance test at Quad Cities NPP (BWR), the swing diesel generator cooling water pump (DGCWP) breaker locked up on antipump protection. The licensee determined that the potential for lock-up existed since the initial start-up whenever the pump power source was aligned to Unit 2. A modification implemented in 1992 ensured that the cooling water pump would be powered from Unit 2 if a LOOP occurred on that unit. Unavailability of cooling water for 5 to 10 minutes is sufficient to damage the EDG.

About 1 month earlier, inadequate bearing oil level was found in the Unit 2 dedicated DGCWP as a result of an incorrectly reassembled oiler. The pump would have been expected to fail if it had been required to run for more than a short time. The Unit 2 emergency power system was vulnerable to failure for a 7 month period beginning in August 1992.

The root cause for the ½ DGCWP not starting is a design deficiency in a bus breaker close logic that existed since the plant was originally designed. The problem was introduced during the installation of a modification in 1985. The conditional core damage probability estimated for this event is 6.0 10-5. (LER 265/93-010)

3.4.3 Auxiliary Feedwater System

Main lessons learned from the following events underlined the need to examine carefully the interfaces between non safety-related and safety-related equipment. and for utilities to investigate the adequacy and completeness of their design bases documentation

3.4.3.1 Failure to meet the single failure criteria

In February 1985, at Salem NPP (PWR), the licensee discovered that the low suction pressure trip circuits for the auxiliary feed water (AFW) pumps in Units 1 and 2 did not meet the single-failure criteria. The discovery resulted from an ongoing review of design changes in the AFW system, selected from various systems, which were being performed by the Safety Review Group.

The AFW pump low suction pressure trip circuits were installed by design change request in March 1982. The review of the design change revealed that a postulated short across contacts 1 and 2 of the circuit test switch would prevent operation of all three AFW pumps. The apparent cause of this failure was an error in design which resulted in an improper interface between non safety-related (control grade) and safety-related equipment, which resulted in multiple safety trains interface through a single device. (IRS 825.G2)
3.4.3.2 Inadequate net positive suction head

From August 16 to 22, 1989, the licensee for H.B. Robinson NPP (PWR) informed the NRC of various AFW pumps net positive suction head (NPSH) deficiencies on Unit 2. The licensee shut down the reactor on August 22. Design errors resulted in the supply header from the AFW tank being too small to provide adequate NPSH when the three pumps were operating simultaneously at rated conditions. This could lead to multiple pump failure as a result of cavitation.

The AIT dispatched for this event identified the following root causes for the slow recognition of the AFW NPSH problem identified by a self initiated safety system functional inspection (SSFI) at the end of 1986:

- a lack of design-basis information concerning simultaneous operation of the three AFW pumps
- a lack of priority assigned to the findings of an SSFI conducted from October to December 1986 (the initial priority assigned to the SSFI findings was lost when entered in the regulatory action item list for completion, although the NPSH concern was listed as significant)
- inadequate system operability criteria. (It was determined that equipment that performs its function is considered to be operable, even though it may be operating in a degraded condition or operating below design)
- insufficient communication and delayed management involvement.
(IRS 1054.00)

3.4.3.3 Deficiency in the containment penetration isolation valves

On September 13, 1990, in the course of resolving open items associated with design-basis documents at Fort Calhoun NPP (PWR) several conditions were identified as being outside the plant design since plant construction. An analysis of the AFW system piping between the containment penetration isolation valves showed that, in the event of a MSLB or LOCA inside the containment, the piping would be overpressurized because of thermal expansion of the process fluid between the closed valves.

The potential pipe failure could result in the inability of the AFW system to provide coolant to the intact steam generator following a MSLB.

This event was attributed to design and analysis deficiencies by the original plant architect/engineer company. The precise root cause could not be determined because of insufficient amount of information and documentation concerning practices and procedures used by that company.

3.4.3.4 Venting problems in the nuclear service water discharge piping supplying the auxiliary feedwater system.
In March and April 1992, at McGuire NPP (PWR), air pockets were discovered in the nuclear service water (NSW) discharge piping supplying the AFW system for both Units 1 and 2.

Specifically, the air pockets were discovered in the NSW system at the high points of the standby shutdown system line upstream of the isolation valves that separate the NSW and the AFW systems. This air could have potentially affected the operability of the AFW system since initial plant operation.

To correct the problem, permanent valves were installed to provide a continuous drainage flow sufficient to vent any air that might accumulate in the emergency feedwater supply. (IN 93-12).

3.4.4 Flooding, Seismic, Fire and Environmental Protection

Design deficiencies in flooding protection outside containment were identified at Beaver Valley Units 1-2 (PWR) in September 1986, at Trojan (PWR) in March 1987, and at Nine Mile Point (BWR) in December 1986. The following factors contributed to the deficiencies:

- inadvertent use of nonconservative assumptions in the flooding design analysis
- failure to recognise all possible flooding flow paths
- failure to install flood protection features determined to be necessary.

These deficiencies illustrate the potential for loss of safe shutdown capability as a consequence of flooding of the safety-related equipment outside the containment. (IRS 814)

During winter 1989, in preparation for a design change at the Millstone NPP (PWR), the licensee initiated a safety analysis which included analysing the effects of a failure of the house heating steam lines. During this investigation the licensee discovered that during a seismic event, a failure of the house heating system could potentially degrade some safety-related equipment needed to shutdown the reactor and maintain it in a safe condition while remove of residual heat.

The cause of the oversight was an incorrect conclusion drawn from the high energy line break study performed in 1973. That report concluded that an auxiliary steam line break was not relevant to safety-related equipment, and that the environmental conditions following any break would be of no consequence to any shutdown methods.

Similar concerns existed at Haddam Neck NPP (PWR). (IRS 1160.G0). In August 1990, the NRC issued IN 90-53, 'Potential failures of Auxiliary Steam Piping and the Possible Effects on the Operability of Vital Equipment'.

In January 1991, the Engineering and Construction Division of Electricite de France (EDF) initiated a review regarding modification on the AFW system of the 900-MWe reactor series. This review revealed that the AFW system was not designed to fully respond to the efforts induced by a safe shutdown earthquake (except at Fessenheim and Bugey). All AFW pumps had been installed on flexible bearing pads in order to absorb the vibrations.
engendered by their rotation; however it was discovered that, following a severe seismic event, the flexible bearing pads could involve travelling motions of the pumps with regard to the piping and lead to circuit deterioration. Corrective actions for this generic deficiency relied on implementing lateral stops in order to block the pumps horizontally with regard to the floor.

On July 26, 1991, at Washington NPP (BWR) Unit 2, an unanalysed condition was discovered on the fire protection and the safe shutdown capability for the plant. The licensee found that a fire in the control room could cause hot shorts, (i.e. short circuits between control wiring and power sources) for certain MOVs needed to shut down the reactor and maintain it in a safe shutdown condition.

If a fire forces reactor operators to leave the control room, the MOVs can be operated from the remote/alternate shutdown panel. However, hot shorts combined with the absence of thermal load protection could cause valve damage before the operator could shift control of the valves to the remote/alternate shutdown panel.

On November 20, 1991, after learning of the problem at Washington NPP, the licensee for Susquehanna NPP (BWR) determined, that a similar condition existed for both units of Susquehanna NPP. On December 10, 1991, a similar condition was discovered at the Monticello NPP (BWR). (IN 92-18)

In June 1992, the licensee for Tihange and Doel NPPs (PWRs) attempted to demonstrate the overall functionality of essential electrical equipment like MOVs and instrumentation sensors, considering globally the electrical connections up to the primary containment. During this attempt, the licensee found that the minimum requirements for the insulation resistance might not be met.

Most initial qualification test campaigns had been performed on single components but some important parameters had not always been measured (in particular the loss of insulation resistance).

Prototype circuits were submitted to a LOCA profile (after suitable ageing and irradiation) in a qualification loop. The results confirmed the adequacy of some circuits, but also the excessive losses of insulation resistance when unsealed terminal blocks were used. In case of a design-basis accident, leak currents might result in drift of measuring channels, leading to undesirable effects.

3.4.5 Component Cooling Water System

3.4.5.1 Deficiencies in the Line Connected to the Thermal Barrier of the Reactor Coolant Pumps

Following events are of particular interest since they indicate the way different design deficiencies leading to an non-isolable LOCA outside of containment, not addressed in the original design of different NPPs, were discovered in the line connected to the thermal
barrier of the RCS pumps. Specifically, these events underline the interest of an appropriate experience feedback.

On May 15, 1989, at Surry NPP, a design deficiency was discovered in the component cooling water (CCW) system. The deficiency resulted from underdesign in the relief capacity of the CCW lines connected to the thermal barrier heat exchangers on the RCS pumps.

Component cooling water flows through the thermal barrier heat exchangers inside tubes with an internal diameter (ID) of half an inch. Assuming a double-ended break of the half inch ID tube, a calculation modelled the reactor coolant flow upstream of the break and the flow out the break in the CCW system and predicted an in-leakage of approximately 275 gallons per minute (gpm). Since the CCW lines outside the containment were designed to pass only 167 gpm, failure to isolate the leak inside the containment or to provide adequate relief capacity could lead to a reactor coolant leak outside the containment building.

In July 1984, Westinghouse notified the NRC of a similar problem involving potential overpressure of CCW systems at 18 plants with Westinghouse-designed low-pressure CCW systems and recommended several corrective actions to prevent overpressurization.

Surry was not included with the 18 plants identified by Westinghouse because the CCW system at Surry was not designed by Westinghouse. (IRS 1052.00)

On August 5, 1991, at Palisades NPP (PWR), an evaluation Safety Analysis revealed that a postulated break in the reactor coolant pump integral heat exchanger could result in a primary coolant system leak outside the containment building. Radiological consequences of such a leak could exceed those specified in Title 10, Chapter 100 of the Code of Federal Regulations (10 CFR 100) within 90 minutes.

The postulated failure leading to an intersystem LOCA within the reactor coolant pump was not addressed in the original design basis of the plant.

This determination was based on Palisades specific calculations developed as a result of the review of IN 89-54, "Potential Overpressurization of the Component Cooling Water System", issued by the NRC after the Surry notification.

In January 1991, the same analysis suggested similar consequences at Palo Verde NPP (PWR). Specifically, an engineering review determined that the failure of a reactor coolant pump seal cooler could result in a non-isolable LOCA outside containment, if the cooler inlet or outlet valve to the reactor coolant system (RCS) could not be closed. These valves are not supplied with emergency power. However, the possibility of a tube rupture in the seal cooler was not considered in the original plant design. Instead, the design basis of the reactor coolant pump seal coolers described in the Combustion Engineering standard safety analysis report (SSAR) was that any leakage from the RCS would be detected by a combination of the nuclear cooling water system radiation monitors and the high surge tank level switches which have alarms in the control room. Once detected, the leakage would be isolated using the reactor coolant pump seal cooler isolation valves.
On February 5, 1993, during a shutdown for the 10-year inspection of Tricastin NPP (PWR) Unit 4, the licensee discovered that three isolation lift check valves in the CCW system of the thermal barrier of the RCS pumps were stuck in the open position.

This finding resulted from a verification campaign carried out at all sites following discovery in September 1992, of the blockage of these isolation valves in open position at certain sites. This campaign was prompted at the request of Institut de Protection et de Sûreté Nucleaire (IPSN) after an expertise revealed cracking affecting the coil casing of a thermal barrier during the ten-yearly inspection at Fessenheim Unit 2. IPSN took consideration of the potential consequences of such cracking in similar events at Zaporozhe (Ukraine) and at Fukushima Daini (Japan) reported respectively in IRS 6279.00 and 959.00 which led to the spreading of significant metallic particles though the RCS.

The blockage anomaly proved to be generic among plants in the 900-MWe and 1300-MWe reactor series.

None of these check valves had been inspected since the initial commissioning tests, because no provision had been made in the preventive maintenance programmes for their inspection.

In the event of a cooling coil tube failure in the CCW system, the stuck open lift check valve in the affected line would allow reactor coolant to penetrate upstream into the CCW system into the portion of the system that is not designed to withstand reactor coolant system pressure. This penetration could result in a LOCA that could not be isolated by the CCW cooling coil isolation valves either inside or outside the reactor building. The possibility of a tube rupture in the seal cooler was not considered in the original plant design.

To remedy this situation, temporary operating instructions were given to the operators pending the completion of repairs to the check valves.

The valve blockage anomaly evidenced a design error associated with the choice of unsuitable material for valve construction and which remained unknown a long time because of shortcomings in the preventive maintenance programmes (which made no provision for testing or inspection of the CCW cooling coil isolation valves), as well as delays in the feedback of information.

The discovery of the stuck open check valves should have prompted identification of a linkage between this malfunction and the fact that the valves had neither been tested nor inspected. In addition, remedial measures should have been introduced as soon as the first precursor events occurred. In fact, 3 years elapsed between the time at which the first malfunctions were detected and the subsequent notification of a significant incident. (IRS 1542.G0)

When comparing similar events described above, one may conclude that foreign experience feedback failed also to work satisfactorily. A careful examination of the deficiency in the thermal barrier cooling line design reported by Surry NPP in 1989 should have led to a
more questioning attitude, which could have permitted the licensee to detect the problem earlier.

Preventive maintenance and periodic testing programmes were implemented by EDF and approved by the DSIN. Subsequently EDF decided to replace the lift check valves with swing check valves.

In order to reduce the susceptibility of the thermal barrier casing to cracking, a new generation of casing has been developed and will be installed on-site from 1996 onwards.

In 1993, at Sequoyah NPP, eight check valves in the CCW supply to the reactor coolant pump thermal barriers were found stuck open on Unit1.(LER 327/93-029)

3.4.5.2 Deficiencies in Post Accident Containment Cooling Conditions

On September 13, 1990, at the Fort Calhoun Station (PWR), in the course of resolving open items with design basis documents, the licensee identified conditions involving the CCW, raw water (RW), and containment spray (CS) systems which placed the plant outside its design basis for post-accident containment cooling as defined in the updated FSAR and the basis for technical specifications (TS):

- the CCW conditions involved the potential for degradation of containment air cooler performance and/or loss of CCW system operability following a loss of instrument air.
- the RW conditions involved the inability of the RW system to provide backup cooling for the containment air cooler.
- the CS conditions involved the potential for the loss of operability of a single CS pump following a single active failure of an EDG.

3.4.6 Residual Heat Removal System

On January 22, 1992, at North Anna NPP (PWR), the licensee reported that the residual heat removal (RHR) relief valves would not pass the design-basis flow to relieve an overpressurization of the RHR system. The function of these valves is important when the RHR system is aligned to the RCS and when the RCS is solid. In such situations, the RHR system is susceptible to overpressurization, such as from a charging-letdown flow mismatch or a temperature change.

The licensee reported this condition after conducting an engineering evaluation to respond to a 1990 dated notification by Westinghouse recommending to its customers to review the following three items:

- adequacy of the RHR relief valves for protecting against cold overpressure events
- discharge capability of relief valves for probable back pressures
• design basis commitments for valve specifications, as well as commitments in the FSAR and TS. (IRS 1377.00)

3.4.7 Containment Integrity

Insufficient instrumentation to accurately determine reactor building differential pressure and failure to take account of interaction between containment environment and the motors and valves of the containment air return system are respectively the two deficiencies that had the potential to impair containment integrity in a postulated accident.

In November 1987, the licensee for Nine Mile Point NPP, notified the NRC that since plant began operation, the secondary containment of Unit 2 had not been maintained at the required sub-atmospheric pressure at higher building elevations because of a phenomenon not considered in the design of the secondary containment pressure control system. Specifically, the design of the system did not account for the temperature-induced differences in the pressure gradients inside and outside the containment. As a result the installed instrumentation was insufficient to accurately determine reactor building differential pressure at higher elevations.

In a postulated accident, whenever outward positive pressure existed across the secondary containment boundary, a potential existed that the leakage prevention function of the secondary containment might be negated. In such cases, all primary containment leakage could be released directly to the environment, exceeding the regulatory limits for fission product release. (IRS 926.00).

On February 15, 1991, a design review at McGuire NPP (PWR), identified that the plant’s containment cooling systems could exceed their cycle duty and become inoperable before completing their safety function following a LOCA. This potential could arise because of severe stresses on electric motors and electrically operated valves in the systems.

The review was performed by the plant’s Design Engineering personnel in response to a concern expressed by a McGuire Nuclear Production Engineer regarding the CS system pumps and the containment air return and hydrogen skimmer (CARHK) system during requalification training.

This event has been designated as a design deficiency because of unanticipated environmental interaction between the cycling of the fans and dampers with the cycle duty of the fan and damper/valve motors. The fans and damper motors were designed to cycle, and the cycle duty for each is known. It is also known that there will be pressure fluctuations in the containment during a LOCA. At that time, however it was not recognised that the interaction between the containment environment and the cycle duty of the affected motors could present a problem. (LER 369/91-006)

3.4.8 Service Water Systems

In November 1988, the NRC issued NUREG 1275 Vol. 3. a comprehensive review of operational experience of SWS failures and degradation reported by licensees from
January 1980 through June 1987, including various design deficiencies. Among these, the most significant deficiencies fall into 2 categories:

- potential single failure vulnerabilities of the system
- inadequate system flow to provide adequate cooling during a postulated design-basis accident

Many of the affected plants had operated for years (and a few for more than a decade) before the vulnerabilities were discovered.

On February 8, 1988, at Shearon Harris (PWR) Unit 1, during surveillance testing of the emergency service water (ESW) system the non safety-related portion of the ESW pump seal water supply system failed when the MOVs failed to close because of accumulated debris from the ESW raw water supply. Additionally a check valve downstream of one of these valves failed to seat properly.

The licensee raised concern that the seal water piping configuration may be vulnerable to single passive failure that could render both ESW trains inoperable.

The concern regarding the configuration of the safety-related ESW pump seal water supply is that the two trains are connected without the capability to automatically isolate, causing the potential for a single failure to affect both ESW pumps. As a result the seal water supply design did not comply with the requirements in the FSAR, which stated that the ESW system must be protected from passive failures. The conditional core damage probability associate with this deficiency is estimated to be $4.8 \times 10^{-4}$ (LER 400/88-006).

In November 1989, during a probabilistic risk assessment (PRA) of the emergency core cooling system (ECCS) at Haddam Neck NPP (PWR), the licensee discovered that a single failure of the SWS MOV to open in response to a LOCA could disable both RHR pumps. This single failure would cause the diversion of the cooling water flow from the RHR pump seal coolers resulting in inadequate seal cooling and possible pump failure.

This type of problem could occur in any auxiliary cooling water system that provides sizably different cooling needs to different redundant components such as RHR heat exchangers and seal coolers. The important feature in the system is the interconnecting piping between the auxiliary cooling water system branches and the piping to the individual components.

In the situation described here, a single failure of a valve in the SWS to open would cause one branch of auxiliary cooling water to be unavailable to service multiple redundant components, thereby reducing flow in relation to design requirements. This could ultimately cause RHR pump failure as a result of inadequate seal cooling. (IRS 1032.00)

3.4.9 Emergency Core Cooling System

As indicated by the following events, ECCS has necessitated a greater demand on design review than other systems: deficiencies including single failure of a component, inadequate NPSH, inadequate consideration in isolating valves design and installation, pipe
installation, have been the cause of potentially inadequate performance or unavailability of ECCS as well during the direct injection mode as the recirculation mode following a LOCA.

Many of these design deficiencies were generic and affected mainly PWRs; they were discovered by engineering evaluation or review of plant system subsequent to testing or operator observations. Most of them affected components that are run only during periodic tests. This emphasises the special attention that must be dedicated when analysing the operating experience of these components.

The plugging of emergency core cooling strainers which occurred during the Barseback incident deserves a special attention considering its generic implication for the vast majority of LWRs.

3.4.9.1 Low Pressure Coolant Injection Valve Single Failure Vulnerability

On July 30, 1992, at the Cooper NPP (BWR), the licensee discovered that the worst single failure in the ECCS had not been correctly identified during the analysis of a LOCA in conjunction with a LOOP. The licensee discovered the problem while performing a plant design-basis reconstitution.

The previous analysis by the licensee assumed that the worst case single failure was a failure of the low pressure core injection (LPCI) system injection valve in the ECCS train that is connected to one recirculation loop, concurrent with a pipe break in the other recirculation loop.

The licensee recognised that failure of a 125-Vdc bus that provides control power for the LPCI injection valve serving the unbroken recirculation loop is the worst single failure for this accident. (IN 93-28)

3.4.9.2 High Pressure Injection Pump Inoperability

At Oconee NPP (PWR) and Turkey Point NPP (PWR), potentially inadequate ECCS performance during recirculation operation following a LOCA were discovered. The design analysis was found to be inadequately performed for the recirculation phase following a small-break LOCA.

Subsequent engineering analysis indicated two deficiencies at Oconee:

- high-pressure coolant injection (HPI) pumps could be rendered inoperable by inadequate NPSH.
- a single failure of an ECCS switchgear during a LOOP could prevent the remote alignment of the LPCI system to the high-pressure injection system in the piggyback mode.

At Turkey Point NPP, inadequate NPSH for the CS and the SI pumps during the recirculation mode was caused by the throttling position of the valve at the discharge of the RHR pumps (which provide the flow to the CS and SI pumps). (IRS 915.G0-IN 88-74)
3.4.9.3 Hydrogen Gas Binding of Low Pressure and High-Pressure Coolant Injection Pumps During Direct and Recirculation Modes

Numerous events related to gas binding problems occurred although the hydrogen build-up problem in the high pressure safety injection (HPSI) pumps suction lines was early recognised.

Corrective actions were inadequate because of a design deficiency in the modification. In one case the licensee failed to identify the problem after industry notification.

On July 9, 1990, an engineering evaluation performed at Haddam Neck NPP (PWR) revealed the existence of a deficiency that could disable both centrifugal charging pumps during a LOCA. While the plant was shut down, the licensee discovered that water was draining from the volume control tank (VCT) at a rate of 10 to 12 gpm when the VCT was pressurised to approximately 30 psig. The licensee after contacting the valve vendor, learned that, two solenoid isolation valves (SOIVs) installed in the vent line during the 1989 refuelling outage would not stop flow in only one direction, from the charging pump suction to the VCT and would unseat with a differential pressure of 15-30 psig in the reverse flow direction.

When the VCT pressure was higher than the charging pump suction pressure, these valves would not prevent draining of the VCT. This could result in hydrogen accumulation in the charging pump suction line and gas binding of the charging pumps during a LOCA.

The licensee also identified a second scenario involving the recirculation phase of a small-break LOCA, when the RHR pumps supply reactor coolant from the sump to the suction header of the charging pumps. which would allow a release of reactor coolant outside the containment. The conditional probability of core damage estimated for this event, during power operation, is 6.0 10-4. (LER 213 / 90-008)

Following this event, the NRC issued IN 90-64 'Potential for Common-Mode Failure of High Pressure Safety Injection Pumps or Release of Reactor Coolant Outside Containment during a Loss of Coolant Accident'.

In 1980, Westinghouse determined that HPSI pump suction lines were susceptible to gas build-up, and the architect engineer designed a venting system containing two SOIVs with automatic isolation capabilities. The SOIVs were oriented to isolate flow from the VCT to the HPSI pump suction line.

In 1982, the licensee implemented a modification to reorient the SOIVs in the opposite direction. The modification was based on these valves being incorrectly oriented in the original design.

On August 22, 1990, while troubleshooting a gas bound centrifugal pump at Sequoyah NPP (PWR), Unit 2, the licensee discovered that substantial accumulation of hydrogen existed in the charging pump suction header and in a recirculation supply line from
the RHR system to the charging pump. In fact gas quantities were sufficient that successful performance of the safety injection and charging pumps could not have been guaranteed, particularly for recirculation modes. The conditional probability of core damage associated with this event is \( 6.0 \times 10^{-4} \) (LER 328/90-012).

A special review team was formed to investigate the disposition of the NRC items to determine if the hydrogen problem at Sequoyah could have been recognised at an earlier date. The team concluded that the principal cause of the failure was incomplete review of IN 88-23, "Potential for Gas Binding for High-Pressure Safety Injection Pumps During a Loss-of-Coolant Accident".

On October 11, 1990, the licensee for Comanche Peak NPP (PWR), during a review of plant systems performed, in response to IN 90-64, discovered a similar design error. Specifically, as a result of discussion with the valve vendor, the licensee determined that the SOIVs, when closed, would not isolate flow from the VCT to the HPSI pump suction.

The licensee therefore determined that original application and technical review of the design inputs for the SOIVs were not adequate. The SOIVs installed were not designed to isolate the flow in both directions. Subsequent review of all design conditions applicable to the SOIVs either failed to consider all flow conditions for the SOIVs, or failed to consider that the valves were not designed to isolate the flow in both directions.

On March 26, 1991, the licensee for Comanche Peak Unit 1 (PWR) reported an additional event involving hydrogen-induced charging pump damage which occurred in October 1990.

Specifically, the licensee reported that ultrasonic examinations of the chemical and volume control system (CVCS) suction piping performed revealed voids in the alternate boration line and the gravity feed line from the boric acid storage tank (BAT). The ultrasonic examinations were performed following a recommendation in a letter (dated October 25, 1990) from Westinghouse in response to NRC IN 90-64 regarding the formation and venting of hydrogen in charging system piping.

Engineering evaluation indicated that the observed voids could exist following transfer of charging pump suction from the VCT to the refuelling water storage tank (RWST) during a safety actuation. Such voids would then cause damage to or gas binding of the centrifugal charging pumps when the BAT gravity line is used for boration, forcing the gas bubble into the suction header, or when the pressure conditions change (causing expansion of the bubble into the suction header). The unavailability may have existed since initial criticality, which occurred about one year before the event. The conditional core damage probability estimated for this event is \( 6.2 \times 10^{-5} \) (LER 445/91-012).

On April 16, 1991, with Oconee NPP Unit 2 (PWR) at full power, hydrogen was being added to the letdown storage tank (LDST). Upon completion of this operation, a non-licensed operator observed that the hydrogen supply had not been isolated when the fill-line solenoid valve was closed. After isolation, the LDST pressure exceeded procedural limitations, and the excess pressure was vented. Both trains of HPCI were declared inoperable because of the potential for hydrogen to enter the HPCI pump suction and damage the pumps following a LOCA.
LDST hydrogen overpressure is normally adjusted so that the borated water storage tank (BWST) will provide flow to the HPCI pumps during a safety actuation. In this situation, the higher BWST pressure seats the LDST outcheck valve and prevents hydrogen from expanding into the HPCI suction piping. During review of a 1971 Babcock-Wilcox curve of maximum LDST pressure as a function of inventory, the licensee determined that the curve was based on an assumption that the LDST would be isolated within 6.5 minutes for certain scenarios. However this action was not specified in the procedures. In addition, the single valve provided for this purpose was not safety-related and was not provided with safety-related controls or power.

Subsequent analyses by the utility, which considered flow-related pressure drops, indicated that hydrogen entrainment would occur if one of the BWST isolation valves failed to open. In this case, the additional pressure drop would allow hydrogen to expand into the HPCI suction lines and damage the pumps. The conditional core damage probability estimated for this event is 1.2 10-4. This deficiency has existed on all three Oconee units since initial start-up.

3.4.9.4 Failure of Low-Pressure Safety Injection Pumps and Containment Spray Pumps in Recirculation Mode as a Result of Air Entrainment

On September 3, 1993, following an application of the Safety Quality Assurance (SQA) approach to maintenance work on the SI and CS systems at Dampierre NPP (PWR), the operator of Unit 1, discovered a filling and venting fault in the recirculation piping of these systems. Among others, the SQA has the objective of specifying the requalification tests required to ensure correct operation of the system following a maintenance operation. In this instance, the SQA approach revealed that part of the recirculation piping of the SI and CS systems was not completely filled with water after completion of filling operations.

As a result air pockets in this piping could cause these systems to fail in the recirculation mode.

The analysis carried out by the operator revealed that two site teams shared the responsibility for the filling of this circuit's section since 1992:

The recirculation section from the sump to the closed isolation valve was filled with demineralized water by the maintenance team, since it carried out the earlier internal video camera inspection to verify the cleanliness of this section.

The section downstream from the check valve was filled with water from the RWST by the operations team. In addition, the operator's analysis revealed that the procedure used for this application did not account for the vent pipe downstream from the containment spray circuit recirculation check valve. This vent pipe was a modification implemented in 1984.

The generic character of this anomaly on the 900-MWe units (except the Fessenheim and Bugey units), was evidenced by inspections carried out on all other sites, although ultrasonic measurements in the piping showed appreciable differences from plant to
Following a LOCA, entrainment of air pockets during the recirculation mode, would reduce the pump hydraulic capacity on passage of the air pocket into the pump volute. Should the air not being vented from the volute, the discharge pressure would decrease and the flow rates required in this situation might not be reached; further reduction to below the pressure required to open the check valve downstream from the pump, would stop the flow and could lead to pump destruction by overheating. Moreover if the air pocket completely fills the volute, this would also lead to pump loss as a consequence of overheating.

Inspections revealed that both redundant lines in the same safety system could be affected by this anomaly. The increased risk of core damage probability for this event is estimated to 7.3 10^{-4}. Assuming that the two redundant lines in a single system are affected, the core damage probability would be then equal to the probability of the initiating events that result in the recirculation mode of these systems.\textit{(IRS 1582.G0)}

This event emphasises the importance that must be attributed to the preparation of interventions on parts of a system, like structures, that cannot be functionally tested. This is particularly true for safety features the availability of which rests only on the rigorous application of procedures.

3.4.9.5 Inadequate Relief Setpoints of the High-Pressure Safety Injection System

On April 10, 1991, at Millstone NPP (PWR), during testing of the HPSI system of Unit 3 while the plant was in hot standby, HPSI relief valve "A" lifted and would not reseat until the HPSI pump was stopped. An investigation determined that the incident occurred because of the relief valve set pressure was too close to the system operating pressure.

A similar condition existed with HPSI relief valve "B"; however, that valve was "gagged shut" during the test to prevent it from lifting. Had both valves lifted during accident conditions, the system would have been unable to perform its safety function.

The utility stated that the root cause of the event was a design deficiency. Specifically the HPSI relief setpoints were at values only slightly above normal operating pressure. Moreover, the system had historically operated close to the relief valve setpoint. The system design pressure was subsequently reanalyzed, and the setpoint of both train relief valves was increased to 2250 psia from 1765 psia. The conditional core damage probability of the event was estimated to be 8.1 10^{-4}.\textit{(LER 423 / 91-011)}

3.4.9.6 Emergency Core Cooling System Minimum-Flow Line Deficiencies

From 1985 to 1986, ECCS minimum-flow design deficiencies were reported at various BWR units (Brunswick 1 and 2, Peach Bottom 3 and Pilgrim 1) and PWR units (Point Beach, HB Robinson, Ginna, and Turkey Point). A single failure of a flow sensing instrument resulting in the loss of the minimum-flow path concurrent with safety injection would cause the safety injection pumps to operate ‘deadheaded’. Such operation would result in pump damage and failure within in a few minutes and would disable all trains of the ECCS.
The error most likely resulted from inadequate consideration of the effects of miniflow isolation during design of logic for determining the proper coolant loop through which emergency coolant would be injected following a LOCA. (IRS 654-720.G0-721)

On April 3, 1991, at the Shearon Harris NPP (PWR), the licensee determined that the high head safety injection (HHSI) system had been in a degraded condition during the previous cycle because of component damage in the associated minimum-flow system. Shearon Harris is equipped with three charging/safety injection pump each of which is provided with a normal miniflow path and an alternate minimum-flow path. During normal operations, the minimum-flow path is via the seal water heat exchanger back to the pump suction. During safety injection, this path is isolated, and two alternate paths are aligned via relief valves to the RWST. During testing, these relief valves were both found to be damaged along with associated piping.

The reported apparent cause was the existence of an air void, which remained in the HHSI associated minimum-flow lines following previous maintenance and testing by the plant operators. Additionally, the following design weaknesses were identified by the NRC special team inspection at Shearon Harris:

- the potential for water hammer events upstream and down stream of the relief valves had not been analysed.
- the associated minimum-flow system piping had not been analysed for transient or water hammer loads.
- the potential for relief valve chatter and setpoint drift had not been analysed.

Static testing to verify the valve lift setpoint had been routinely performed during the plant life time. However, testing to simulate flow through the valve to ensure proper operation and reseating apparently never was performed.

The loss of the HHSI function resulted from the use of pressure relief valves for the HHSI pump's mini-flow discharge lines, as well as the use of MOVs in the inlet lines to the relief valves, which caused the relief valves to be damaged by chattering. To resolve these deficiencies the licensee modified the design by removing the relief valves, installing flow restricting devices upstream from the MOVs, and changing the MOVs logic.

The NRC inspection team identified that it is questionable whether operators would have been able to detect and isolate the flow diversion from the HHSI system in a timely manner because of a lack of flow indication in the HHSI associated minimum-flow system piping and the lack of adequate instructions in the emergency operating procedures (EOP). The conditional core damage probability estimated for this event is 6.3 ×10−3. (IRS 1350.00)

3.4.9.7 Design Deficiencies in Installation of Instrumentation Taps on ECCS Lines

On June 22, 1991, during a routine test of the LPSI system, at Belleville NPP (PWR), with unit 2 shut down for refuelling, the licensee noticed a leak at the instrumentation tap at the discharge of a LPSI pump. The leak resulted from a circular crack in the weld
between the instrumentation tap and the main piping, and extended for 30 mm along the main pipe.

Following this discovery, extension of controls to other reactors of 1300-MWe series and other safety systems revealed similar cracking phenomena on medium pressure SI and reactor CS systems; approximately 30 cases of cracking spread over a dozen units involving 12 types of taps were found in the course of inspections. Theses cracks already showed significant circular lengths at the base of the tap and on extension of the main piping, they could have rapidly led to ruptures at the level of the tap.

Consequently, the cracks were considered precursors of failures following a LOCA. The origin of the damage was determined to be vibrational fatigue due to excessive loads as a result of the concentration of stress to the geometry of the taps.

Occurrence of one of several leaks on the piping located outside the containment would considerably complicate the management of a post-accident situation because of the difficulty in maintaining (simultaneously and overtime) the inventory of reactor coolant and the confinement of radioactive products.

Pending studies to implement a definitive solution, the cracked instrumentation taps were temporary reinforced in 1991 by a clamp type anti-vibration-device. The subsequent occurrence of new cracking on the instrumentation taps equipped with these clamps led EDF to develop a new assembly procedure. Clamps were disassembled and then assembled again.

The definitive solution involved replacing a length of the main pipe with a thicker pipe section on which a new welding pad and a shortened instrumentation tap are connected; this solution was implemented on the 1300 MWe-units from the beginning of 1994. Its extension to 900-MWe units was planned during 1995.

This anomaly revealed deficiencies, both of design and fabrication, in various lines and their taps, in the presence of vibrational stress. It also illustrated the limitations in the ability of the commissioning tests to recognise this type of anomaly and the necessity for further thinking in this area. (IRS 1200.G3)

3.4.9.8 Emergency Core Cooling System Switching Deficiency from Injection to Recirculation mode

On January 31, 1992, at Trillo NPP (PWR), investigation of a small leakage of borated water into the annulus during a refuelling outage, led to the discovery that some actuation of the ECCS were crossed at the protection system between trains. This happened in three out of four trains, and the affected safety feature was the inhibition, under certain conditions, of automatic ECCS switching from injection to recirculation phase during a postulated LOCA.

The safety significance of this deficiency, is that, in certain scenarios, included in the design basis of the plant safety analysis the unique train of ECCS suctioning from the containment sumps would be the broken line causing a discharge of coolant to the annulus,
where it is not possible to recover. In such scenarios, the plant safety would depend on the skills of the operators to understand the contradictory and confusing information offered by several monitoring systems, as well as their ability to investigate the real situation in a timely manner and take appropriate measures not included in any emergency procedure. The origin of this crossing was a design error by the NSSS, which was not discovered by neither start-up nor surveillance tests during 4 years of commercial operation. The event was not detected during the start-up tests because the goal of the test at that phase is to verify that the systems have been assembled according to design (being a design deficiency it was not detected). Moreover, the event remained undetected during 4 years of operation because functional tests were carried out ‘step by step’, the first step testing the analog section from the sensor to the logic cabinets to verify coherence among electrical trains, disregarding verification of sensor location. This was so because tests were carried out at one electrical redundancy at a time. Other parts of the protection system are tested in separate steps to verify coherence among electrical trains. Only an integrated test, based on a real increase of water level at the sector of the annulus or just at the sensor well, would have been able to detect the error. (IRS 1307.00)

3.4.9.9  Plugging of Emergency Core Cooling Suction Strainers

On July 28, 1992, a steam line loss of coolant accident occurred at Barseback NPP (BWR), unit 2, when a safety relief valve inadvertently opened. The steam jet stripped fibrous insulation from adjacent pipework. Part of this insulation debris was transported to the wetwell pool where it clogged the intake strainers for the drywell spray after about 1 hour, approximately 10 times faster than estimated. Although the incident was not serious in itself, it revealed a weakness in the defence-in-depth concept which under other circumstances, could have led to failure of the ECCS to provide water to the core.

Before the Barseback-2 LOCA, many European countries had followed the strainers-related guidance at Barseback NPP contained in US NRC Regulatory Guide 1.82, "Water Sources for Long-Term Recirculation Cooling Following a Loss-of-Coolant Accident", 1974. However, data obtained from European experimental programmes carried out in the late seventies to determine the performance of strainers indicated that this guide was not adequate. In addition, Swedish plant owners had used this guidance to judge performance of ECCS in their plants. Analysis at that time indicated that strainer clogging, if it occurred at all, would at least not occur during the first 10 hours after a LOCA. Since operation of the ECCS would be needed for a long time, backflushing capabilities and monitors of pressure drop across the strainers were installed in older Swedish BWR plants with small strainers areas. These actions were judged to be adequate compliance with the revised Regulatory Guide 1.82, issued in 1985. Consequently, international regulators and the power plant industry considered safety questions related to strainer clogging to have been resolved until the incident happened in Barseback-2, which showed that clogging and loss of NPSH margin could occur quickly.

After the incident, the Swedish Nuclear Power Inspectorate (SKI) expressed great concern regarding the clogging of the suction strainers. SKI required that both units at Barseback should make modifications to ensure availability of specified water levels to the CS system and the low pressure core spray (LPCS) system. Approximately 80% of the mineral insulation in the containment has since been replaced with metallic insulation. Also larger suction strainers have been installed in the systems mentioned above.
The Barseback-2 incident spurred immediate action on the part of regulators and utilities. Research and development programmes of varying intensity were subsequently launched in many countries; in several cases, these programmes yielded findings that earlier strainer clogging data was incorrect because essential parameters and physical phenomena (such as insulation ageing) had not previously been recognised. Such programmes resulted in substantial backfitting being carried out for BWRs and some PWRs in several countries. (OECD/CSNI/ PWG1 International Working Group; 'Knowledge Base for Emergency Core Cooling System Recirculation Reliability' 1996).

3.5 Inadequate or Incomplete Testing

Many events relate to the inability of in-service testing (IST) to identify deficiencies in a timely manner. In depth review of these events shows that test programmes and procedures were incomplete or inadequate. The following factors, alone or in combination, contributed to delays in discovering the deficiencies:

- inappropriate prerequisites
- wrong initial configuration
- tests performed in an inappropriate mode
- operability requirements absent from TS or not sufficiently rigorous
  operating conditions different from those that would exist at the time a
  component would be required to perform its design basis function
- IST requirements established with the unique scope of identifying trends in the
  operation of the tested components
- unforeseen interactions between systems.

Many instances are reported of testing logic methods that may not completely test the functionality of a safety-related component because they failed to verify testing overlap.

Moreover, many deficiencies remained undetected because of insufficient assessment of differences between plant conditions during testing and those expected to exist when the equipment is required to perform its function, before accepting the tests results.

Effectiveness of IST relies also on the pertinence and quality of information obtained during the tests, with emphasis on the following factors:

- collecting and reporting anomalies that occur during testing
- implementing appropriate instrumentation identifying causes of components
  malfunction
- developing and implementing programmes for trending specific parameters that
  affect component operation in order to predict performance degradation
  (development of diagnostic tools).

This underlines the need to enhance existing test programmes and procedures in
order to render them more comprehensive and to implement appropriate instrumentation and
monitoring or diagnostic techniques for trending component performances. An effective IST
programme should prevent failures to occur.
Among the inadequate testing related-events, two events: with an associated conditional core damage probability of 1.0 10-4 have been selected as precursors, one is related to the unavailability of emergency power to the AFW and CCW pumps after a LOOP, and the other to the potential loss of ESW to 2 units.

3.5.1 Motor-Operated Valves Testing

Events related to deficiencies of gate valves involving pressure locking and thermal binding represents a potential common-cause failure, that could render redundant trains of certain safety-related systems or multiple safety systems inoperable. Such events have been voluntarily omitted from this study for two reasons. First, these events were largely developed during a recent NEA/AIEA joint meeting. Second, valve surveillance testing may not detect the susceptibility of inadequately designed valves to these failure mechanisms. Such tests are normally conducted during either refuelling outages or normal operating conditions in which thermal binding and pressure locking phenomena do not exist. Most of these effects occur during infrequent plant evolution such as heat-up, cool-down, and rapid depressurization.

In many cases, a comprehensive evaluation is needed to determine susceptibility to the binding mechanism for a gate valve. This often requires detailed analyses involving transient conditions and some unknown factors, which may need conservative assumptions to demonstrate that the analyses are adequate and complete.

Nevertheless, the potential for valve inoperability caused by pressure locking and thermal binding has been known for many years in the nuclear industry. Moreover, in spite of numerous communications issued in the past, pressure locking and thermal binding continues to occur in gate valves installed in safety-related systems. Such occurrences were still reported in 1995 by the licensee for Haddam Neck NPP who had previously evaluated these valves for possible pressure-locking and thermal-binding and had concluded that the valves were not susceptible to pressure-locking problem. (IRS 1525.00)

It is worthwhile to examine the findings of an NRC survey of six selected US plants reported in IRS 1391.00. Such examination yields the following abilities:

- understand the past and recent licensee evaluations and corrective actions concerning gate valve pressure locking
- identify any nonconservative or incomplete aspects of these licensee assessments.

This survey showed that the scope of licensee reviews varies widely because there are no uniform guidelines:

- some completed their reviews based on engineering judgement without analysis
- others used engineering analysis, but the methods may not have been comprehensive or conservative

36
most licensees surveyed did not initially consider the problem as being credible based on a limited assessment. Some did not implement corrective actions after the potential problem had been identified.

The potential for valve locking has not been fully evaluated or corrected for all system operating modes, transients, or infrequent plant alignments. Oversights exist in design either or operation, but remain undetected because of insufficient instrumentation to provide feedback on the system status. Improving detection techniques and valve operation analysis remains a major concern for licensees and regulatory organisations.

3.5.2 Tests Never Performed

Containment isolation valves test in the emergency cooling system not included in the IST programme.

In September 1990, at Palisades NPP (PWR), the license reported potential problems resulting from the leakage of isolation valves in emergency cooling system recirculation to the safety injection water and refuelling tank, which is vented to the atmosphere.

A plant safety review committee determined that excessive leakage from these valves, leak tightness of which was never verified at the plant, could result in radiological doses at the site boundary and to control room operators exceeding regulatory limits. Since such leakage was not considered during earlier analyses, this condition was considered a non-reviewed safety question with respect to the valves.

Fort Calhoun NPP (PWR) reported a similar concern on August 19, 1991. To resolve this concern, the licensee implemented procedures to lessen the consequences of valve leakage, and leak rate testing of these valves was included in the IST programme. IRS 1240.00.

3.5.3 Unforeseen Interactions and Incorrect Initial Configuration

3.5.3.1 Procedural deficiencies resulting in incomplete testing

On October 25, 1988, at Zion NPP (PWR), with Unit 1 at 50% power and unit 2 in refuelling outage, the licensee reviewed the results of a procedure performed on unit 2 to confirm the availability of emergency power to engineered safety features (ESF) components. By simulating a LOOP that procedure verified that the EDGs correctly start and that ESF components are correctly sequenced onto their respective buses.

During this review, the licensee determined that the AFW pumps and component cooling pumps might not start on emergency power as required following a LOOP. This was determined by examining results of the test for ESF bus B, which supplies power to the B component cooling pump B. During the test, offsite power to bus B was removed per the procedure. Pumps A and B were observed to auto-start on low component cooling header pressure. This occurrence was in accordance with design, because component cooling pumps

37
received the low-pressure signal to start. Since an auto-trip signal was also present in the B pump circuit, that pump subsequently tripped on undervoltage per the test.

To prevent the breakers from cycling on and off, two signals (autoclose and autotrip) are concurrently received. In addition 4-KV ESF pump breakers have anti-pump feature that inhibit a close signal until the control switch has been placed in the after trip position.

In this case, the low header pressure signal cleared because pump A had started. This cleared the auto signal and pump B started on EDG power when sequenced on by the blackout sequence timer because the anti-pumping had been reset.

On reviewing the test, the licensee realised that pump A had started because it was powered from ESF bus A, which was not being tested. During an actual station blackout, both component cooling pumps would receive signals to trip on low pressure concurrent with signals to trip on undervoltage and would lock out as a result to anti-pump feature. As designed, this lockout would not clear even after the EDGs came up to speed and voltage and picked up the ESF bus.

The licensee further realised that the AFW pumps also have an anti-pump device. With the unit at power, however, a LOOP would result in reactor and turbine trips. The resulting shrinkage in SG level would cause the AFW pumps to receive the start signal on low-low steam generator level. In this case the anti-pump device would prevent the AFW pump from starting. Further investigations showed that a similar problem existed in the SWS.

Numerous factors prevented earlier discovery of the deficiency in this design:

Procedures used were performed at hot shutdown in a mode where SG level would never shrink during these tests, providing no opportunity for AFW autostart and subsequent lockout caused by the anti-pump. Because these tests were performed on a bus-by-bus basis, a component cooling or SW autostart signal on system level or pressure would be cleared by the other ESF buses, which are not being tested.

These factors prevented occurrences of component cooling or SW breaker lockout as result of the anti-pump circuitry during previous tests. However, receipt of IN 88-75, “Disabling of Diesel Generator Output Circuit Breakers by Anti-Pump Circuitry” sensitised the licensee to problems with anti-pump circuitry. The conditional core damage probability of this event was estimated to be 1.0 10-4. (LER 295 /88-019)

3.5.3.2 Procedural deficiencies masking deficiencies

On May 4, 1990, during a reactor building exhaust ventilation inspection at Duane Arnold NPP (BWR) Unit1, a licensee employee discovered a large hole in the duct. This hole allowed the main plant ventilation system to communicate directly with the reactor building ventilation system, thus bypassing the standby gas treatment system (SGTS) and providing a direct path for an untreated release of radioactive effluents into the environment.
The cause of secondary containment degradation at Duane Arnold was a design/construction deficiency compounded by inadequate surveillance procedures. Specifically the surveillance test procedural inadequacy resulted in operation of the main plant ventilation exhaust and major plant system fans during the test, which masked the break in the ventilation shaft. The procedural deficiency also masked the degradation of door seals, ventilation dampers, electrical penetration, and steam tunnel boot seals that occurred over the plant’s life. The faulty results erroneously assured the plant staff of an intact containment, when in fact the secondary containment integrity was degraded. (IRS 1092.00)

3.5.4 Tests Not Simulating Actual Conditions

In June 1990, while commissioning Unit 1of Golfech NPP (PWR), the operator fortuitously identified an anomaly in the control logic of the system for re-injection of nuclear service building effluents into the reactor building. Re-injection of radioactive effluents had been instituted within the framework of the post-TMI actions to limit the extent of contamination of the nuclear service building in the event of an accident.

In post-accident conditions, this re-injection is anticipated to confine radioactive products in order to recover possible leaks from the reactor building. The instrumentation monitoring the activity of the water collected in the sumps of the buildings would enable the operator to localise the leaks in order to isolate the concerned circuit or building. In case of activity detection on a sump of the nuclear service building, an automatism would shut down the pumps of the concerned sump and close the connecting valve to the waste auxiliary building. The operator would then re-inject the radioactive effluents in the reactor building by opening the injection valve and starting the pumps.

In many cases, the licensee found that the monitoring instrumentation did not correspond to the adequate sump; had there been an accident and a leakage in the safety system circuits during re-circulation, the anomaly would have failed to isolate the proper sump and would have led to extend the contamination to peripheral buildings.

This anomaly proved to be generic, since it was found in the most recent 1300-MWe units. The anomaly could have been detected earlier if the instrumentation detection automatism had been checked with a radioactive source simulating the actual conditions during the commissioning tests. (IRS 1187.G0)

On December 27, 1993, at McGuire NPP (PWR), MSIV B failed to close on demand on Unit 2. This failure would result in a dry-out condition of the associated SG during an event initiated by a LOOP followed by a safety injection. In this case, however, MSIV B closed fully following the event when a technician working on the valve loosened one of the yoke rod guides. In addition, analysis of transient data after the event indicated that MSIV A had also failed to close fully at the onset of the event and had leaked excessively.

Failure of the two MSIVs to close as designed was attributed to inadequate setting of clearances between the yoke rod guides and the yoke rods. These clearances should be set when the valve is closed and heated to normal operating temperature. Licensee procedures specified that clearances be set while the valve was at ambient temperature, and all testing was
done under cold conditions. The IST requirements did not include performing testing under the operating conditions that would exist at the time a valve would be required to perform its design basis function. Rather the current IST requirements, were intended to establish a monitoring programme for identifying trends in the operation of the tested components.

This event illustrates an example in which IST alone could not be relied upon to ensure operability of the MSIV. The licensee determined that additional testing, supplemental to that required by the IST programme, is necessary to verify that the valves are capable of performing their design basis function. (IN 94-44)

In October 1994, at Trillo NPP, as required by the Consejo de la Seguridad Nuclear (CSN), the licensee repeated the IST of the emergency 24-Vdc system and found that the reactor protection cabinets received 19.2 V (i.e., 2.3 V less than the design requirement of 21.5 V).

The Trillo FSAR postulated various conditions under which IST might take place. Among others, these conditions includes the following:

- one out of four E 24S buses in maintenance
- single failure in another

Under these conditions it is not guaranteed that, in case of a LOOP, the emergency batteries would be able to start the EDGs. Therefore, the core cooling safety was not guaranteed.

Analysis revealed that the event was caused by design errors motivated by insufficient use of applicable regulations and inadequate design control. These errors remained undetected because there was no measure of actual voltage drop. No regulation require these measures, therefore it is not expectable from the Engineering Company to have made them. No real functional tests were carried out (i.e., disconnecting the emergency 24-V dc system train from the power and verifying whether the battery is able to feed two trains until start-up and connection of the safeguards EDGs). Such tests, although not intended to measure voltage drops, provide confidence in system operability. (IRS 1506.00).

Corrective actions are part of a vast programme named ‘Operating Experience and System Analysis’ (AOES) examined in section 4 of this report.

3.5.5 Inappropriate Prerequisites

On May 19, 1992, at South Texas NPP (PWR), the operator discovered that testing of the switch contacts that directly actuate the shunt trip attachment of the reactor trip circuit breakers was not adequately conducted. These initiation contacts are actuated by either the manual safety injection or reactor trip switches and are the means by which operators directly actuate the shunt trip. They are also one of the two means by which the breaker is tripped; the other being the undervoltage trip.

The licensee had been performing surveillance tests of the safety injection switches and reactor trip switches without opening the associated block switch. If not opened,
the block switch allows the same manual switch contacts that actuate the undervoltage to indirectly actuate the shunt trip attachment. Therefore, the manual switch contacts are not independently verified as operable.

This surveillance inadequacy to verify the operability of the contacts in manually operated safety injection and reactor trip switches has also been identified at Callaway (PWR), Seabrook (PWR), and Wolf Creek (PWR). (IN 93-15)

3.5.6 Incomplete Testing

3.5.6.1 Failure to Verify Testing Overlap in Logic Testing of Safety-Related Circuits

In 1994, many examples of inadequate surveillance testing occurred in different NPPs. Many involved logic testing methods that may not completely test the functionality of a safety-related control circuit, as reported in IRS 1523.G0.

Although inadequate logic system functional testing of safety-related circuits has been the topic of numerous INs issued by the NRC (IN 93-38, IN 92-40, IN 88-83), licensees continue to report instances in which a particular component or section of logic has not been included in the testing. The complexity of some of these circuits, combined with a lack of understanding of the depth of the review required to verify the testing overlap, has resulted in continuing occurrences of inadequate test scope.

Reported problems include the following:

- failure to verify that all appropriate electrical loads were being removed from the buses before the EDGs powered the buses
- inadequate testing of permissive interlocks for the emergency bus undervoltage
- failure to verify that safety-related buses would properly deenergize and subsequently realign to the correct power sources
- failure to test one contact for a train of CS initiation logic because it was bypassed by the manual initiation push-button
- failure to verify initiation logic for a HPSI pump when the pump was being powered from either EDG
- failure to verify circuit breaker position interlocks used in the HPSI pump auto-start circuitry

Because ESF logic is tested during reactor operation when actuation of the system under test would be undesirable, the logic test must be broken into parts so that the system does not actuate. To ensure that no part of the logic is overlooked, the procedures for these partial functional tests must ensure that there is an overlap between the end of test section and the beginning of the next.

3.5.6.2 Failure to Verify the Operability of a Check Valve on the Reactor Coolant Pump Fire Protection System

On September 4, 1990, in the course of an in-service test at Gravelines NPP, Unit 1, the check valve isolating the reactor coolant pump fire protection system was found to have
been mounted in the direction opposite to that indicated on the side of the valve. This error resulted in the unavailability of the fire protection system.

An inspection revealed that the same anomaly existed on two out of the three reactor coolant fire protection systems at Cruas NPP, Unit 2. However, at Chinon NPP, Unit 4, the system's availability was unaffected since the arrow on the valve was pointing in the wrong direction.

The unavailability of the fire protection systems resulted from incorrect check valve alignment either during initial installation of the system or during reassembling of the valve in the course of a maintenance inspection.

The initial start-up testing campaign included full functional testing on the fire protection system installed in the reactor series reference plant in order to verify the design of the system. The spray nozzles in the other units in the series were then simply swept with compressed air injected through the nozzle located downstream from the check valves. Consequently, during both the start-up tests and all subsequent in-service tests, no air was routed through the check valves. The operator therefore failed to realise that some of the valves had been incorrectly installed. (IRS 1189.00)

3.5.7 Inability of Routine Testing Measurements to Identify Certain Failure Modes

As illustrated by the following instances, the routine pump surveillance tests, provided in the IST programmes, may not be capable of detecting early component degradation and there is the potential that degradation occurs without the awareness of the plant operators. The following events illustrate degradation caused by corrosion and flow recirculation problems.

On May 22, 1986, at Susquehanna NPP (BWR), an overcurrent alarm for an ESW pump was received in the control room of Unit 1 and the pump was declared inoperable. Subsequent disassembly of the pump revealed that the bottom portion of the pump suction bell had separated from pump body and fallen into the pump pit. In addition, the pump's impeller vanes were eroded through. Similar, but less severe, damage was found on the three other ESW pumps as well as the RHR pumps.

The licensee determined that the damage to the ESW and RHR pumps was caused by recirculation cavitation, which resulted from operation of the pumps at flows significantly below their design flow rate. These events illustrate that such damage occurred with slow deterioration of the pumps internals occurring over a long period.

During the early phases of degradation, the pumps were still functional and remained operable. The pumps had to be disassembled before the internal damage be seen. Therefore, routine pump surveillance tests, provided in the IST programmes, may not be capable of detecting early component degradation and therefore the potential exists that one pump may be run at low flow within the recirculation zone without the awareness of the plant operators.
On March 9, 1987, at Gravelines NPP (PWR), in the course of an inspection of the LHSI pumps of Unit 5, the results of an acoustic monitoring test of the pump bearings drew the operator's attention to possible degradation of the bearings on the two pumps of the unit.

Subsequent disassembly of the pump and examination of the bearings revealed signs that the pump bearings had been significantly damaged by widespread corrosion in an aqueous medium. According to the operator, this corrosion might have been caused by the flooding that affected pumps room following inadvertent draining of the component cooling system on November 26, 1984.

This incident raised questions concerning which parameters should be monitored during periodic testing, since vibration amplitude and frequency remained below the alarm and shutdown setpoints, as did bearing temperature. Since that event acoustic monitoring of bearings has become a specified requirement for all pumps and is included in the basic maintenance programmes. (IRS 846.00)

On March 3, 1994, while performing vibration tests on standby service water pump B, at Grand Gulf NPP (BWR), personnel noted that vibration levels at all monitored points were higher than the reference values. However, any degradation in developed head, flow, or vibration had been observed during quarterly IST.

The pump in question is a two-stage vertical line shaft pump with the pump impellers coupled to the pump motor via a segmented line shaft, approximately 18 metres long. Six couplings are used to connect the shaft segments. Disassembly of the pump showed extensive corrosion of the carbon steel bolts and lockwashers used in the pump shaft coupling assemblies. Some lockwashers were missing and were assumed to have corroded away completely. This allowed the gaps between the pump shaft sections to increase. Vibration measurements are taken near the motor bearing housing because the pump's bearings are submerged. However, vibration measurements taken at this location may not identify this type of failure mechanism until significant damage occurs.

Current manufacturer recommendation do not require "as found" measurements and evaluation of pump lift whenever the pump is uncoupled from the motor. This inspection has since been added to the IST programme. (IN 94-45)

3.5.8 Inadequate Calibration and Instrumentation Setpoints Evaluation

Many problems have resulted from errors in calibration and setpoints. The predominant evaluation of instrumentation of these problems arise in the following areas:

- use of unsuitable equipment
- improper calibration of instrumentation
- inadequate methods used to determine and evaluate instrumentation setpoints
- inadequate evaluation of instrumentation and control system modifications before implementation

Deficiencies in these areas were discovered during the following activities:
- actual system operation through the transients they initiated
- inspections of instrumentation and control system design modifications
- functional inspections of electrical distribution systems
- reviews of calibrating procedures

The role and contribution of inspections in the discovery of errors cannot be overemphasised. Many of the findings were identified during NRC inspections.

Some licensees operated equipment outside acceptable limits because they did not determine proper setpoints and did not evaluate and account for instrument drift. Operating the equipment under these conditions could compromise the safety functions of the equipment. This is particularly true for those instruments in which the licensee has determined the setpoints (as opposed to instruments for which the setpoints were determined by the architect/engineer or the NSSS). Setpoints not contained in the plant technical specifications were also found to be deficient.

The NRC found also that some of the licensees failed to verify that the magnitude of instrument drift assumed in the original setpoint calculation coincided with the magnitude of drift observed in the plant.

Left undetected, such errors might compromise the ability of an instrument to initiate a safety function before a process variable exceeds its safety limits and may create the potential for unanalysed situations as illustrated by the following instances:

- unit operating above the facility’s core thermal power limit at the Dresden NPP (IN 91-75)
- inadequate margin in case of small-break LOCA at the Vogtle NPP(IN91-75)
- non requested movements on the isolation valves of the pressurizer discharge lines during nominal power operation at the Chooz NPP (IRS 983.00)
- potential loss of ESW to both Catawba units
- MSRVs design opening pressure out-of-limit conditions at Ringhals Unit 2-3-4 (IRS 1550)

Moreover IRS 1140.00 reports a case where the HPCI system of Fitzpatrick NPP had operated with a setpoint that adversely affected its reliability for 14 years until several changes were made to the system.

Electrical distribution system functional inspections conducted in 1989 and 1990, at San Onofre (PWR), Susquehanna (BWR), and Waterford (PWR), revealed that under certain conditions, the voltage available at the safety buses would be inadequate to operate safety-related loads and associated equipment, these conditions could occur when a plant’s electrical distribution system supplied from an offsite grid that has become degraded but continues to supply voltages that remain above the setpoints at which the degraded grid relays would be activated. (IN 91-29)

On February 25, 1993, with Catawba Unit 1(PWR) at 100% power and Catawba Unit 2 in a refueling shutdown, three of the four ESW pump discharge valves failed to open during
surveillance testing. The licensee later determined that the torque switch settings for all of the ESW pump discharge valves were improperly set.

Four ESW pumps serve both units. However, during normal operation, only one pump is used. If the pump with the operable valve tripped, it would result in the loss of ESW for both units. When the licensee began IST on the B train of ESW pumps, the crossconnect line between the trains was closed. This depressurized the ESW header downstream from the ESW motor-operated discharge valves. When pumps 2B and 1B were separately started, their respective discharge valves failed to open. The failures were attributed to higher than expected torque to open the valves when the downstream header was depressurized. Consequently, the A train of the ESW was declared inoperable. When pump 2A was started, the actuator for the discharge valve tripped and reset several times before it finally opened.

The licensee conducted a study of the history of torque switch settings for the ESW valves and discovered that improper settings in 1985, 1989, and 1992 had affected the different valves. As a result, from August 1992 to February 1993, three of the four discharge valves were unable to open against full pressure. This resulted in a potential loss of ESW to both Catawba units, assuming a single failure of the one operable ESW pump discharge valve or failure of the single ESW pump associated with the operable valve. The conditional probability of core damage estimated for this event is $1.2 \times 10^{-4}$. (LER 413/ 93-002)

3.6 **Inadequate Control of Modifications to Safety-Related Systems**

Often modifications are introduced with the intention of increasing the reliability of safety systems. However, because of incomplete review and testing, these changes did not fully achieve the intended results.

The following events highlight the importance of thoroughly reviewing any safety-related design change, including considering the effect of the change on all related systems. These events also show the need to completely test the systems affected by the design change under conditions that simulate as nearly as possible those conditions that are expected to exist when the systems are needed.

It is crucial to assess differences between plant conditions during testing and those expected to exist when the equipment is required to perform its safety function, before accepting the test results. This may lead to appropriate compensatory dispositions. Even minor modifications to safety-related components may have major consequences for system operation affecting adversely the safety of the installation. This is particularly true if such consequences may not be detected during periodic or requalification testing following routine or non-scheduled maintenance operations.

In one case, functional requirements for MOVs changed, during the commissioning phase, as a result of a design change. However, the new functional requirements were not accompanied by subsequent verifications to check the impact of the change.
In another instance, a like-to-like component replacement which apparently, did not require testing according to the TS, led to the discovery of an anomaly and subsequently contributed to change the TS. Another instance involved an anomaly and led to increase a test frequency as a result of individual differences of components assumed to have identical dimensions.

Two events have been selected as precursors with estimated conditional core damage probabilities of 3.2 10-5 and 2.1 10-6.

On April 4, 1989, at Zion NPP (PWR), the licensee inadvertently created a deficiency in the turbine-driven AFW pump cooling water system of Unit 1 while modifying the AFW turbine to satisfy the ac independence criterion. The modification changed the pump’s cooling water supply from service water to leak-off from the fifth stage of the AFW pump. If the AFW pump suction was aligned to its emergency source (service water) rather than its normal supply (the condensate storage tank), the suction pressure could increase to 90 psig. Since the pump cooling water pressure was regulated to 75 psig and returned to the AFW pump suction line, this would have resulted in the loss of cooling water flow to the AFW, eventually causing the overheating and ultimately failure of the pump turbine. (IRS 1053.00)

On August 21, 1991, at the Loviisa NPP (PWR), in a discharge test of a pressurised water tank of the ECCS during annual maintenance of Unit 1, the licensee discovered that the check valve between the tank and the reactor pressure vessel did not open sufficiently at the tank’s hydrostatic pressure. In the 1988 annual maintenance, the licensee had modified the housings of the axle seals of the valve in question to enhance structural reliability. Components had been sized according to the design drawings since all valves were assumed to have identical dimensions.

However, individual differences between valves caused the gaps of the axle sleeve of the valve in question to become too narrow. The first post-modification tank discharge test was performed late in the 1991 annual outage.

Based on the event, the licensee decided to test all tanks once in every two years instead of the previous interval of four years. Furthermore, a tank discharge test is always performed after extensive repairs and modification of the system components.

On September 18, 1991, at Cattenom NPP (PWR), while Unit 2 was operating at full power, the operator found that one of the two control panels for a protection system logic unit had been unavailable for a period of 52 minutes. These logic units form part of the reactor protection system (RPS). The redundant control panels trigger automatic actuation of the safety-related systems in the event of an accident. Each of the two logic units are connected to two independent electrical supplies.

When changing from one supply to the other, the operator was unable to re-supply one of the logic units because of incorrect calibration of a circuit breaker.
This fault resulted from a modification of the power supplies to the boiling detection panel, previously installed in channel B and reassigned to channel A, for which an electrical distribution box had been added. This box is supplied through a changeover switch from one of the protection panels. It includes two circuit breakers rated at 10 amperes, one supplying the channel A boiling detector, and the other re-supplying the panel of the channel A logic system.

This fault was discovered fortuitously by the operator of Cattenom Unit 2 when the changeover switch mentioned above was being used to change supplies (this caused the circuit breaker supplying the channel A logic unit to trip). Subsequent investigations showed that the two circuit breakers were set at 5A instead of 10A as provided in the modification specification.

Depending on the type of safety action called upon during an incident or accident, the presence of underrated circuit breakers could lead, to the loss of the channel A logic system. The safety of the unit would then depend only on the redundant channel B, which is capable of providing the safety function on its own. The fault also existed in Unit 1.

This incident demonstrates the importance that must be given to post-modification testability when modifications can lead to common mode failures. (IRS 1268.00)

On September 21, 1990, at Sequoyah NPP (PWR), while Unit1 was operating at full power, plant personnel heard aloud noise in the east steam valve vault. The control room indications, however were normal.

On October 8, 1990, the plant was shut down subsequent to a radiographic determination that the disc of one main steam check valve was detached from its post and swing arm and lodged in the valve. Discs, weighing about 600 pounds, also failed on two other steam check valves and were found lodged 500 feet downstream, in the MSL piping.

The cause of the disc failures was determined to be a fatigue failure of the post. A break in one of the three MSLs and the failure of a MSIV to close under reverse flow conditions would have resulted in an unanalysed condition. Also, the three failures involved a common cause, and all occurred in service less than 4 months after a modification involving welding overlay to correct and reduce wear of the post and arm.

The assessment of this incident by an NRC AIT found that the potential effects of the stresses produced by the welding modification were not evaluated in the licensee’s in their design change analysis. The vendor concurred in the repair method, and the licensee stated that they relied on this concurrence as sufficient basis for accepting the change, without ensuring adequate bases. (IRS 1164.00).

### 3.6.1 Incomplete Post-Modification Testing

On October 6, 1987, at TVO NPP (BWR), a turbine trip occurred on Unit 1. As a result, because of inoperability of the turbine bypass valves, a reactor scram issued along with opening of the system valves and the transfer of reactor pressure control to the control valves.
The reactor overpressure protection and pressure control system of TVO Units 1 and 2 comprises 10 relief valves and 2 quick-opening valves and control valves.

The motor-protection switches of the control valves also tripped during pressure adjustment. The valves switched on to manual control and remained in about a 15% open position. This position did not suffice to maintain the reactor pressure constant, which proceeded to rise it slowly. By restoring the motor protection switches several times after a trip, the licensee could gradually drive in the valves into open position.

The cause of the inoperability of the control valves was a modification made during the annual maintenance outage in 1987, during which the motor-protection switches of the control valves had been set to trip at a too low an electrical current value. The original setting from the manufacturer was not modified because the work plan was not checked by the experts of the TVO electrical office as it should have been. The error was not discovered because the valves were not tested in transient flow conditions after the modification.

In June 1988, at Loviisa NPP (PWR), the licensee noted that certain primary shutoff valves of the impulse lines of some pressure measurements of Unit 2 were in the closed position. These pressure measurements are related to the plant protection system signals, the function of which is to identify a leaking SG on the basis of a pressure difference, and to close the AFW lines that connected to it.

This situation was discovered in connection with the settlement of the reason for the comparison signal of pressure measurements. The valves were closed in refuelling shutdown during 1986 in connection with a modification of the impulse lines. The correct positions of the valves were not checked after the work as they should have been. All of the pressure measurements, with the exception of the aforementioned comparison alarm, had continuously given normal indications because of the looseness of the shutoff valves.

On October 10, 1991, at Arkansas Nuclear One NPP (PWR), during post overhaul testing of unit 1, the licensee observed that one of the HPSI pump was loosing its lubricating oil at a rate of more than 15 gallons per hour as a result of oil spraying from the bearings. The licensee found that the oil would always leak at this rate during emergency operation because of excessive oil pressure caused by simultaneous operation of two oil pumps that serve the HPSI pump. This condition existed since the plant began operation.

The bearings of the HPSI pump are supplied with lubricating oil by two oil pumps, one attached directly to the HPSI pump itself and the other a separate electric backup pump. Originally, the electric oil pumps were intended to be used during start-up of a HPSI pump or to replace a malfunctioning attached oil pump. The electric oil pumps could be started manually and would start automatically when the oil pressure decreased below a certain point.

This method of control is used when the HPSI pumps are used for normal reactor water make up. However, during construction, the licensee decided that the HPSI pumps would be more reliable if the electric lubricating oil pumps ran continuously during emergency operation. Consequently, the licensee modified the emergency controls to keep the electric oil pumps operating whenever an emergency safety features actuation system
(ESFAS) was present. Anticipating that the simultaneous operation of both oil pumps could cause excessive oil pressure, the licensee added an oil pressure relief valve to the oil system. However, the relief valve settings were not appropriately selected to prevent oil spraying from the bearings.

The required periodic pump surveillance tests were conducted with the HPSI operating in the normal makeup mode with only one pump running at a time. The effectiveness of the ESFAS signal was tested during each refuelling outage. However, the test only required verification that the test signal would actuate the HPSI system and did not result in the simultaneous operation of the two oil pumps for an extended time. As a result, neither of these tests revealed the oil leakage problem. The licensee estimated that an HPSI pump would have performed satisfactorily for only 80 minutes without operator action to replenish the oil or to stop the electric oil pumps. (IRS 1323.00 and IN 92-65)

In September 1991, at the River Bend NPP (BWR), the licensee discovered that the outlet valves for the hydrogen mixing system would immediately close if an operator attempted to start the system by opening these valves when a LOCA signal was present. An interlock prevented the mixing system fans from operating with the outlet valves closed. Consequently, the hydrogen mixing system would have been inoperable if a LOCA signal was present. This condition had existed since the plant was constructed.

The redundant hydrogen mixing systems each have two lines penetrating the drywell; an outlet line with a recirculating fan draws suction from the drywell, and an inlet line that allows diluted air to renter the drywell. Each of these lines has two isolation valves that are normally closed during plant operation. During construction, in 1983 the licensee added a LOCA interlock to the hydrogen mixing system to automatically close all eight of the mixing system valves upon receiving a LOCA signal. In 1984, the licensee revised the control logic for the mixing system valves to automatically override a LOCA signal when the operator opened the drywell inlet valves. However, the licensee did not provide this LOCA override capability for the outlet line valves.

The control logic to automatically close all of the mixing valves was provided to ensure that the drywell integrity would be restored if a LOCA occurred during a mixing system test with the valves open. Apparently, the LOCA override for the inlet valves was provided later to permit the drywell to be depressurized to clear a false LOCA signal that might be caused by a LOOP. The false LOCA signal could be generated by the drywell pressure rise that would accompany a loss of drywell cooling. Since the drywell could be depressurized without opening the outlet valves, the LOCA override was not provided for these valves. The need to open the outlet to operate the hydrogen mixing system was apparently not considered for this change. Normal testing did not reveal this design error because it was never conducted in the presence of LOCA signal. (IN 92-65 and IRS 1323.00)

On December 2, 1992, at Oconee NPP (PWR), with all three units at 100 % power, both emergency power sources (Keowee Hydro Units 1 and 2) were determined to be inoperable.

On January 29, 1992, Keowee 2, one of the two hydroelectric generators that provide emergency power to the Oconee Station, failed to start during a routine attempt to
supply power to the grid. The failure to start was caused by a mechanical failure of the antipump relay in a Westinghouse (type DB) circuit breaker. Corrective actions included replacing the existing electromechanical scheme with an electric 'antipump scheme'.

During the design review prior to the modification, Westinghouse expressed a concern that the closing coil could be damaged if it remained energised for too long. Because of this concern, each type-DB breaker was individually time tested before and after the modification to ensure that the electric new antipump scheme would keep the closing coil energised for the same time as the old electromechanical scheme.

On November 24, 1992, the licensee performed the annual Keowee emergency start test for both units. This test differed from the post-modification testing described above in that a loss of auxiliary ac power was also simulated. With no output from the battery charger because of the unavailability of auxiliary ac power, dc voltage (supplied only by the battery) was lower than during the post-modification testing.

During attempts to tie Keowee 2 auxiliary power to the overhead path (one of the two power paths from Keowee to Oconee), the Keowee 2 auxiliary power alternate feeder breaker could not be closed after the normal feeder breaker was opened. On December 1, testing demonstrated that the Keowee 1 auxiliary power alternate feeder breaker failed to close at low dc voltages. The testing indicated that the available dc voltage was inadequate to ensure closure of the breakers.

The utility stated that, under reduced dc voltage situations, the closing mechanism moves more slowly and therefore has less momentum. This reduced momentum was inadequate to complete the breaker travel for the actual dc voltage. The problem was corrected by increasing the time the closing coils were energised. In this case, the modification to the antipump relays in the breakers did not consider the reduced control circuit dc voltage, which would exist following a LOOP, when the battery chargers are not supplying the dc buses. The conditional core damage probability estimated for this event is 3.2 10-5.(LER 269/92-018)

On September 23, 1992, at Arkansas Nuclear One NPP (PWR), flow imbalances and degraded flow rates were discovered on Unit 2 during a full flow test of the HPSI system performed in response to GL 89-04, 'Guidance on Developing Acceptable In-service Testing Programmes'.

An investigation revealed that replacement stem disc assemblies on the system valves, supplied as like to like and installed as early as 1982, were not identical to the original assemblies. The TS for the plant did not require periodic flow balance testing, unless system modifications affected flow characteristics. The licensee did not recognise that the replacement stem disc assemblies were different from the original stem after changing the components. The licensee revised the HPSI flow testing procedure to require confirmation of satisfactory flow balance and capacity during each refuelling outage. (IN 93-13 'Undetected Modification of Flow Characteristics in the High Pressure Safety Injection System')

3.6.2 Inadequate Design Control and Insufficient Post-Modification Testing
In November 1986, at Nogent NPP (PWR), during the commissioning tests of Unit 1, with the reactor vessel open, the licensee found that the isolation valves on the minimum-flow lines from the SI pumps to the RWST were not leaktight. Because these lines which may be vented to the atmosphere, radioactivity could be released to the environment by this path. Leaktightness could be attained only by applying manual pressure to the gear motor flywheel. The same statement was made with the SI valves, which partially close the safety injection flow to the cold legs during the switch-over to injection to the hot legs.

Further investigations, carried out on the units of Belleville and Cattenom NPP, revealed the generic nature of the problem. Specifically, the problem was identified as an undersizing of equipment that affected the MOVs of the SI system and constituted a common mode failure in both trains of the SI system of all the 1300-MWe series units.

The undersizing fault was discovered during start-up of the eleventh unit of the 1300-MWe series (that is, after 4 years of operation of the first unit of the series). Moreover, the discovery was fortuitous, incomplete closing of the valves, non signalled in the control room, could only be detected locally.

From June 1987, it was established that this fault resulted from a design change in the SI system for the main injection lines to the hot and cold legs. The initial design provided for switching simultaneous injection 20 hours after the beginning of the accident and distribution of balanced hot and cold legs. Thereafter, studies led the licensee to adopt switchover to simultaneous injection 14 hours after the beginning of the accident with different flow rates to the hot and cold legs. The flow rates in the minimum flow lines were increased during the course of the project.

Undersized motorization in more than 30 valves of the SI system of the 1300-MWe series, resulted from a design change in the system without updating the parameters used for servomotors selection. This deficiency led the licensee to replace and requalify the valve actuators.(IRS 1062-G0)

The equipment had been ordered before the safety studies were completed. These studies resulted in changes to the functional requirements, which should have been accompanied by subsequent verification that the equipment ordered was still compatible.

The significance of the fault led the DSIN to address different requests to EDF concerning the following issues:

- sizing method used for valves, actuators, couplings and torque limiters fitted to design-basis loading
- developments undertaken or realised to implement MOVs diagnostic techniques, capable of correctly assessing, trending and evaluating valve failure modes.

In January 1993, the licensee for Ringhals NPP, Unit 4, discovered that the alarm for low temperature in the component cooling system did not actuate despite the temperature had decreased below the set-point 9 °C. Subsequent examination indicated that both pumps 3
and 4 were without alarm function for both low and high temperature in the system. Similar deficiencies existed at Unit 3.

The safety implication of these deficiencies is very limited, because redundant parameters in connecting systems will alert operators if out of limit temperatures are reached.

The cause of the latent deficiencies was assessed to be modification works during the 1988 annual refuelling outages, when the alarm function in both units was disconnected and not restored after the completion of the modifications.

The pumps were used as stand-by pumps from the time for discovery to the respective unit’s annual refuelling outage 1995, when correct connection of the alarm function was made.

On November 4, 1993, at the Beaver Valley NPP (PWR), with Unit 2 in cold shutdown, the licensee tested the train A, two-to-one EDG load sequencer. This sequencer failed to automatically load safety-related equipment onto the emergency bus. Two suspected relays were replaced, and the surveillance test was successfully repeated.

On November 6, 1993, the licensee continued the surveillance testing, focusing on the train B, EDG load sequencer. Again, the sequencer failed to automatically load safety-related equipment onto the emergency bus.

The EDG load sequencers control the sequence in which safety-related equipment starts after the EDG restores power when normal power is lost on the emergency buses. Timer/relays are used to load the safety-related equipment in six discrete steps during a 1-minute period. The same type of timer/relay is also used to reset the EDG load sequencer if a safety injection or a containment isolation phase B signal is received. Resetting the load sequencer allows the necessary ECCS to be loaded. The load sequencer originally used electro-mechanical timer/relays to generate the timed steps and sequencer reset function. The electromechanical timer/relays were replaced with microprocessor-based timer/relays during the second refuelling outage, in November 1990.

The actual cause for both EDGs sequencer failures was determined to be the intermittent misoperation of the new timer/relays identified by post-event bench testing of these relays. The new timer/relays were purchased as commercial-grade items and dedicated for safety-related service.

The root cause of the failures was inadequate design control before installation, and insufficient post modification testing following the installation of the microprocessor timer. The modification design data did not identify the potential for voltage spiking by the auxiliary relays, and did not translate that potential into electromagnetic interference requirements for the equipment purchase specification and the dedication testing specification. As a result of the inadequate design control, a common cause failure mechanism was introduced into the diesel generator load sequencers. The conditional core damage probability estimated for this event is \(2.1 \times 10^{-6}\). (LER 412/93-012)
To resolve this failure, the licensee instituted a variety of corrective actions. The most significant actions include an evaluation of the post-modification programme practices, and development of engineering guidelines that address engineering requirements for application of digital solid state components as a replacement for electromechanical or non-solid state components.

In January 1995, during the refuelling outage of Ringhals NPP Unit 2, the writing of a document for control of operational functionality of safety related components allowed the licensee to identify that periodical testing of the charging pump rooms cooling in accordance with the TS had not been performed since the refuelling outage 1988.

This testing had earlier been part of the testing of the charging pumps, because starting of the actual room cooling automatically resulted in charging pump swap. After implementation of an improved fire separation of the charging pump rooms, and installation of separate room cooling, made during the refuelling outage 1988, the above automatic function had been replaced by thermostat control of the cooling. The modification resulted in the automatic testing of the cooling function, earlier part of the charging pump testing, to cease. This modification had not been reflected into similar modification of the operating and test instructions.

The safety implication could have been a delay in identification of malfunctions in the cooling system. In case of safety injection, this event could have resulted in a reduced, but not insufficient, cooling of the charging pump motors.

After the verification of correct function of the cooling fans, the actual test instruction was updated including the annual calibration of the controlling thermostats.

During the 1995 refuelling outage of Ringhals NPP, Unit 1, RHR pump 2 was started and short thereafter stopped by activation of the short circuit protection. A control of the pump was performed locally without any finding, and the pump was restarted successfully. The electrical maintenance department could not under testing identify any failure neither on the engine itself nor in the relay protection.

During subsequent root cause analysis, the licensee identified that the pump main breaker had one short circuit protection, assumed earlier to be blocked because adjusted in blocked position, which probably had been activated when the pump was started. The analysis showed that the protection was not blocked in spite of its adjustment, but received a signal which, considering the protection inaccuracy, could be activated by the start current and thus stop the pump.

Since the 1990 refuelling outage, pump 2 had been started once or twice times a month without any problem. The same has been valid after the reported event. It is thus confident that it had been possible to restart the pump after the spurious stop, should a real demand have existed.

The failure mode could have also affected RHR pump 1 availability to start on demand.
The cause of the event resulted from preventive replacement of old breakers for several components performed in 1989 and 1990. The new breakers have 'built in' protection device. At the time of the replacement, the proper function of the device had not been identified which explains the poor adjustment of the protection relays.

As corrective action the protection trip set-point was increased to 320 ms in order to get enough margin compared with the start current. Both RHR pumps were then tested without remark. Other components with similar protection have been controlled and their protection relays adjusted to the same value. These components belonging to the containment cooling system, reactor component cooling system and service water system were later tested without remark.

In December 1995, Oskarshamn Unit 1 (BWR) resumed operation after having been shutdown as a consequence of the Barsebäck event in July 1992. An almost total verification of the condition of the unit has been carried out, as well as extensive modernisation work.

The reactor being defueled, in May 1993 the water level in the reactor pressure vessel was decreased as preparation for cutting and replacement of piping. Alarm for low water level was obtained at -2.3 m on two out of four level transmitters. This value deviated from the set-point which is -1.75 m.

The hypothetical consequence was that if a large LOCA was postulated, the reactor protection condition which isolates the emergency primary condenser had been triggered somewhat later than provided in the FSAR.

The cause of the latent failure was a calculation error for the theoretical calibration signal for the level transmitter. In 1989 the water level monitoring system of the reactor pressure vessel was improved by density compensation of the reference legs. The error has been latent because of the assumption that the calculated calibration signal was correct. Though the safety implication of the event was thus judged to be relatively insignificant the event shows that the post-modification test programme was not complete. Should simulation listings of the process computer have been examined, then had the error been discovered.

On July, 7, 1993, during reactor shutdown at St-Laurent NPP unit 1, the licensee found an orifice plate erroneously assembled on each of the three steam feed lines for the AFW turbine-driven pump and the emergency turbine generator set (intended to ensure safety injection at the primary system pump seals in case of LOOP).

These orifice plates were fitted in 1981 onto the steam pipe work used both for the carry-over to the AFW turbine-driven pump and for the by-pass of the MSIVs. The orifice plates which should have been fitted only on the by-pass line for isolating the steam pipe work of the MSS limited the drive of the turbine-driven pump without making it totally unavailable.

The requalification of the modification and the tests conducted until 1992, which were satisfactory failed to detect the assembly fault.
In 1992, under a further comprehensive IST programme, a test which was more representative of actual conditions was carried out for the first time, to make sure that the turbine-driven pump could feedwater to the SGs, starting from the reactor at power up to the conditions setting off the RHR system. This test failed because at a pressure of 11 bar, the turbine-driven pump could no longer be driven. On nearing safe shutdown, this would lead to premature loss of both AFW turbine driven pump and emergency turbine generator set and consequently to inadequate core cooling.(IRS 1594.00)

Prior to 1991, IST programme for the AFW system was not comprehensive, it did not include tests at low steam pressure. In addition quality assurance on a subcontracted work was deficient, the licensee failed to verify and detect the erroneous assembly of the orifice plates.

3.6.3 **Deficiencies in the Quality Organisation**

**Inversion in the Air Supply of Safety Relief Valve on Main Steam Line**

On November 10, 1993, at Tricastin NPP (PWR), the licensee discovered that the lines for air assistance of safety valve lift and closing were reversed on two SRVs of the same MSL of Unit 4. The licensee made this discovery the during leak repair conducted on the air supply circuit connection line of an air-operated SRV of the main steam system (MSS). A subsequent inspection performed at all other units revealed the same anomaly affecting several air assisted safety valves on Bugey Unit 2 and Gravelines Unit 5.

An analysis of the incident at Tricastin unit 4 showed that this air supply inversion would increase the lift pressure of two SRVs to an estimated value of around 100 bar (more than 110 percent of the design pressure for the shell side of the SGs (i.e., 83.3 bar absolute). The failure of two SRVs on the MSL during a category 2 (loss of condenser vacuum) or category 3 transient (total loss of steam flow without automatic reactor trip) would breach the design basis requirements considered in the safety analysis.

The inversion in the air supply for the safety valve lift and closing was related to a previous change performed in 1988. Until that time, connections between the head of the SRV and the compressed air system (for air-powered assistance to opening and closure) were accomplished by means of hoses of different diameters that were originally fitted with identical fool-proof connector implemented in the SRV head. However, when testing the set pressure of the SRVs, the licensee disconnected the hoses from the valve on the head side to allow connection of a test pump. Disconnection at the level of the nozzle presented a risk of the two air lines being reconnected the wrong way after the test.

In 1988, the licensee welded the nozzles to SRV heads in order to be in compliance with the original drawings; the licensee later suggested that the most likely explanation for the wrong air connection is that the fool-proof connectors on the air lines had been reversed before welding.

This incident revealed that quality organisation at the plant during the 1988 modifications for the welding the nozzles onto the SRV head, had failed to avoid the risk of connecting the air supply for the SRV in the wrong way. The periodic tests of SRV set
pressure, carried out during each operating cycle, also failed to detect the anomaly. These failures emphasise the importance of performing functional qualification tests each time maintenance work is performed on components. (IRS 1432.G0)

3.7 Improper Installation

In the IRS file there are events where original installation deficiencies have remained undetected for an extended period because of inadequate configuration control during the design, construction and start up phases. Insufficient quality organisation, and lack of management were the main causes of deficiencies resulting in potentially generic implications in post-accident conditions.

Functional inspections identified many deficient electrical terminations in safety-related components as a result of the licensee’s installation procedures. Failures involve multiple grounds in direct current distribution systems with potentially serious consequences. In a few cases these deficiencies caused actual damages to components.

Erroneous instrumentation installation has concerned a limited number of plants. However like the design deficiencies described in earlier sections of this report, most of the installation errors existed since initial plant start-up and remained also undetected during years of routine surveillance. Because of the absence of alarms, personnel would not be able to recognise in time when a required component becomes inoperable or is becoming deteriorated.

One event with an estimated conditional core damage probability of 2.8 10-4 has been selected as a precursor. An extra contact in a control circuit would affect two SW pumps to restart in case of SI.

3.7.1 Deficient Electrical Terminations in Safety-Related Components

Several deficiencies in electrical terminations in safety-related components have been reported at various plants. These deficiencies were discovered during functional testing, operability tests, before start-up, or events initiating transients. Had they remained non corrected, they would have jeopardised the ability of the components to perform their intended safety functions.

The following examples emphasise the need to carefully monitor the receipt, installation, and maintenance of safety-related components to their cable or wire terminations. They also identify the need for proper attention to wire terminations during installation, modifications and maintenance activities, this is particularly true for wiring operations involving error-risks with reduced control feasibility.

On October 19, 1987, at the Shoreham NPP (BWR), the licensee discovered that many of the installed termination lugs were inadequately crimped to the control wiring in 4;16-KV switchgear equipment manufactured by the General Electric Company. In some cases, the lugs could be removed by hand. Inspection of these lugs by the licensee led to replace 42 % of the 1400 installed lugs of this type.

56
The licensee subsequently determined that GE personnel had deviated from the crimp process described in their installation procedures during the manufacture of the equipment. Therefore, the insulation around the control wires was not properly stripped before being inserted in the lugs. (IRS 894.G0)

On January 19, 1988, the licensee for River Bend NPP (BWR), notified the NRC of oversized motor operator termination lugs for the motor lead conductors in three main steam shutoff valves and two feedwater isolation valves of Unit 1. One of these shutoff valves experienced a high current surge that tripped its motor overload heater during functional testing and prevented the valve from fully closing. During investigations, the licensee found two motor leads burned and the lugs were oversized for the motor lead conductors.

3.7.2 Multiple Grounds in Direct Current Distribution Systems

Direct current power systems provide control and power to safety-related valves, instrumentation, EDGs and many other components during all phases of operations, including abnormal shutdowns and accident conditions. Batteries have a designed capacity to supply power during a station blackout. However this capacity can be affected by unanalyzed loads in the form of multiple grounds which can cause indiscriminate operation of equipment with potentially serious consequences:

- unpredictable spurious operation of equipment
- inoperable equipment
- unanalyzed loads on batteries
- unanalyzed equipment failure modes that could be expected to occur during harsh environments attendant to accidents

The following list highlights multiple grounds in the direct current distribution systems that were identified during NRC inspections and remaining undetected during an extended period of use at operating plants:

Quad Cities Unit 2 (BWR) operated for a significant time with known multiple grounds on the negative side of the 125-Vdc system. When a momentary ground developed on the positive side, it caused a fuse to blow in the auto-start circuitry of an EDG thereby disabling the EDG for nearly 6 months.

Oconee NPP operated for nearly 4 months with the 125-Vdc system ground activated. The ground detection alarm system had not been calibrated since 1976 and was found to be inoperable.

At DC Cook NPP (PWR), a negative dc system ground existed for nearly 7 months before it was cleared. (IRS 932.G0)

3.7.3 Inadequate Configuration Control

On October 12, 1989, at Arkansas Nuclear One NPP (PWR), during a comparison of electrical schematics of Unit 1 with the actual wiring configuration for engineered safeguard
equipment, the licensee discovered a relay contact not shown on the schematics in the control room circuits for service water pumps A and C. An evaluation of the extra contact revealed that it would prevent closure of the feeder breaker for the affected pump if an ESF actuation signal occurred before or without a main generator lockout.

The extra contact in the control circuit would have affected the ability of the two pumps to restart if a safety injection was present and buses A1 and A2 had completed a slow transfer to an offsite source. This situation would exist if a spurious safety actuation signal occurred during power operation, or if a valid safety actuation signal was generated prior to main generator lockout, as would occur following a large-break LOCA. In these instances, the slow transfer of buses A1 and A2, combined with the extra contact in the "A" and "C" pump control circuits, would cause the "antipump" circuit in the breakers to lock out the closed circuit to the breakers, effectively disabling the two pumps. In addition a loss of service water could result in the failure of these systems to perform their function, which is necessary to safe shutdown of the unit and for accident mitigation.

The wiring error was determined to be the result of inadequate design control during the design, construction, and start-up phases of Arkansas Nuclear One. The conditional core damage probability associated with this deficiency was estimated to be 2.8 10^-4.(LER 313/89-028)

Because of the potential generic implications of this wiring discrepancy, Arkansas NPP initiated an action plan to inspect selected additional electrical equipment in the control room of both units.

On January 8, 1993, during a scheduled shutdown of Unit 4 of Cattenom NPP, the draining of the spray additive tank associated with the CS system led to discover a design fault in the installation of the bottom instrument tap connection of the low-level sensors in the CS additive tank. The draining was performed to allow work to be carried out on the CS tank mixing pump.

This design fault could lead, in the event an accident requiring actuation of the CS system, to the loss of the CS pumps by overheating as a result of air entrainment from the spray additive tank once this had been emptied.

The deficiency remained undetected during both start-up tests and IST because such tests consist to simulate a low level in the tank by isolating the tank from the levelsensing instrumentation lines.

This design deficiency proved to be generic to all 1300 MWe units. Subsequently the low level sensors were re-installed at a higher level.

This deficiency emphasises the need to establish whether test are representative of actual conditions. Differences between standard and tests conditions must be assessed if standard operating conditions cannot be reproduced during a test, and measures drawn up to compensate for such differences. (IRS 1586.G0)

3.7.4 Quality Organisation Deficiencies

58
Breaches in the Integrity of the ECCS Sumps

On January 1990, during the commissioning tests of Unit1 at Golfech NPP (PWR), the IPSN representative on the site during the commissioning tests discovered during a walkdown that the possibility existed for bypassing the filters installed on ECCS sumps located inside the reactor building. This possibility arose because clearances existed between screens and water level instrumentation and clearances between screens and concrete.

Different types of anomalies raised the possibility of introducing debris in the ECCS sumps. Potentially the debris could be of sufficient design tolerances, and could clog fuel bundles as well as the SI and CS systems during the recirculation phase following a LOCA. Such clogging would create a common mode failure of both the emergency injection and the CS systems. Further inspections and investigations on different sites revealed that this installation deficiency existed, more or less pronounced, in different 1300 MWe operating units (IRS 1124.G0).

Failure to recognise the safety significance of screen sump deficiencies showed a plant management unawareness with regard to these problems. Consequently, control of the sump screens and their structure was included in the IST programme of the general operating rules (GOR).

In 1993, breaches were reported in the integrity of the reactor building sump-bypasses to the sump screens and holes in the screens at Arkansas Unit 1 and 2, Susquehanna Unit 1, and South Texas Unit 1 (PWR).

Another late discovery, on September 9 1992, involved adhesive tapes that were left in certain piping of SI and CS systems since the construction of Cruas NPP, Unit 2. This anomaly was found to be generic to 900-MWe and 1300-MWe reactor series, necessitating extended controls to remove them.

These tapes served to ensure an inert atmosphere during welding operations of pipe assemblies. Under radiation, the tapes could be detached by circulating water and clog diaphragms and spray nozzles on ECCS piping.

3.7.5 Erroneous Installation of Instrumentation

As illustrated by the following events, erroneous installation of instrumentation could prevent personnel from recognising when required equipment becomes inoperable. Under these conditions, the equipment may remain inoperable for an extended period until its condition is discovered though testing or fortuitously.

At certain BWR, the steam tunnel is equipped with temperature detectors that initiate steam line isolation upon detection of a steam leak, based on either an increase in steam tunnel ambient air temperature or an increase in the temperature differential between the tunnel ventilation inlet and outlet. These steam tunnel differential temperature and ambient temperature sensors provide redundant methods for detecting leaks and isolating the main steam lines (MSLs).
In July 1988, at Susquehanna NPP (BWR), the inlet and outlet differential temperature sensing elements in Unit 2 were found to be reversed. Consequently, in the event of a leak, the instrumentation would sense zero or negative differential temperatures when in fact they should have read above zero both during normal power operation and in the event of a leak.

The problem at Unit 2 was further compounded by the fact that the thermocouples for sensing the inlet temperatures were not located in the air inlet but rather in the fan cooler room for the steam tunnel cooling systems. Consequently, even if the thermocouples were properly connected, the increase in differential temperature in the event of a steam leak would have been substantially less than the instrumentation trip set value.

The scope of the start-up and surveillance tests was too narrow to identify the location errors although these tests verified that the inputs were of the proper magnitude for a given steam leak or detected that they were reversed. During these tests and during years of routine surveillance, neither the technicians nor the operators recognised the zero or negative differential temperature readings as being abnormal.

Differential temperature thermocouple location errors were discovered at Nine Mile Point Unit 2. The two mislocated thermocouples were installed away from the inlet air stream instead of ventilation inlet air temperature.

On May 23 1991, at the Palisades NPP (PWR), a containment spray pump failed to start locally on two attempts during testing. Personnel confirmed that the control power lights (both in the control room and locally at the circuit breaker) were lit. An auxiliary operator removed the closing fuses, found them adequate, and reinstalled them. The pump started on the third attempt.

The fuse holder fingers, which connect the fuses to the circuit, had become deformed, such that no contact was made to close the circuit. The NRC therefore questioned how power lights could be energised with no power available to the closing coil circuit. In addition, the NRC inspector questioned the “as found” operability of the pump.

Review of the wiring diagram showed that the closing coil circuits were wired and fused separately from the remainder of the control power circuits for most of the plant’s 2400-volt and 4160-volt circuit breakers. This separate circuitry allows blown or improperly installed fuses to remain unnoticed because there was no alarm or loss of local or control room indication. This lack of indication of a loss of control power could prevent personnel from recognising when required equipment becomes inoperable through testing or initiation of an actual signal.(IRS 1261.00 and IN 91-78).

On August 24 1992, at Cruas NPP (PWR), when performing a periodic test, with unit 1 in hot shutdown, the AFW turbine-driven pump was stopped, as a result of a rapid increase of temperature of the pump back thrust bearing. Subsequent investigations revealed that deterioration of the thrust bearing had occurred because of a lack of lubrication; the oil filter was found to be clogged.
An analysis showed that the "low oil pressure" alarm, which should have indicated that the filter was clogged, did not appear. This alarm is initiated by a pressure sensor, which according to the mechanical drawings, is situated downstream from the oil filter. In fact, the operator discovered that the pressure sensor nozzle was upstream from the oil filter; therefore, the clogging of the oil filter could not be detected and the low oil pressure alarm could not be initiated.

This faulty pressure sensor implantation existed since plant construction and also affected the three other units. It could have prevented detection of the oil filter clogging and could have quickly led to the pump deterioration and the resulting loss of AFW to the steam generators in case of total loss of electric power sources.

In March 1993, at Grohende NPP (PWR), the licensee checked analog isolating transformer units in the framework of an instrumentation and control quality assurance programme. These units electrically separate the signal path of analogue signals and protect the instrumentation and control equipment designed for a voltage between 20 and 30-Vdc from non permissible high voltage (above 30V).

Deviations from the specified status were revealed at 182 module positions of such units. In four instances the units were missing; in other cases, the overvoltage barrier in the module was missing or was installed on the wrong side (input/output) since the plant was commissioned.

The safety significance of this event resulted from the possibility of coupling overvoltage into safety-related instrumentation and control equipment in more than one redundancy.

The analog isolating transformer units are delivered by the manufacturer for various tasks, and six different types are used. When installed during the construction of the plant, the type of transformer unit was confused (The specific type of unit can be distinguished by an order number only visible if the unit is racked out.)

During the recurrent functional tests of the instrumentation and control system, the incorrect installed units could not be detected, because the overvoltage protection did not influence the signal under normal circumstances. This event reveals deficiencies in the quality assurance during the installation of the analog transformers units.

The wrongly installed units could not be tested during normal operation or in regular in-service inspections because of the overvoltage cannot be tested under realistic conditions.

Consequently, it was necessary to develop methods for implementing reliable recurrent tests of the overvoltage protection function as a long-term improvement; these recurrent tests required a different design of the protection function. (IRS 1436.00)

3.8 Inadequate Maintenance
Inadequate corrective or preventive maintenance have led to degraded conditions of components and resulted in events with actual or potential safety consequences often revealing common mode failures. They resulted from:

- inadequately detailed procedural guidance,
- improper implementation or lack of vendor recommendations,
- incomplete post-maintenance testing

In addition, maintenance effectiveness was impaired by quality organisation problems such as

- poor maintenance management
- lack of work process control
- poor personnel sensitivity to the effects of cleanliness after maintenance operations
- poor operating experience feedback

Some events highlight the risk of common mode failure involved by lubricant practices, interventions on parts of systems that cannot be tested, those associated to wiring operations with reduced control feasibility. These events underline the interest to carry out, whenever possible, staggered tests particularly on redundant lines of safety systems.

A number of events with very serious safety potential consequences have to be ascribed to maintenance deficiencies as follows:

- failure to carry out post-maintenance testing
- inadequate personnel sensitivity to the effects of cleanliness resulting in deficiencies on ECCS availability.

Eight events with estimated conditional core damage probabilities ranging from 10-6 to 5,5 10-2 have been selected as precursors, four with probabilities higher than 10-4. Among them, two resulted in situations creating unprecedented challenges for the operators, during plant operation at full power, in one case, operators had to cope with a situation not covered by existing operating procedures and further complicated by a fire (Cruas, October 1990). In an other case, they were required to take high-priority actions in a high stress environment while many indicators and alarms were missing in the control room.(Nine Mile Point, August 1991).

The two other precursors are related with ADS relief valve inoperability, and poor performance of the RHR system operating in the suppression pool cooling mode.

The destructive turbine overspeed which occurred at Salem was the result of lack of post-maintenance testing and deficiency in the process of experience feedback.

3.8.1 Lack of Maintenance and Imprecise Guidance in Maintenance Procedures

On March 30, 1990, at the Calvert Cliffs NPP (PWR), one of the two pressurizer-operated relief valves of Unit 1 was found to be inoperable for 19 months. The thermal
overload contact was found open, indicating that an overcurrent had existed for a sufficient period of time to cause the circuit to open. No indication of this open contact existed in the control room. The thermal overload resulted from excessive current draw caused by a stuck roller for the movable solenoid slug. The same valve had been found in this condition in April 1988. An inadvertent actuation of this valve occurred on June 26, 1988, the last time this valve was known to have been operable.

This inoperability resulted in bleed-and-feed being unavailable for the same period of time. The conditional core damage probability estimated for this event is 1.1 10-5.(LER 317/89-005)

The root cause of this incident was a lack of vendor information concerning the positioning of the slug. Other contributing factors were as follows:

- inadequate maintenance procedures which did not include steps to ensure that personnel performing the procedure visually verified the proper position of the slug
- lack of post-maintenance testing to require to verify the current to the solenoid against the design rating
- insufficient depth of assessment and root cause analysis when a similar condition was previously identified

On October 30, 1990, at Cruas NPP (PWR), while Unit 4 was operating at full power, an arc strike occurred on one of the poles of a contactor of the 6.6 KV emergency switchboard B, resulting in its destruction. The deterioration, resulting from heating associated to ageing, of the damping washers located in the contactor, provoked the arc striking. The operating crew had to cope with a situation no covered by the existing operating procedure, which was further complicated by a fire in the switchboard.

The cause of the incident was the destruction of a contactor as a result of damage to the damper washers causing an electrical flashover and an explosion in the cell; washers damage was ascribed to ageing. This type of defect was already detected in November 1988 on 6.6-KV contactors of Blayais NPP Unit 4 and ascribed to ageing of the damper washer in the moving parts of the contactor. The extreme sensitivity of the Vulquolan washers to ageing was also noticed at Chinon NPP in 1989. The ageing was caused by inadequate cooling as a result of lack of ventilation of the washers leading to a loss of their elasticity.

The manufacturer suggested the installation of new covers with ventilation slots for cooling the washers. Following the incident at Chinon NPP, and the previous one at Blayais NPP, EDF Central Services issued a recommendation requesting that sites inspect all of the contactors and improve ventilation of the covers. These instructions were not still applied at Cruas Unit 4; it is clear that there was too long a delay between the initial signs at Blayais and Chinon and review and recommendations by the EDF Central Services (end of 1989) and implementation.

Ageing of the damper washers ultimately leading to their damage is a common mode failure that could result in the loss of the two emergency switchboards in the event of a simultaneous incident on a contactor on each of the two switchboards. In this case the
"beyond design" procedure H3 (for a total loss of external and internal electrical sources) would have been utilised. However, if the two boards were damaged, it would have been impossible to reconnect them to an internal or external supply until at least one board had been fully repaired. The conditional core damage probability for this event is estimated to be 5.5 10^{-2}.

This incident raised a concern that the damage to the damper washers was responsible for phase-ground flashovers causing an insulation fault in the switchboard. This fault between phase and ground appears to have quickly progressed into a three-phase fault. The protection systems located below the contactor consisting of current transformers, were activated late or not at all, and the switchboard tripped on maximum current protection. (IRS 1439.G0)

According to the IPSN, this situation could call into question the design of the principle of selectivity of protective systems for emergency switchboards. In fact, by virtue of this principle, the design of these switchboards should not allow a phase-ground flashover at one contactor to affect the entire switchboard.

Moreover, in order to anticipate fast ageing problems of such complex components as contactors, the IPSN recommended that EDF perform, a systematic expertise of all sub-components and piece parts of a randomly selected component in addition to those already included in the preventive maintenance programmes.

Similar conclusions are reached in IRS 1526.00 concerning problems with relatively small electrical sub-components in the GE reactor trip breaker assembly, observed at ST. Lucie NPP Unit 2, which could be made less likely by appropriate inspection and maintenance and therefore reduce the frequency of reactor trip breaker failures.

Potential problems associated with failures of electrical buses caused by cracked insulation or debris build-up in bus bar housings occurred also previously at PaloVerde Unit 1 (PWR), Kewaunee (PWR), Millstone Unit 1 (BWR), Sequoyah unit 1(PWR), and Browns Ferry Unit 2 (BWR). (IN 89-69 dated September 7,1989 )

Failure of medium-voltage electrical bus bars, principally involving 4.16 and 6.9-KV ac buses, have resulted in the following events:

- bus bar electrical faults and fires
- electrical power system undervoltage conditions
- plant transients and reactor trips
- engineered safety features actuations

Failures of the bus bars have been attributed to cracked bus bar insulation, combined with the accumulation of moisture or debris in the bus bar housing. Insulation failures provided undesirable phase-to-phase, or phase-to-ground electrical paths, which resulted in catastrophic failures of the buses. Poor design of the bus duct and inadequate implementation of the vendor-recommended preventive maintenance are among the causes of these failures. (IRS 1046.G0 and IN 89-64)
On August 13, 1991, at Nine Mile Point NPP (BWR), an internal failure of the main transformer of Unit 2, caused a degraded voltage that resulted in the simultaneous loss of power outputs from five non-interruptible power supplies (UPS) and equipment. The main generator and turbine tripped, and the reactor scrambled. The power outputs from the five power supplies were lost because of a combination of a wiring problem and the failure of the internal batteries to supply control power. The five power supplies provide power to the main control room annunciator system and to other systems important to safety.

The safety significance of this event is that it presented an unprecedented challenge to the operators who were required to take many high priority actions in a high-stress, time-sensitive environment while many of their normal indicators, alarms, and communications were unavailable or misleading. The conditional core damage probability of this event was estimated to be $3.8 \times 10^{-4}$. (LER 410/91-017)

According to an augmented inspection team (AIT), the major contributing factors for the failure of the power supplies were inadequate maintenance of the batteries that supply power to the control logic and inadequate maintenance of the power supply output breakers:

Identical maintenance practices used for all five UPS units introduced a common cause maintenance deficiency. Internal control logic batteries had not been replaced in any of the five UPS units, and they were dead. Although being charged, they degraded due to age.

On September 24, 1991, at the Peach Bottom NPP (BWR), following a refuelling shutdown of Unit 3, three safety relief valves (SRVs) were removed for preventive maintenance. On examination, the control solenoid valve wiring insulation was found to be degraded on each SRV. An investigation revealed that the damage occurred because the SRV insulation was improperly installed during the previous outage, this caused an unusually high temperature environment in the immediate vicinity of the solenoid valve and associated wiring. As a result, an engineering analysis determined that there was no longer a reasonable assurance that the ADS relief valves were operable.

This condition had existed since the last refuelling outage in November 1989, when the MSRV insulation was improperly installed after it had been removed to support the piping replacement modification. In addition, the licensee found that the maintenance procedure used to remove and reinstall the MSRV thermal insulation did not provide the necessary level of detail to ensure that the insulation was properly installed. The conditional core damage probability estimated for this event is $3.3 \times 10^{-4}$. (LER 278 / 91-017)

On November 9, 1991, Salem NPP Unit 2 (PWR) experienced a destructive turbine overspeed. The event occurred while the plant staff was conducting routine turbine testing at 100-percent power. The overspeed occurred as a direct result of simultaneous common-mode failures of three SOVs in the turbine’s overspeed protection system. The event did not result in any release of radioactivity or personnel injury; however, it did cause extensive damage to non-safety equipment, and resulted in a 6-month outage.

An AIT sent by the NRC to investigate the event concluded that all three overspeed system solenoid valves were mechanically bound and could not shift position on demand. Several precursor factors contributed to the event:
The Salem 2 licensee had no preventive maintenance programme for any of the three SOVs. The surveillance and operational testing of the turbine trip and over-speed circuits did not specifically and independently verify the proper hydraulic functioning of each SOV. There was an inadequate review and feedback of operational experience.

The licensee had two earlier indications of problems with these SOVs. Similar valves on Salem Unit 1 required replacement, yet no effort was made to effectively verify the operability of the SOVs in Unit 2. Another indication occurred during a start-up in October 1991. In that instance, the over-speed controlled SOVs failed to open when a test of the system was performed. Nonetheless, the licensee continued the start-up without further diagnosis and resolution. (IRS 1234.02).

In September 1993, at Arkansas NPP (PWR), an engineering evaluation of Unit 1 indicated that a RHR /LPI pump might have been incapable of performing its recirculation mode function following a LOCA. The procedure did not provide the necessary guidance for accurately determining the motor's magnetic centre and correctly coupling the pump to the motor. This condition existed for 4 months, while the plant was at power until the plant shut down.

The maintenance procedure was revised to incorporate guidance on how to correctly identify the motor magnetic centre and couple the pump to the motor. The estimated conditional core damage probability for this event is 5.1 10^-5. (LER 313/93-003)

On November 16, 1991, at Gravelines NPP (PWR), a lubricant anomaly occurred while Unit 1 was in the shutdown state for maintenance, with the primary coolant level above the reactor vessel seal, and the steam generator water boxes opened for tube bundle inspection. As a result, one of the RHR pumps was declared unavailable following an abnormal increase in the pump's bearing temperature. On November 1991, the pump was replaced. Subsequent investigations revealed that the problem was caused by the use of two incompatible types of lubricants. The same problem was found on the other RHR pump. This incident raised particular attention with regards to lubrication practices that may cause of a common mode failure. (IRS 1260.00)

On March 4, 1993, at Tricastin NPP (PWR), during periodic testing of the reactor protection system of Unit 2, a MOV on the HHSI line failed to open on receipt of a safety injection signal. The valve failed to open by actuation of its thermal load protection without engaging the torque limiter. When the servomotor was examined, the licensee found that the worm gear wheel /shaft assemblies were damaged as a result of insufficient lubricant in the servomotor. Six other servomotors of the same type were found to contain insufficient lubricant.

Lubricant originally supplied for all electrically-operated servomotors of this type had been replaced over a 3 year period with a lubricant of better quality; however, insufficient lubricant had been added. Half of the servomotors potentially affected would have been required to operate in the event of engineered safeguard actuation.
A close relationship between insufficient lubrication and damage to the servomotor worm-gear and shaft was established. This common mode failure resulted from imprecise guidance in maintenance procedures which did not indicate the quantity of lubricant required, contrary to the manufacturer's instruction. The maintenance schedule indicated a lubricant level, in the gear casing, rather than a quantity. Moreover, although the manufacturer's instructions did indicate a theoretical volume, in practice, reassembly made it difficult to use the full amount of grease. (IRS 1459.G0)

3.8.2 **Deficiencies in the Quality Organisation**

On May 19, 1988, at Cruas NPP (PWR), the licensee discovered large tears in the four ESW strainers servicing Units 1 and 2. This system, which filters the ESW system upstream from the water intake trash rakes, had been in a degraded condition for almost 5 months, unknown to the operating organisation.

The tears in the screening drums were caused during servicing in December 1987 (temporary modification of ventilation systems) when old sections of ventilation duct were left in place and subsequently fell onto the screening drums. The damage to the screening drums meant that the system was no longer able to provide the quality of filtration required (1 mm mesh), since the downstream rakes could only retain objects larger than a few centimetres. This incident identified a potential common mode failure that could have occurred on equipment important for safety. Specifically blockage of the component cooling water heat exchangers could cause a loss of the RHR and the CS systems.

This incident identified a fault in work practices, since these strainer failures were apparently caused by the presence of debris left by maintenance personnel during previous work carried out on the ventilation system. It also highlighted that it would be advisable, whenever possible, to carry out staggered maintenance on redundant lines of a safety-related system (IRS 973.00).

On May 30, 1992, at ST Alban NPP (PWR), during the annual outage of unit1, the licensee discovered that an ECCS sump suction valve in the train B was partially open, although it should have been closed. Moreover, the piping upstream the valve was found without a water seal. Potential problems from this lack of closure would have resulted in the following conditions:

- a nonisolable radioactive release to the environment through the minimum flow lines of ECCS pumps returning to the RWST
- loss of the train B ECCS pumps by air entrainment
- contamination of the RWST by water collected in the sumps and discharged to the tank via the minimum-flow lines of the pumps before these switch over to the containment.

Analysis of this incident led to several findings:

In September 1991, the valve actuator was replaced by two teams operating independently. Disassembly and assembly of the actuator was performed by mechanics after
electricians disconnected the power supply cables; after assembling the actuator, the valve was operated manually.

The electricians reconnected the cables and performed a requalification test of their intervention by automatically actuating the valve, and setting of the position switches on the valve stem. The closed position switch was then set without the opercul reaching the bottom of the valve seat for an unknown reason.

The leak rate test of the check valve downstream from the sump suction valve was performed after the valve requalification; in spite of an intervention the check valve remained untight, nevertheless, the reactor was restarted without any consideration of the status of the sump suction valve.

Moreover, there was a failure to perform a surveillance requirement, the leak rate test of the valve, which should finally have permitted plant personnel to detect the anomaly was not performed because a necessary temporary device for this test was not available.

This incident revealed that defence-in-depth was seriously deficient in operations concerning safety-related equipment. Application of proper work process control was deficient in its lack of co-ordination; this could probably be avoided by nominating a unique responsible in order to ensure a better co-ordination between operators and maintenance personnel.

Potential ECCS Failures Caused by Foreign Material Blockage

Failure to remove temporary materials used during maintenance operations, or debris left in the sumps have been and continue to be the cause of potential ECCS failures, mainly during the post LOCA recirculation phase.

The important fact concerning these foreign materials is that they may not be detected during post-modification testing and remain undetected for an extended period. Moreover, possible migration of small debris from these materials necessitates, before restarting, a careful examination of all areas where the debris could collect and cause blockage after extended operation. Two of these events have conditional core damage probabilities estimated to be 9.9 10-6 and 1.2 10-4.

On August 1, 1989, at Fessenheim NPP (PWR), while checking the NPSH of the train B LHSI pump during a scheduled shutdown of Unit 1, for a 10 years inspection, test personnel noted that the breaker on the power supply to the pump motor assembly had tripped as a result of overcurrent. Subsequent investigation revealed that the rotor had seized as a result of a blockage by a piece of foam jammed in the inlet suction. The malfunction was detected in the course of a test that had not been carried out since the initial plant start-up tests (NPSH verification of the of the pump taking suction from the ECCS sumps).

Had the piece of foam found in the containment system lines migrated further downstream toward the spray valves, it might not have been detected during system venting. None of the tests scheduled for the start-up phase of operations would have revealed the presence of foreign material. Had this material not been found, it could have jammed one of
the CS valves and could have therefore completely blocked one of the CS lines in case of accident. The pieces of foam were excavation plugs that workers had failed to remove from inside the pipes after completing welding work on the lines. (IRS 1149.00)

On September 18, 1992, at Point Beach NPP (PWR), with Unit 2 at 100% power, the train A CS pump failed to pass the quarterly test. The pump was disassembled, and a foam rubber plug, which had been installed in the RHR system 10 months earlier, was found in the suction line of the CS pump.

This plug had been installed as a temporary cleanliness barrier during modifications to the RHR system during the 1991 refuelling outage. The most likely original location for the plug was in the portion of the common line between the train A RHR pump discharge to the train A CS pump and the train A SI pump suction. In its location, the plug could have prevented both train A CS and SI pumps from operating in the long-term recirculation mode. The conditional core damage probability estimated for this event is 9.9 10-6. (LER 301/92-003)

On March 26, 1993, Perry NPP (BWR) was scrammed in response to a rupture in a 30-inch. service water line. This event led to flooding in various auxiliary buildings where safety-equipment was located, but had no impact on that equipment. Three weeks later, the RHR suppression pool strainers were inspected, and one strainer was fouled and deformed.

These strainers had previously found to be deformed, during a maintenance outage in January 1993, because of excessive differential pressure caused by strainer fouling, during normal was inspected and cleaned. Then, in May 1992, an accumulation of dirt and debris was noticed on both RHR strainers. However, strainer cleaning was scheduled for a later date, since RHR system performance was considered acceptable based on surveillance testing.

The excessive differential pressures across the RHR strainers from debris accumulation would have failed suppression pool cooling if this mode of RHR was required to operate for long periods of time. The conditional core damage probability estimated for the clogged suppression pool strainers and service water flooding is 1.2 10-4. (LER 373/93-015)

The cause of the reduced capability of the RHR pump strainers is considered to be inadequate cleanliness in the suppression pool. The root causes include inadequate programme requirements and inadequate personnel sensitivity to the effects of cleanliness on ECCS operability. Before these events, adequate material accountability requirements were not in place for material introduced into the containment.

Until the complete inspection and cleaning of the suppression pool in April 1993, inspection and cleaning efforts were limited to easily visible and accessible pool areas. This was clearly demonstrated by the disproportionate amount of debris found in April in areas non routinely inspected, after the pool was thought to have been cleaned in February 1993.

The debris consisted of glass fibbers that had been inadvertently introduced into the suppression pool from temporary drywell cooling filters, and corrosion products that had been filtered from the pool by the glass fibbers adhering to the surface of the strainer.
In response to this event, the NRC issued Bulletin 93-02 ‘Debris Plugging of Emergency Core Cooling Suction Strainers‘ requesting that both PWR and BWR licensees to take the following actions:

- identify fibrous air filters and other temporary sources of fibrous material in containment that were not designed to withstand a LOCA.
- take prompt action to remove the material and ensure the functional capability of the entire ECCS.

In response Perry NPP took the following significant actions:

- increase the suction strainer area from 1.9 to 3.9 square meters.
- provide for a suction strainer backflush capability.
- improve measures to maintain a high level of cleanliness in the suppression pool.

Following a more recent event at Limerick NPP, Unit 1, on September 1995, the NRC issued Bulletin 95-02 ‘Unexpected Clogging of a Residual Heat Removal Pump Strainer While Operating in Suppression Pool Cooling Mode‘. This bulletin requested that the BWR’s licensees take actions to resolve the issue, highlighted by the Limerick event, of the potential blockage of ECCS suction strainers during normal operation by debris that is present in the suppression pool, or may accumulate in the pool during normal operation.

On October 10, 1993, at Cattenom NPP (PWR), while implementing a modification during a plant outage of Unit 1, the licensee discovered a plastic plug clogging the cooling heat exchanger of the mechanical seal of the train A CS pump. The plug at the inlet of the heat exchanger was not removed in March 1993 when the pump had to be replaced because of an operating anomaly. This involved to replace the inappropriate seal cooling heat exchanger with an other one which was installed with a plastic plug.

This anomaly remained undetected by all periodic tests performed on the pump after the intervention.

A subsequent analysis determined that failure to cool the pump seal in case of a LOCA would have resulted in the pump seal failure with a subsequent leak outside the containment estimated at 5 m3/h and would finally have caused the pump unavailability. This condition is explained by the fact that, in March 1993, the plant was operating at full power, and the decision was taken to complete the CS pump replacement within the allowed outage time (AOT), which did not leave sufficient time to perform the usual risk analysis required for a replacement of safety-related equipment.

3.8.3 Inadequate or Incomplete Post-Maintenance Requalification Testing

In June 1991, during performance of a calibration procedure on RCS flow instrumentation, at Harris NPP (PWR) a reactor trip signal was inadvertently generated on Unit 1.
Reactor trip breaker B correctly responded to the signal, opening to cause insertion of rods, but the reactor trip breaker A failed to operate. The licensee subsequently determined that circuitry in the A train solid state protection system (SSPS) had failed in a way that prevented it from responding to automatic reactor trip signals. This failure apparently occurred during maintenance on the closing circuitry of reactor trip breaker A on May 1991. The post-maintenance testing verified the closing circuit problem was corrected, but failed to detect the problem in the SSPS undervoltage output driver card. (HARRIS 1, March 6, 1991).

On February 18, 1992, after annual maintenance on the site EDG, at Gravelines NPP (PWR), it proved impossible to proceed with full-load requalification tests (at 4000-KW) to ensure full EDG availability. This condition arose because two resistors on the load test bench were out of service. (All 900-MWe unit plants have a site EDG set that can be hooked up to replace two EDGs on any unit in the event that these are unavailable.)

Investigations conducted by the operator revealed that the 1991 annual periodic test at 100% rated power, had in fact been conducted at 3300 KW on both EDGs of Unit 1; at 2700-KW on both EDGs of unit 4, and at 2600-KW on one EDG of Unit 6, because the load test bench had been partially inoperable on several occasions. Based on the difference between the loads that these generators could have been required to supply, and their outputs during the tests, it could not be guaranteed that the five EDGs would have been capable of supplying the maximum load under accident conditions during the previous cycle.

Poor maintenance of apparatus needed for the requalification of safety-related equipment and the operators' lack of awareness of the risks of common mode failure led to the unsatisfactory performance of periodic tests. This compromised the availability of five EDGs and the site EDG set. (IRS 1507.00)

3.8.4 Incidents Caused by Installation of Temporary Devices

Installation of temporary devices is necessary in certain maintenance operations and tests carried out during unit-shutdown in order to inhibit protective actions or to isolate circuits or components for interventions. Blind flanges, electrical jumpers, knife terminals and plugs, are the most well known of these temporary devices. These are mainly used during outages and pre-start operations and in a few cases for periodic tests or fortuitous interventions during plant operation in configurations not provided by design.

Their installation induces a safety risk because most cannot be operated nor monitored by control instrumentation; therefore their safe use relies mainly on the quality of management.

Failure to detect their presence or to recover them after use may have potential adverse consequences on safety. If the consequences of deficiencies in the management of temporary devices are often limited, in most cases, to spurious protection action actuation, some of them may lead to extended latent failures of safety systems, as illustrated by some events described hereafter.

On April 17, 1987, at Bugey NPP (PWR), during an inspection of the Unit 2 reactor building in cold shutdown for refuelling, a blind flange was discovered on the
containment atmosphere monitoring system discharge pipe. This flange made the system unavailable for its hydrogen mixing and sampling functions after a LOCA.

Blind flanges are normally installed during leak tests on the outer part at the mixing system containment and it is very likely that the flange in question was installed during the annual shutdown in 1986. The containment atmosphere monitoring system was unavailable for an undetermined period, unknown to the utility. (IRS 879.00)

In August 1989, at Dampierre NPP (PWR), the discovery of blind flanges on the discharge pipes of the same system in Unit 1 proved that the analysis of the Bugey incident was inadequate, since it did not prevent the second incident from occurring. In this case, the periodic test of the mixing system operating at full flow after the leak tests, was the only means to ensure that the system was available. After this second incident, this periodic test was included in the IST programme of the general operating rules (GOR). (The GOR comprise technical specifications, periodic testing requirements, and criteria for safety functions, as well as rules of operation under incidental and accidental conditions)

Lessons learned from these two incidents were the starting point of the following considerations:

- the possibility of limiting the use of temporary devices
- management of these devices during testing and maintenance operations
- the possibility of performing requalification tests after servicing

On August16, 1989, at Gravelines NPP (PWR), a problem came to light during the annual calibration check of the supply line of the three RC S pressurizer pilot controlled valves of Unit1. This problem concerned the restriction of the valve supply line. Specifically, a non-conformance resulted from an installation error involving solid bolts instead of normal banjo bolts, during a previous servicing operation in June 1988. This error could have led, to the pressurizer relief valves opening later and at higher pressure values than planned.

An operability test performed just after this intervention would have discovered the anomaly in time. This test, which is required under the national restart procedure after each refuelling, was performed successfully at the beginning of April 1988, when restarting the reactor after the outage. However, the plant had to be halted and restarted in June 1988; in this second restart, the intervention was not followed by valve operability tests, as the GOR required the test after refuelling.

In the case of the start-up at the beginning of June 1988, the situation was not that of restarting after refuelling. The operator was therefore not required to carry out the operations corresponding to requalification of the valves. Since this event, the valve operability test has been included in the GOR for any intervention involving these valves.

This highly significant discrepancy in terms of safety emphasises the potential hazards of all maintenance operations involving the installation of special devices such as blind flanges, plugs, and straps, as well as the need to carry out requalification tests whenever possible (IRS 1004.00).
On August 21, 1992, at Cattenom NPP (PWR), failure to withdraw a fine-mesh filter at the bottom of the reactor cavity following shutdown of Unit 1 could have caused a retention of reinjection water in case of LOCA requiring containment spray. This failure potentially created inadequate performance during recirculation operation of the ECCS following an accident.

On June 26, 1993, at Gravelines NPP (PWR), when performing a nonload test of an incidental procedure on Unit 2, while the reactor was at full power, the licensee discovered that knife terminals at the interface of the reactor protection system (RPS) and the AFW system were left open. This oversight rendered the anticipated transient without scram (ATWS) actuation unavailable by inhibiting AFW system start-up and turbine trip on train A. This situation existed since September 1992, after the licensee performed an ECCS test. Putting the knife terminals back in configuration was not explicitly stated in the worksheet and therefore was not done. Moreover, at that time, the interface between the AFWS and RPS could not be tested.

Corrective actions identified by EDF relied on the addition of test-switches in order to improve the interface testing; these actions were not yet implemented. This design weakness was identified during a similar event that occurred a few years before on another plant. As a result of that event, the DSIN had required EDF in 1991, to improve the test interface between the AFWS and RPS. EDF has since implemented a test-switch on each train to permit personnel to check the AFWS availability and the logic-starting commands of the RPS.

The conditional core damage probability for this event has been estimated to be 1.07 $10^{-6}$ compared to the value of 1.02 $10^{-9}$ mentioned in the 900- MWe French reactors PSA study, as a result of ATWS failure.

### 3.9 Ineffective Experience Feedback

Events reviewed in the previous sections have evidenced factors that contributed to delay the discovery of latent failures such as insufficient instrumentation to provide feedback on the system status, deficient test procedures not including all requirements that would exist at operating conditions, maintenance procedures with inadequate guidance, insufficient depth of assessment and root cause analysis when a similar condition was found.

In addition, certain weaknesses appear in the process of experience feedback. This is particularly evident from the recurring events associated with previous similar event this indicates that appropriate corrective actions were not taken in time by the licensees.

This will be illustrated by the three following examples. Licensees' evaluation of...

As shown hereafter, the main weakness was in one case, failure to identify the potential of the root cause. In the other case, the weakness involved a delay in implementing a valve leaktightness test in the appropriate direction after performing a campaign of non-destructive controls. In the third case, an incorrect inspection protocol diagram contributed to an incorrect conclusion drawn by the licensee.
Sequoyah 2- and Oconee 2

On August 22, 1990, while troubleshooting a gas-bound centrifugal charging pump on Sequoyah Unit 2, the licensee discovered that a substantial accumulation of hydrogen existed in the charging pump suction header in a recirculation supply line from the RHR system to the charging pumps. Sufficient gas quantities were identified that successful performance of the safety injection and charging pumps could not have been guaranteed, particularly for recirculation modes.

While reviewing for previous similar events throughout the industry, the licensee identified several Nuclear Experience Review (NER) items involving events that were possible precursors to the Sequoyah event. These items included NRC IN 88-23," Potential for Gas Binding for High-Pressure Safety Injection Pumps During a Loss-of-Coolant Accident", and Westinghouse Letter TVA-88-825.

The licensee then established a special review team to investigate the disposition of the previous NER items to determine if the hydrogen problem at Sequoyah could have been recognised at an earlier date. The team concluded that the licensee failed to identify the potential for gas binding from hydrogen at the centrifugal charging pumps after receiving industry information.

The principal reason for this failure was incomplete review of IN 88-23. The licensee's review of that notice principally focused on piping elevations located above the VCT because of the emphasis on this configuration in the industry information. In responding to IN 88-23, the major licensee's emphasis was on comparing Sequoyah to the Farley Nuclear Plant, (where the event described in IN 88-23 occurred). Because Sequoyah has no ECCS above the VCT, the licensee concluded that an event similar to Farley's would not occur at Sequoyah.

In hindsight it appears that the licensee did not fully understand the hydrogen gas desorption mechanism. Additionally, the licensee performed an inadequate review of a Westinghouse Letter TVA 88-825. This letter referenced the local pressure phenomenon discussed by the IN 88-23, referring to it as a "two-phase" mixture, and identified the mechanism for gas desorption at low pressure points in piping systems, (such as valves, tees, elbows, or orifices). The Westinghouse letter indicated that evaluation of the issue is plant-specific and recommended that, since hydrogen accumulation is difficult to predict, the accumulation is best determined by venting. The evaluation conducted by the licensee did address the issue on a plant-specific basis. However, because indications did not exist in the plant at the time that the potential existed for hydrogen to come out of solution, the licensee failed to make a recommendation to vent.

The potential for hydrogen entrainment leading to pump damage was recognised at Oconee Unit 2 on April 16, 1991. In that instance, operational guidance was provided; however, that guidance was based upon inappropriate operator response times and operation of equipment which does not have sufficient provision for single failure.

Dampierre 2
In September 1992, an incident occurred at Dampierre NPP Unit 2 (IRS 1362.00) which was similar to two incidents that 4 years earlier occurred involving reactor coolant leaks, one at Farley Unit 1 on December 1987 (IRS 851.00), and the other at Tihange Unit 1 on June 18,1988, (IRS 864.00). Both of these earlier incidents related to thermal fatigue in non isolable piping connected to the RCS.

During the 4-year period preceding the Dampierre incident, EDF had analysed the two foreign incidents. Considering the similarity of the 900-MWe units with these two facilities, EDF expended considerable efforts to reach a better understanding of the thermohydraulic phenomenon affecting the auxiliary piping of the reactor coolant system. These efforts included, investigations, theoretical studies, and bench onsite tests, in order to take the appropriate corrective actions on the 900-MWe units. Based on this understanding, EDF developed strategy to detect eventual flaws.

In February 1989, EDF established a programme of non destructive controls of weldings and elbows selected as being sensitive to thermal fatigue. This programme included radiographic examination of the weldings and ultrasonic testing of the elbows. EDF implemented this programme in all 900 MWe units between 1989 and 1991 with satisfactory results, since no cracks were found. As a result, the licensee did not extend the control campaign. It was only after the Dampierre incident that EDF recommenced the controls which again revealed no cracks.

EDF then implemented procedure to check, at hot shutdown state, the leaktightness of isolating valves between the header of the charging pumps and the headers of the cold and hot safety injection lines. Initiated in 1989, this action was only carried out in October 1992. Since that date the scope of this test, performed before each refuelling outage on each 900 MWe unit, involves searching for any leakage between the chemical volume control (CVC) system and the SI system that may give rise to an entry of cold water into the reactor coolant system.

As required by DSIN, since 1993, this test is also performed, after each refuelling outage, before restarting. In case a valve leak is discovered the programme of non destructive controls mentioned above is applied.

Before the implementation of this test, the leaktightness of isolating valves between the CVC system and the SI system relied, erroneously, on the integrated leak rate tests, performed at each refuelling outage, on these valves which also have a containment isolating function. The fact is that the purpose of these tests is not well-suited to the problem because leaktightness is checked from inside the containment to outside. The licensee failed to consider the possibility of leakage in the reverse direction.

Had the leaktightness test of the isolating valves between the CVC system and the SI system been implemented earlier and more systematically, the Dampierre incident would probably not have occurred.(Afterward, examination of previous test results performed in 1991 indicated that the valve probably responsible of the cracks was untight).

This case suggests that experience feedback has not worked satisfactorily, since the Dampierre incident happened despite the understanding of the root cause of the Farley and
Tihange incidents, the similarity of 900- MWe facilities with these two units, and the variety of actions taken.

**Lovisa 1**

On May 28, 1990, a main feedwater line pipe ruptured at Lovisa NPP Unit 1 (IRS 1102.02). The rupture was downstream from a feedwater pump in the flange of an orifice plate used for flow measurement close to a welded seam. The rupture was attributed to heavy erosion/corrosion, which had reduced pipe wall thickness to a circumference of only 1 to 2 mm at the rupture point. The outside diameter of the feedwater line piping is 325 mm, and the nominal wall thickness 18 mm.

Erosion/corrosion of piping is monitored by means of in-service inspection programmes based on experience. The programmes were not sufficiently comprehensive, however, to permit the licensee to detect the thinning of the flanges of the orifice plates used for flow measurements. In connection with the 1991 and 1992 refuelling outages, the licensee undertook several corrective actions including inspection in accordance with an extended programme.

In spite of these actions, a second feedwater pipe ruptured at the Lovisa NPP, Unit 2 on February 25, 1993. (IRS 1352.02)

Prior to the rupture, the licensee was aware that the broken pipe section was prone to erosion. Also, based on an analysis using a computer-aided condition evaluation system, an inspection was recommended during the 1992 refuelling outage. However, during a review of these recommendations, the licensee decided not to conduct the inspection, since the piping wall thickness after the check valve had been measured and deemed sufficient during the 1991 refuelling outage. In reality, though, the end of the inspected area was about 20 mm from the broken point, the broken connecting flange, located after the check valve flange, was entirely lacking from the inspection protocol diagram and was thus not measured in 1991. The incorrect inspection protocol diagram contributed for its part to the incorrect conclusion drawn by the licensee.

### 3.10 Results and Conclusions

Review of operating experience during these last ten years has evidenced risk-significant events involving a widespread field of long duration latent failures, a broad class of systems and a great variety of deficiencies.

Many deficiencies existed in original plant designs and those deficiencies could only be detected through engineering design reviews, design-basis reconstitution studies or exceptional demands on equipment during transients. Also, the deficiencies remained undetected during extended periods until theses studies were completed.

It is reasonable to expect that such studies would lead to a better involvement of utility engineers, as well as a greater understanding of their plant-specific design.
characteristics. In addition the studies encourage further studies in order to eliminate remaining initial design deficiencies.

Deficiencies (including inadequacies in design and installation) existed since initial start-up and should normally have been detected by commissioning tests. Nevertheless, these deficiencies remained undetected by surveillance tests during years of commercial operation because of a lack of exhaustivity in IST programmes or because inadequacies in testing methods and practices, many of these deficiencies were discovered fortuitously. Ultimately, these deficiencies can only be resolved progressively through the increasing level of operating experience achieved in this particular field. Nevertheless, some reports of recurring deficiencies indicate that licensees efforts in preventing or minimising the deficiencies in their respective plants are not always sufficient.

Moreover, latent failures have been introduced in the course of inappropriate and ineffective maintenance activities, as well as through incompletely reviewed and tested design changes or modifications implemented with the intent of increasing the reliability of safety systems. In many cases, deficiencies in the quality organisation as well as failure to implement corrective actions in time have also contributed to maintain these failures during an extended period. A few recurring events illustrate also how carelessness may render the experience feedback process ineffective.

In addition, problems have appeared without warning as a result of phenomena that are unknown or not well recognised at the design stage. Because these phenomena involve an incubation period, they are frequently not detected in time, thus delaying the required corrective actions.

If any of the failures had no real safety consequences, certain had an high risk potential. Moreover, as severe incidents which occurred in the past were scarcely caused by a unique deficiency but resulted often from multiple deficiencies, any of these latent failures may become the ingredient of a serious incident.

In light of the events reviewed in this report which entails a widespread field of failures involving a broad class of systems and a great variety of failures, it appears that a lot of these failures could have been detected by more complete surveillance tests or prevented by better monitoring and more effective post-maintenance testing. Therefore, licensees’ efforts should aim at:

- Enhancing existing test programmes and procedures in order to render them more comprehensive. Assessing differences between plant conditions during testing and those expected to exist when the equipment is required to perform its safety function
- assessing modifications implementation by a better design control and subsequent requalification
- establishing post-maintenance testing requirements in order to verify the performance of repaired or replaced component and the functional requirements of the whole system.
• implementing appropriate instrumentation, monitoring or diagnostic techniques, for trending component performances in order to early identify causes of component malfunction that could become problems.

4. CORRECTIVE AND PREVENTIVE ACTIONS CONDUCTED BY LICENSEES AND REGULATORY ORGANISATIONS

Undetected failures of safety systems are of great concern especially when the failures remained undetected for a long time. Such deficiencies have been discovered in all nuclear activities from initial fabrication, design and installation, commissioning tests, in-service testing and maintenance. Recent events indicate that undetected failures of safety systems are still being discovered.

This difficulty to detect these problems in a timely manner indicates that existing means to demonstrate the functional capability of equipment to comply with regulatory requirements have to be used more efficiently or need to be upgraded.

System operability and reliability depends on high-quality design, procurement, installation, commissioning and periodic tests, and maintenance. In the light of the mentioned failures, the applicability of these failures to particular designs should be determined. This may be the joint responsibility of the regulatory organisations and utilities.

Means that have the potential for improving the effectiveness of latent deficiencies detection are to be found in:

• existing regulatory requirements
• findings and insights gained from operating experience

Section 4 of the report recalls the benefits that can be provided by periodical safety reassessments, probabilistic risk assessments, individual plant examinations and gives an overview of the specific findings, insights, and actions as reported in the individual contributions of the participating countries. Although these contributions identify the particular concerns resulting from their respective operational experience, some of the findings and insights could be useful to the different countries in their efforts to implement corrective and preventive actions. The report provides also additional relevant findings and insights resulting from generic studies on specific issues.

4.1 Regulatory Requirements

This section is related to insights gained in the course of the regulatory process in France and in the United States.

4.1.1 Periodic Safety Reassessments
Periodic safety reassessments (PSRs) are generally characterised as overall reviews of the safety status of NPPs. Their scope, relative to that of the initial safety reviews for operating licensees, varies considerably among countries that include such reviews in their regulatory process. Most countries with PSR programmes intend to perform such re-evaluations at intervals of roughly 10 years.

In France, one objective assigned to a PSR is to examine the current safety level of the reactor by comparison it with the standard adopted as the reference level for the initial design studies. This comparison provides a mean to appraise any degradation of the reactor that may have occurred since initial start-up. It also identifies reactor weak points that were not fully analysed or not well known at the time of the initial studies. Reference to operating feedback is indispensable to this objective. PSRs carried out every 10 years usually combines the following assessments:

- operational
- design review of equipment qualification to determine whether of the required equipment performance capability was initially ensured
- review of the initial start-up test programme
- validation tests on certain incidental or accidental procedures
- review of design specifications and actual operating conditions

For this purpose there is a need to investigate the adequacy and completeness of the set of design bases, as well as the design analysis and final design documents of the plant. These are important, since it is necessary to refer to these fundamentals in order to verify that structures, systems, and components have been designed to perform their intended function. In addition, these fundamentals constitute the basis for past and future modifications. The standardised designs of the French PWR units series permits to perform the PSR of identical units.

In addition, at the request of the DSIN, the IPSN performs every two or three years operating experience feedback assessments of all the French units. In the United States, PSRs are not required as part of the regulatory processes. Instead the NRC relies upon the following:

- a comprehensive set of regulations and surveillance requirements addressed to the licensees
- a strong and systematic inspection programme
- established programmes that continuously look for ways to improve safety
- the normal regulatory processes are supplemented by the Systematic Assessment of Licensee Performance (SALP). This programme collects and periodically evaluates (every 12 to 18 months) a wide range of safety-relevant information (such as licensee event reports, inspection reports, and enforcement history and licensing issues) in an integrated manner.

4.1.2 Decennial Inspections and Tests

French regulations stipulate that the reactor cooling system (RCS) hydrotest must be repeated every 10 years. This regulation also specifies that each hydrotest shall be
accompanied by an overall inspection of the entire system. These 10-year outages provide an opportunity for extensive control of the primary circuit. The DSIN also considers it imperative to take advantage of the special conditions associated with ten-yearly outages to perform different types of tests, in accordance with the following principles:

Start-up tests that were not initially performed on the first unit of the series, but were subsequently performed on the oldest units, in compliance with more recent requirements. Start-up tests that were initially performed in bounding conditions (such as loss of dc power sources).

Full system tests on certain safety functions, which have not been validated since, unit start-up. These tests constitute a mean of ensuring that safety criteria were respected for systems not in use during normal operation (notably the safety injection system and the containment spray system) and not covered by the IST programme. These systems may have deteriorated over time, as a result of natural ageing. In addition, full system tests offer the opportunity to assess the cumulative effects of plant modifications on design margins.

Validation tests on certain emergency operating procedures (EOPs). It is noteworthy that acceptance criteria for such tests could only be defined on the basis of the reference studies, which means that these studies may be reassessed.

Decennial inspections also give the opportunity to examine complex components. Such inspections permitted to discover cracks in reactor vessel head piping penetrations at Bugey 3 (IRS 1232.04) and in the casing of the RCP pump thermal barriers at Fessenheim 2. (IRS to be issued)

4.1.3 Probabilistic Risk Assessments

According to NRC and industry insights, probabilistic risk assessment (PRA) provides the most complete compilation of data and analysis to develop an integrated perspective to demonstrate an acceptable level of risk. In addition, PRA methods can identify human, procedural, design, and operation-related vulnerabilities that were not recognised by traditional methods.

PRA methodologies also offer significant benefits:

- methods to identify and evaluate various vulnerabilities and operational dependencies that exist between and among plant systems
- insights to identify, evaluate, and prioritise plant design modifications and procedures
- support for 10CFR59 reviews and evaluation of modifications
- support for procedural changes and technical specification improvements,
- practical means to explore and select cost-effective alternative solutions to plant vulnerabilities

Examples of vulnerabilities that have been identified by PRA are given in Appendix A to Generic Letter 88-20 "Individual Plant Examination for Severe Accident Vulnerabilities" which the NRC issued on November 23, 1988.
4.1.4 Individual Plant Examinations

In GL 88-20, the NRC requested that each nuclear power plant perform a systematic examination to identify any plant-specific vulnerabilities to severe accidents. As stated in this letter, licensees were expected to report their findings to the NRC and expeditiously correct any identified vulnerabilities.

IPEs reported vulnerabilities that were unlikely to be identified by other traditional methods. IPEs have also led licensees to implement where appropriate hardware and procedural modifications that would help prevent or mitigate severe accidents.

Through the IPE process, the industry has gained important insights regarding improvements in plant design as well as operational practices and procedures, to mitigate potential problems resulting from common dependencies in the CCW system. Several licensees have also identified that a common dependency in the CCW system (to provide cooling for RCP coolant seals and ECCS components) could significantly contribute to core damage frequency. In addition, licensees found that changes in plant operational practices and procedures or cost-effective global change in design could reduce the calculated core damage frequency (Turkey Point, Units 3 and 4, H.B. Robinson Unit 2, Watts Bar, Unit 1,-Diablo Canyon, Units 1 and 2, and Donald C. Cook Units 1 and 2). (IN 93-92)

4.2 Specific Corrective and Preventive Actions Conducted by Licensees and Regulatory Organisations

4.2.1 United States

Previous sections in this report describe specific actions conducted at the initiative of US licensees. These actions include among others design-basis reconstitution studies, and design basis accident re-analyses. In most cases, these actions were initiated following a PRA or IPE or on the basis of a particular event.

Regulatory actions issued by the NRC following these events are included in Gls and Bls. In addition, the NRC has initiated and conducted generic studies on specific issues.

After evaluating the resolution of the generic issue related to ESW system failure at multi-unit sites, the NRC staff concluded that the following administrative improvements would significantly enhance the availability of the ESW system:

- technical changes, including limiting conditions for operation (LCO) and surveillance requirements for at least two independent service water loops per unit, with the cross-tie between the service water systems of each unit in an operable condition (these are technical changes detailed in Enclosure 1 of GL 91-13)
- improvements of emergency procedures for a loss of service water using existing features:
- operating and maintaining high-pressure injection pump integrity in the event of loss of the RCP seal as a result of an ESW system failure,
• testing and manipulating the ESW cross-tie between the units during an accident involving a loss of ESW.

In GL 91-13, the NRC requested that affected plant licensees review the recommended TS and procedural improvements (listed above) to evaluate the applicability of those improvements at their respective facilities.

4.2.1.1 Findings and Insights gained from Operating Experience Feedback of Specific Issues

Insights and recommendations provided in the following generic studies for early detection and resolution of potential generic deficiencies could be very useful to all licensees. Moreover, some of these insights have more general implications that could be useful in improving testing and maintenance practices.

4.2.1.1.1 High-Pressure Coolant Injection System at US Commercial BWR Plants During 1987-1993

In 1995, at the request of the NRC, the Idaho National Engineering Laboratory performed an engineering evaluation of the HPCI operational data derived from LERs and the ASP data base in order to provide insights into the performance of the HPCI system throughout the industry and at a plant-specific-level.

This evaluation compared responses of HPCI turbines during IST and unplanned demands, as follows:

During surveillance tests, the HPCI turbine is not run for an extended period with varying flowrates, and the injection valve is not tested at rated pressure and flowrates.

The TS requirements for the surveillance tests do not require flow to the vessel or the governor to function for an extended period with varying flowrates. During unplanned demands, the HPCI system generally responds to the initial event and is placed in a full-flow test mode for reactor vessel pressure control or for future injection needs. However, the injection valve was observed to fail in 20% of the subsequent injection attempts.

The following insights were gained from this comparison:

• surveillance tests are effective in identifying problems associated with the HPCI system; however, there are a limited number of components (governor and injection valve) that are not fully tested in the manner in which they are operated during an unplanned demand.
• the largest contributors to surveillance test failures are the steam line MOV and turbine governor, however there have been no steam line MOV failures during unplanned demands.

This report provides an example in which deficiencies can be identified through analysis and equipment trending, as well as surveillance testing that duplicates service conditions as much as practical.
4.2.1.1.2 Reliability of Safety-Related Steam Turbine-Driven Standby Pumps

NUREG-1275, Vol.10 report, published in October 1994, reviewed operational failures of AFW, HPCI, and RCIC pump turbine assemblies, installed in US PWRs and BWRs. The purpose of the study was to gather and review available data on failures of standby turbine-driven pumps (TDPs) to identify failure mechanisms and corrective actions for feedback to the NRC staff and the industry. The findings and conclusions documented in this study are based on the following sources of information:

- a review of approximately 2000 LERs, and 660 failure reports from the Nuclear Plant Reliability Data System (NPRDS) from 1985 to 1992
- discussions with appropriate personnel at selected plants to gain a better insight into specific failures that had been reported
- discussions with the turbine and governors manufacturers to gain a better understanding of the components involved

Recurring failures identified during this study were reviewed to determine the root causes and failure initiators that had not previously been addressed in generic communications. This study indicated that plant-specific differences in such areas as system design, installation and environment, maintenance, installed modifications, surveillance testing, and failure reporting thresholds could result in variations in reported turbine failures. In addition, differences in surveillance testing methods were identified to determine why certain plants reported no failures of standby turbines and governors, while other plants had several failures.

PWR plants typically require monthly operability surveillance tests, which are typically initiated by a standby pump turbine quick start. Some tests involve hot quick-starts which are a quick start initiated after an initial cold-start during which any condensate in the inlet steam line is drained, and the system is warmed up and possibly checked for factors that could cause a quick-start to fail. (A standby turbine could trip on a cold quick-start because of viscous oil, but would not trip on subsequent starts after the oil had circulated and become more fluid. This would result in the initial overspeed being declared spurious or unknown).

TS for PWR and BWR plants typically require a simulated actuation of the automatic start of the turbine-driven AFW pumps (TDAFWPs) or the HPCI and RCIC pumps in accordance with the ASME/ANSI standard «Operation and Maintenance of Nuclear Power Plants» but this standard does not address the testing, or operability of pump turbine-drivers, which historically have been identified as the cause of the majority of failures of these standby pumps.

PWRs typically test and operate their TDAFWPs more often than BWRs. This affords a greater number of opportunities to detect failed conditions, that could make the turbine more vulnerable to cyclic wear if cold quick-starts are employed without adequate lubrication. This could be significant for plants that do not inspect or replace bearings every 5 years, as addressed in later manufacturer manuals.
Where TDAFWP tests are based solely on the satisfactory opening of the pump discharge valve, proper operation of the TDAFWP may not be verified since the discharge valve can open and the test can be terminated before the turbine reaches full speed and stabilizes. Tests have identified these valves opening in 8 seconds for turbines with governors that have a 30-second ramp bushing.

This report documents that improper maintenance (some of which result from inadequate incorporation of vendor recommendations or corrective actions) is a contributing factor in many failures of safety-related standby pump turbine-drivers. Therefore, it appears that licensees should thoroughly review and update their programmes for interfacing with vendors and other sources who could provide relevant technical information for safety-related standby turbine driven pumps. Coupled with incorporating such information in plant procedures, where applicable, such programmes could reduce the number of turbine-drivers failures.

4.2.1.3 Solenoid-Operated Valve Problems

NUREG-1275 Vol.6 report, published in 1991, analysed US light-water reactor experience with solenoid-operated valves (SOVs) from 1984 to 1989. This discussion addressed widespread deficiencies found in design and application, manufacture, maintenance, surveillance, testing, and feedback of failure-related data. It also focused on the vulnerability of safety-related equipment to common mode failures or degradation of SOVs that cut across multiple trains of safety systems as well as multiple safety systems. Common-mode SOV failures have compromised important safety systems and resulted in reduced safety margins.

The events in which common-mode failures of SOVs have affected multiple trains of safety systems are considered to be legitimate precursors to more significant events. These precursors indicate that actions are needed to ensure that important plant systems function as intended in accordance with plant safety analyses, and that plants are not subject to failures that have the potential for serious consequence. As a result of the findings, this report presented the following recommendations:

Verify the compatibility of the SOV design and plant operating conditions:

- Ensure that life-shortening effects of elevated ambient temperature and of heat-up resulting from coil energization are respectively considered in the determination of SOV service life
- Verify the adequacy of unrecognised SOVs used as piece parts of larger equipment (such as regulators emergency diesel support systems)

Implement SOV maintenance programme on a timely basis:

- account for thermal ageing when establishing the replacement frequency
- reduce the potential for common mode failures
- ensure that SOVs are not subject to fluid contamination.

Emphasise the importance of surveillance testing:
expressly prohibit mechanical agitation of SOVs (tapping) as a technique to assist successful operation during surveillance testing. Many SOVs failures that were observed during surveillance testing were not reported and the SOVs were not repaired. The primary reason was that the SOVs that failed to operate during surveillance testing operated properly after being “tapped” by plant personnel. As a result, repetitive malfunctions were observed, the malfunctioning SOVs were not fixed or replaced expeditiously, and the root causes were not found or corrected on a timely basis. In addition SOVs were declared operable without addressing the cause of the original failures, thus leaving the SOVs in a degraded state vulnerable to future failures upon demand.

- Include actions to be taken when unsatisfactory test results are encountered, as well as a requirement to analyse and evaluate the causes of the unsatisfactory results before declaring the component back in service (even though subsequent re-test results may be satisfactory).

- consider staggering surveillance testing.

- review all SOVs in safety-related applications (as well as applications that support safety-related systems), particularly EDGs, to ensure that they meet the regulatory requirements, and that they have been installed and maintained commensurate with their safety functions.

- give additional consideration to using diverse SOVs (different designs or manufacturers).

4.2.1.2 Insights on Licensee’s Corrective Actions Related to Undetected Failures of Safety Systems

For their contribution to this particular generic study, the United States provided PWG-1 with a comprehensive study based on a set of 33 events identified by a search of the ASP database for selected period, 1991 through 1993 (among these 33 events, 12 are related with long duration failures and were reviewed in part I of the report).

The failures were analysed and evaluated with respect to their discovery methods, failure rate and trend, failure causes, corrective and preventive actions by the licensees, and regulatory actions. The purpose of the evaluation was to gain insights from such failures which could be useful in preventing or reducing the likelihood of such failures.

The specific conclusions related to licensees corrective actions and preventive actions resulting from this evaluation are the following:

The licensees’ analyses of events indicated that the failures were more frequently caused by component failure, design deficiency, and inadequate testing or maintenance procedures. All of these deficiencies could be reduced by appropriate corrective or preventive actions. The more frequent corrective and preventive actions the licensees took were design
change (plant modification), new or change in operating procedure, additional training or
guidance to plant personnel, and change to maintenance procedure. Although the licensees’
actions appeared appropriate for the specific events, it is not clear the efforts would
generically apply to other plants

4.2.2 Spain

After the occurrence of events described in IRS 1307 and 1506 related to design
and/or construction deficiencies at Trillo NPP, the licensee for this plant perceived the need to
carry out a systematic, overall programme to identify other possible hidden deficiencies. The
licensee unveiled to Consejo de la Seguridad Nuclear (CSN), in November 1994, a vast
programme named Analysis of Operating Experience and Systems (AOES). This programme
was defined to apply to all plant safety systems or systems included in plant TS.

(Trillo is an adaptation of a standard 4 loop plant to a 3 loop plant. The 4 loop
plant has 4 trains of ECCS, nuclear component cooling system (NCCS), essential service
water system (ESWS), etc., physically, hydraulically and electrically separated. Trillo has 3
independent trains of ECCS, NCCS, plus a fourth train of ESWS, emergency ac- with 4 EDGs
and dc power, and other systems, that can be connected to any of all other three, in such a way
that is able to substitute any of the other 3 trains, under some rules. Besides, each train of
NCCS contains valves, interlocks, etc. fed from different electrical busses of ac and dc power.
The multiple combinations of inoperabilities and/or single failures of any electrical bus
produce multiple scenarios not always covered by the plant design).

The goal of the programme was to ensure, by systematic design, construction, and
commissioning review, the adequacy of safety systems, structures and components to fulfil their
safety functions. As a result of the programme, it was decided to perform a reconstitution of the
plant design-basis, consisting of a complete, unambiguous, systematic, design-basis definition
and a complete document review of the plant design.

The main organisations engaged in the programme are Trillo NPP, Siemens KWU
- NSSS supplier- and Empresarios Agrupados -the architect engineer. The overall programme
scope and methodology were subjected to regulatory approval and the regulatory staff reviewed
and required some changes to be included in the programme-related procedures.

Diverse existing review procedures defined for similar purposes, such as NSAC 121
NUREG1397 and NUMARC 90-12, were used as references in the programme scope definition,
specially for the design basis review area.

The programme was structured in seven main areas of review: design-basis,
commissioning tests, reactor protection system, operating experience, plant specific design
features, adequacy and completion of construction, "open Items", design changes.

The programme started in January 1995 and is expected to be completed by the end
of 1996, however, definitive resolution of some issues resulting from the programme will be
deferred from this date, e.g., design modifications of the electrical distribution system is planned
to be designed by October 1996, its actual implementation is scheduled for at least one year later
though.
Most safety significant findings of the AOES programme identified so far are the following:

Deficiencies of the residual heat removal Chain (ECCS/CCW/ESW)

Several cases were identified where the residual heat removal chain did not fulfil the design criterion "N + 2" (this criterion requires that the system shall have enough redundancy to fulfil its safety function assuming the worst single failure and one train unavailable for maintenance). The necessary design changes were identified and recently implemented, in the interim the allowed unavailability of every train of the chain was severely limited.

Deficiencies in the emergency feedwater system

A deficiency was related with no compliance of "N + 2" criterion in certain scenarios. Design changes were introduced to cope with this issue, in the interim administrative compensatory countermeasures were required. Another one included wrong setting of flow control valves of the system, because commissioning process mistakes. The required changes were implemented right after the discovery of the deviation.

Deficiencies in ac. plant systems

A complete in depth ac. systems review has been started, as result of diverse detail deficiencies shown in the design. According to the conclusions gathered so far, safety functions are not jeopardised by these deficiencies, but divers design changes will be recommended to cope with weaknesses of the ac. systems, such as very little power margin of some big transformers and some cable sections.

Deficiency in the HVAC system design of the emergency feedwater building

The specified temperature for the heating, ventilation and air conditioning) system design of the emergency feedwater building, where most of the RPS cabinets are located, is 40°C, a figure apart from the design temperature required by applicable codes and the temperature used for HVAC system design in similar plants: 35°C. This point is important to ensure adequate electronic components behaviour in case of an accident involving LOOP. A complete review of the affected HVAC system has been started to incorporate the required design temperature; meanwhile, an evaluation has been carried out to assess the power dissipated by the electronic devices of the cabinets and whether or not they would overpass or not the manufacturer temperature specification.

A relatively high number of deficiencies have been identified in piping supports and snubbers (22 cases of deviations in this area). Because of the relative high number of the deficiencies, a complete on field review of piping support and snubbers has been started.

A remarkable feature of the programme is that it may open up new revision areas, although these have narrower scope. e.g. upon completion of the operating experience review, 11 new areas were opened up, such as review of primary coolant system thermal isolation
regarding its design of thermal efficiency or review of the design interface between two specific manufacturers of certain valves and their actuators

Main lessons that emerged from this review to guarantee operability of the safety systems emphasise the need of:

- an integrated comprehensive IST programme, both for certifying the acceptance of safety systems during construction and for functional tests at commercial operation

- test conditions reproducing real conditions as much as reasonably achievable

- supplementing step by step tests for functional tests at power and verification of individual components, with integrated tests (sensor to final device actuation), in order that system deficiencies do not remain unnoticed to component tests.

4.2.3 **Belgium**

In its contribution to this generic study, AIB-VINCOTTE NUCLEAR (AVN) underlines that the few failures collected for Belgium appear to be related to design and component qualification, and/or to phenomena not well known at the design stage, but not on testing and maintenance testing. AVN rather emphasises the role played by the decennial revision studies in discovering these failures which not only allowed to discover them through more severe testing procedures and through a questioning attitude in the studies, but also provided the opportunity to find more refined solutions to problems which may have been detected in another context.

4.2.4 **Finland**

Based on incidents related to modifications performed at Finnish plants, SATEILYTURVakeskus (STUK) underlines the importance of clearly defined and strictly followed modification processes. For this purpose, STUK has started a study to define the requirements for different phases of the modification process and to evaluate the modification procedures in use at NPPs. This study has yielded following recommendations:

Plants should pay more attention to determining the functional tests after successful modification works so that the tests adequately cover the possibilities of latent failure, with emphasis on the testing of valves in real flow conditions.

The need for independent inspections should be reviewed with care, especially if there are doubts concerning the effectiveness of the tests, which are always the primary defence mechanism against latent failures.

Increased attention should be paid to motivating the maintenance staff to minimise the likelihood of dependent errors.
Attention should be given to work orders and work procedures in general to avoid omissions in routine tasks.

A more detailed study financed by STUK is in progress concerning dependent errors in maintenance tasks at TVO and Loviisa NPPs.

4.2.5 Sweden

The Swedish contribution underlines that the most effective single corrective action category to prevent the occurrence of undetected failures in safety systems is a more systematic, thorough and realistic operational readiness control and testing after maintenance and modification activities. As such testing and control represent often the last barrier after performed maintenance or repair to detect component and system deficiencies, and prevent events, the contribution concludes that operational readiness control should accordingly encompass not only the modified or repaired component(s), but should also include integral system testing and even be extended, on a case by case basis, to testing of the complete relevant safety function.

In addition, as efficient corrective actions, plant management should re-emphasise for the concerned personnel the primary importance of careful work package preparation, which presuppose that enough time has been allocated before the annual refuelling outages for the preparation and an independent checking of these work packages.

Swedish Projects “Boka” and “Reda”

Following the Barseback event, Swedish utilities initiated comprehensive projects for the systematic assessment of the safety criteria to be fulfilled by the NPPs (BOKA project for Barseback and Oskarshamn, Reda project for Ringhals. A similar project, RAK is ongoing for the Forsmark units). All these exhaustive projects, which encompass furthermore the eventual identification of safety weaknesses in the plants’ design, are performed by the vendor in close co-operation with the utilities. Existing safety reports, background reports, experiment results and design construction reports are reviewed in depth by multi-disciplinary groups. These reviews are made in the light of today’s safety requirements. The actual projects which represent more than 300 person-years of studies, were initiated in 1994-95 with a report time to year 1998.

4.2.6 France

Repeated failures during in-service testing, post- maintenance testing and implementation of plant modification have been a concern for EDF, DSIN, and IPSN. During recent years, this concern led to a reassessment of current licensee’s practices during these activities. This reassessment resulted in many EDF efforts to implement innovative measures to better sensitise plant personnel to the impact of these activities. New IST requirements have been included in the GOR. In addition, the remainder of this section presents an overview of the directives that have been addressed to the different units with regard to following activities:

- requalification tests
- modification implementation
- installation of temporary devices

In accord with an IPSN initiative and DSIN request, pre-start meetings are held to inform EDF, IPSN and DRIRE representatives of possible anomalies and difficulties that may be encountered during IST and maintenance operations. This information permits representatives to judge if corrective actions taken by a utility are satisfactory and to determine, at an early stage, that the plant will operate safely during the next cycle. A brief summary is given of the statements made by IPSN during these meetings.

Of considerable interest are the lessons learned from endurance tests performed during commissioning tests with containment spray pumps. These tests illustrate how an early and effective involvement of plant safety can anticipate component malfunctions.

In addition various guides have been established, including a practical guide proposing a method to help plants perform a safety analysis of events.

4.2.6.1 In-service test programme

EDF has improved the methodology used by its engineering units to implement a comprehensive IST programme. This methodology has been backfitted to give new guidance and complementary testing requirements for review of components and structures that were never tested in actual conditions.

The new guidance and requirements are particularly relevant for components and structures used in emergency operating procedures (EOPs) and beyond-design procedures. (these procedures, called ‘H’, specify the actions to be taken in the event of situations leading to total loss of, the ultimate heat sink, steam generator feedwater, electrical power supplies.)

EDF has also established a doctrine on IST to help operators to implement test procedures and analyse test results during plant operation. The main principles and requirements of this doctrine have been introduced in the GOR after approval by the DSIN.

The safety criteria to be selected for equipment and systems as LCO have been clarified and justified from both functional and reliability points of view. Criteria and requirements for acceptance surveillance test results have been categorised as follows:

- completely satisfactory
- partially satisfactory
- unsatisfactory

A periodic test is considered satisfactory if conditions are met with regard to initial test conditions, test results, successful test achievement at the first trial, and other various conditions.

Adequate guidance is given to plant personnel with regard to actions to be taken when partially satisfactory and unsatisfactory surveillance test results are encountered. This guidance specifies actions to be taken, to analyse and evaluate the causes of the unsatisfactory
results before declaring the component or the system back in service, even though subsequent retest results may be satisfactory.

4.2.6.2 Requalification Tests

The purpose of requalification tests is to ensure that design stage requirements involving plant equipment or system are still fulfilled following an intervention (maintenance, modification, etc.).

Such testing needs to be carried out each time maintenance work is performed or modifications are made on all or part of a system. When a test is technically feasible, it is the only effective mean to guarantee the actual operability of a system.

The analysis of maintenance-related incidents has shown that the line of defence constituted by requalification has not always properly played its role. It has become apparent, that requalification tests can be inadequate or fail to correspond to their intended goal. Examples are numerous in which inadequate or non existent requalification failed to reveal certain deficiencies.

As early as 1990, EDF began a critical analysis of the safety-related equipment requalification tests. It became clear that the requalification tests specific to the equipment, were generally performed correctly by the operators. However, it is necessary to supplement those tests with functional tests in order to verify the sequences, automatic functions, operation of actuators, circulation of fluid and performance levels of the system involved.

In certain cases, IPSN found that the operators did not possess a clear doctrine concerning the need for functional tests and that those in charge of the tests in the plants select requalification tests on the basis of their own knowledge and awareness. EDF central services, therefore compiled a list of periodic tests that may be used for requalification.

According to the IPSN, IST is an adequate response in certain cases but is inappropriate for certain maintenance operations. The purpose of periodically assessing system performance in the absence of maintenance tests is indeed to ascertain the durability of that performance. In fact, the only effective method of ensuring the performance levels of a system after certain interventions is to repeat tests performed during commissioning.

Operators found it difficult to apply such a policy, although they have a thorough knowledge of IST, they have only a limited knowledge of the initial start-up tests, (either because the length of time since commissioning of the plants, or because the individuals who carried out the tests are no longer present). IPSN also found that the workload of the personnel in charge of the tests during the restart period is difficult to reconcile with an adequate quality of the analysis and verifications in the available time.

Two types of procedures may be used to perform requalification tests during refuelling outages:

- Starting-up test procedures describe tests that enable a plant to go to an operation mode. These procedures have to be complete and must permit to
check all of the required functions. They require a plant status that may not be compatible with a refuelling outage and so may need to be adapted.

- In-service test worksheets are used to perform IST during the entire life of the plant. They can be used without any adaptation; however, they are often insufficient to ensure a complete system requalification.

To requalify a system following maintenance, repair, or modification, it is necessary to verify that the affected components work satisfactorily and that the functional requirements of the entire system are fulfilled. This involves identifying both component and system-level requirements and establishing the post-maintenance operability testing to demonstrate that the system is capable of performing its intended function before to returning it to service.

Requalification may also require interdisciplinary competencies depending on the scope and complexity of the intervention (representatives of maintenance, automatism, operating branches etc.).

In many cases, it appears that requalification tests performed by plant personnel were not exhaustive (because they were limited to reproducing IST), and they lacked the required quality, which led to situations in which safety-related systems were unable to correctly fulfil their intended functions, without plant personnel being aware of the situation. Moreover, organisational practices differ from plant to plant.

In order to enhance the post-maintenance requalification process, EDF has addressed a directive to the plants. This directive is intended to ensure consistency among plant-specific practices for adequately controlling modifications. This directive enumerates the following principles:

- The requalification process is generally performed in successive steps, starting with the component requalification (intrinsic) and ending with the system requalification (functional).

- Requalification is an integral part of the intervention. Any intervention (scheduled or fortuitous) has to be prepared in advance. This preparation involves the following factors:
  - the necessity or not of the requalification,
  - the type of testing (operating mode, acceptance criteria),
  - the complementary or compensatory measures deemed necessary if no test is adapted
  - the way to keep track of the different documents related to the preparation implementation, and results of intervention.

Requalification tests require different competencies, and responsibilities must be clearly defined during the preparation phase.
Co-ordination is necessary for all requalifications. Means and necessary competencies have to be defined in order to:

- insure exhaustiveness of requalification with relevant interventions or modifications
- verify the consistency between the sequences of intrinsic and functional requalification
- perform an overall test synthesis and take the decision of declaring the component or system operability.

4.2.6.3 Implementation of modifications

In order to upgrade the EDF 900 MWe and 1300 MWe units to the status of the latest generation of these unit series, modifications have to be incorporated. Owing to the standardised French nuclear programme, EDF has adopted a consistent backfitting policy to integrate these modifications according to a batch refit procedure.

Typically a modification is carried out on a ‘first-of-the-kind’ plant, but the decision to extend the modification to other plants is only made once satisfactory backfitting on the operability of the first implementation has been gathered. This process allows improvements in implementation quality. The installation instructions for the modifications are developed by the EDF Engineering Department and incorporated in the modification package when it is issued to the plants.

The modification package includes all the elements enabling:

- to have a precise idea of the goal to be reached and the corresponding means to achieve it
- to implement the modification on the concerned plants and to perform the necessary requalifications
- to take into account the consequences induced by the modification on operating documents (TS, testing and maintenance procedures, emergency operating procedures, operating rules)
- to know exhaustively all of the design bases and engineering documents affected by the modification

Testing requirements (including acceptance criteria) are delineated to demonstrate that the modification has been satisfactorily implemented and to verify compliance with the required surveillance’s.

Requalification of this type of modifications, differs from post-maintenance requalification testing. These modifications are decided at a national level and are not considered as safety concerns. Before a modification may be implemented, the potential consequences are evaluated exhaustively, procedural changes such as component replacements have been performed to establish specific requalification procedures.

In addition, certain modifications involving safety-related systems must be approved by the DSIN before they may be implemented.
Installation of Temporary Devices

Installation of temporary devices may be needed in certain maintenance operations and various tests carried out during unit shutdown in order to inhibit protective actions or to isolate circuits or components for interventions. These devices are mainly used during outages and pre-start operations. In a few cases, they may be also used for periodic tests or fortuitous interventions during plant operation in configurations not provided by design.

Installation of temporary devices induces a safety risk because most of these devices cannot be operated or monitored by control instrumentation; therefore, their safe use relies mainly on the quality of management. Failure to detect their presence, or to recover them after use, may have potentially adverse consequences on safety.

The means to avoid recurrence of such incidents are well known; they rely on a rigorous management of the devices and on performance of qualifications tests whenever possible. Since 1990, in response to a DSIN request, EDF has engaged in efforts to identify, list, and analyse temporary devices used to perform testing, in order to reduce their number.

Representatives of EDF Central Services and of different units and different disciplines have been associated in working groups in order to define appropriate means to mitigate the following causes of incidents:

- failure to identify a risk related to installation of a temporary device
- deficiency in temporary device management
- deficiency of a local signalling device
- failure to restore to the initial configuration after use of a temporary device

By the end of year 1993, these working groups had produced two documents aimed at making uniform the operator practices at different sites. The first document is a directive specific to the definition and management of temporary devices. This directive establishes the following operator requirements:

- perform a risk and need analysis in order to bring the risk under control
- manage (administratively) all temporary devices
- signal any positioned temporary device
- make sure of temporary device withdrawal

The directive also specifies that administrative management depends on ensuring the permanent and exhaustive traceability of temporary devices in the installation.

The second document produced by the EDF working groups is a practical guide with recommendations identifying the main families of permitted temporary devices. This guide also gives examples of incidents, some of which resulted from use of prohibited device.

Restarting Operations

94
During annual refuelling outages, plants perform numerous tests including those required by the GOR, and those necessary to verify that preventive maintenance operations and modifications have been performed correctly. All of these tests have to demonstrate that a satisfactory level of plant availability and safety has been reached by the operator when restarting the plant.

At the request of the DSIN, the utility must ensure that the safety level of the plant has been correctly assessed before restarting. To do so, the utility must present to the IPSN a synthesis of the main test results during a pre-start meeting a few days after the plant has reached 90 percent of its rated power.

When examining the test results, the main objective assigned for the IPSN during these pre-start meetings, is to become aware of possible anomalies and difficulties encountered during IST and maintenance operations. Based on that awareness, the IPSN can then determine, at an early stage, whether corrective actions taken by the utility are satisfactory, and whether the plant will operate safely during the next cycle.

The presence of the IPSN test engineer at these meetings also favours prompt feedback of experience concerning the appropriate treatment of similar difficulties that may be encountered by other units. This feedback encourages coherence in the practices used by different utilities to remedy these problems.

The typical agenda prepared for these meetings includes the following items:

- general presentation of test results and problems encountered
- plant organisation for IST preparation, implementation, follow-up, and analysis of tests results
- requalification tests associated with to modifications or maintenance works, either preventive or fortuitous, performed on safety features systems and some safety-related systems
- periodic tests performed on safety features systems and some samples of safety-related systems.

This agenda may be modified according to specific concerns raised by the IPSN representatives taking into account the plant history, problems encountered at other units, and generic problems.

The pre-start meeting is held a few days after the plant has reached 90 percent of its rated power, as soon as the analysis of test results by the utility is available. The meeting is attended by the IPSN engineer in charge of the in-service tests, the IPSN engineer in charge of the plant, and a representative of the Regional Directorate for Industry Research and the Environment (DRIRE). Tests results are presented by the plant operating team. In addition, various branches involved in the tests participate at the meeting or may be called on if needed.

When examining tests results, the IPSN gives priority to those included in the IST programme of the GOR, which have to satisfy safety criteria. The IPSN also takes advantage
of the opportunity to assess operator practices by requesting and examining additional information on items such as the following:

- adequacy of operating requalification mode for a specified intervention
- adequacy of the tests means and measurement methods
- validity of tests configurations
- operating history

The utility then sends DSIN a restart telex that includes an inventory of the points examined during the meeting, any cautions expressed by the IPSN, and resulting operator commitments to resolve any remaining anomalies or non-conformances.

Based on a review of the numerous statements made by the IPSN during these meetings with regards to the causes of identified deficiencies, it appears that the following areas most frequently suffer deficiencies and need improvements:

The onsite organisation does not always seem well suited to guarantee the exhaustiveness of requalification. This is particularly true when an intervention and its requalification rely entirely on outside contractors, or when multiple participants from different disciplines operate without having defined organisational responsibilities capable of ensuring that interfaces are tightly controlled and that tasks are carried out as defined.

Test procedures and worksheets need to be enhanced to be clear, unambiguous, and more precise with regard to the prerequisites related to system configuration, the accuracy of test results and the margins tolerated for safety criteria.

Delays in introducing an effective safety culture are illustrated by improper testing practices. For instance, repetitive testing to achieve acceptable test results without identifying the root cause of a problem in a previous test has not completely disappeared. On the other hand, serious and satisfactory actions have been implemented for component trending.

4.2.6.6 Site Endurance Tests

At the request of the IPSN, EDF agreed to perform a 2000-hour site endurance test of a containment spray pump to investigate the vibratory behaviour of this equipment with the pump recirculating via the sump and the RWST. The 2000 hours period was determined to be the duration required to obtain an appropriate response of the vibratory behaviour of the pump in operation. EDF included this test in the commissioning test programme of St. Alban NPP.

The shaft of the pump is vertical, with the motor on one floor driving the pump on a lower floor (There are approximately 4 meters between the motor and the pump.) via a shaft with universal joints and a splined joint.

The test was interrupted on a number of occasions due to the following factors:

The appearance of pump vibration peaks revealing inadequate lubrication before the test, since these peaks disappeared after lubricating the bearings. This deficiency
illustrates the importance of lubricating such equipment, which is not accessible in accidental conditions.

Motor vibration peaks appeared, throughout the test, during sump recirculation, particularly when the water temperature was at its maximum. These vibrations disappeared after shutting down and restarting the electric motor (because the design of the motor bearings and the stiffness of the joint).

Analysis revealed that the expansion of the pump body, caused by the progressive heating of the sump water resulted in lifting of the electric motor rotor with coupling problems.

This type of situation could reoccur in the event of an accident when switching the pump suction line from the cold water in the RWST to the hot water in the reactor sumps.

The lessons learned from such an anomaly are related to the importance of carrying out onsite endurance tests which identified lubrication and coupling problems of the containment spray pumps during their continuous operation.

For some equipment, the demonstration of availability was carried out by means of long duration tests at the site. It has become clear that qualification of a machine, such as a pump set, must be supplemented by an endurance test, in addition to the manufacturer tests (verification of the construction specification) and testing on a bench loop (qualification to accidental conditions).

In addition, to verify proper adaptation to actual operating conditions, tests must be performed under prolonged operating conditions, to reveal any anomalies undetected by other tests. This is particularly important for those engineered safety system pumps that never operate for long periods during normal operation.

Similar tests were successfully repeated with safeguard pumps and emergency diesel engines during the N4 series commissioning tests.

4.3 Conclusions

Participating countries have emphasised their topics for consideration in preventing or reducing the likelihood of latent failures. Potential problems have been identified and related corrective or preventive actions have been yet implemented or will be defined after completion of reviews that are still in progress.

These corrective actions are in many cases supplemental actions to the normal regulatory process conducted either at the only initiative of the licensees or the regulatory organisations or sometimes in close cooperation.

In Spain, following the late discovery of design deficiencies at Trillo NPP, left undetected by commissioning tests and during many years of commercial operation, and because of the specificity of this plant which is an adaptation of a standard 4 loop plant to a 3 loop plant, the licensee perceived the need to carry out a systematic overall assessment programme and
started a wide review of plant design, construction and commissioning which has permitted to
discover different deficiencies. Main lessons that have emerged from this review to guarantee
operability of the safety systems emphasise the need of an integrated comprehensive IST
programme, both for certifying the acceptance of safety systems during construction and for
functional tests at commercial operation.

The role played by the decennial revision studies in discovering latent failures has been
emphasised by Belgium. These studies not only allowed to discover them through more
severe testing procedures reproducing real conditions and through a questioning attitude in
the studies, but also provided the opportunity to find more refined solutions to problems
which may have been detected in another context.

Sweden underlines the role of thorough and realistic readiness control and testing after
maintenance and modification activities. However, Sweden mentions that the eventual
identification of safety weaknesses in the plants' design would result from comprehensive
projects initiated by the licensees after the Barseback incident for the systematic assessment
of the safety criteria to be fulfilled by the three types of NPPs.

Efforts in Finland have been focused on the definition of the requirements of the different
phases of the modification process and the evaluation of the modification procedures in use
at the NPPs. Moreover a study is in progress concerning dependent errors in maintenance
tasks.

In the United States, in addition to actions required in the generic letters and bulletins, main
efforts have been dedicated by the NRC to the early detection and resolution of potential
generic deficiencies. Insights and recommendations provided in NRC sponsored generic
studies on operating experience feedback of specific issues to US NPPs and which have
general implications that may be relevant to many national and foreign facilities in improving
their testing and maintenance practices.

In France, reassessment of current licensee's practices during in-service testing, post-
maintenance testing and implementation of plant modifications have led the licensee to
implement innovative measures to better sensitise plant personnel to the impact of these
activities. New in-service testing requirements have been introduced in the general operating
rules including guidance to personnel to analyse tests results. Actions have been implemented
to verify post-outage testing. Moreover, onsite endurance tests on engineered safety system
pumps have illustrated how an early and effective involvement of plant safety can anticipate
component malfunctions.

Considering countries specificities in: regulatory practices, problems encountered, number,
type and variety of power plants of similar design, different approaches to problem resolution
have been adopted involving more or less extensive studies.
Regardless of the countries, all these approaches confirm to some degree that continuous
efforts are needed to:

• enhance existing test programmes and procedures in order to render them more
  comprehensive. Assess differences between plant conditions during testing and
those expected to exist when the equipment is required to perform its safety function

- assess modifications implementation by a better design control and subsequent requalification
- establishing post-maintenance testing requirements in order to verify the performance of repaired or replaced component and the functional requirements of the whole system.
- implementing appropriate instrumentation, monitoring or diagnostic techniques, for trending component performances in order to early identity causes of component malfunctions that could become problems

Aforementioned observations, findings and insights should be reviewed by licensees for applicability to their own facilities, if effectively applied they should contribute to minimise the occurrence of latent failures.
## ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADS</td>
<td>automatic depressurization system</td>
</tr>
<tr>
<td>AFW</td>
<td>auxiliary feedwater system</td>
</tr>
<tr>
<td>AIT</td>
<td>augmented inspection team</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standard Institute</td>
</tr>
<tr>
<td>AOES</td>
<td>Analysis of Operating Experience and Systems (Spain)</td>
</tr>
<tr>
<td>AOT</td>
<td>allowed outage time</td>
</tr>
<tr>
<td>ASME</td>
<td>American Society of Mechanical Engineers</td>
</tr>
<tr>
<td>ASP</td>
<td>accident sequence precursor</td>
</tr>
<tr>
<td>ATWS</td>
<td>anticipated transient without scram</td>
</tr>
<tr>
<td>AVN</td>
<td>AIB- Vinçotte Nuclear (Belgium)</td>
</tr>
<tr>
<td>BAT</td>
<td>boric acid storage tank</td>
</tr>
<tr>
<td>BL</td>
<td>bulletin</td>
</tr>
<tr>
<td>BWR</td>
<td>boiling water reactor</td>
</tr>
<tr>
<td>BWST</td>
<td>boric water storage tank</td>
</tr>
<tr>
<td>CARHK</td>
<td>containment air return and hydrogen skimmer</td>
</tr>
<tr>
<td>CCWS</td>
<td>component cooling water system</td>
</tr>
<tr>
<td>CSNI</td>
<td>Committee on the Safety of Nuclear Installations</td>
</tr>
<tr>
<td>CSN</td>
<td>Consejo de la Seguridad Nuclear (Spain)</td>
</tr>
<tr>
<td>CVCS</td>
<td>chemical and volumetric control system</td>
</tr>
<tr>
<td>DBA</td>
<td>design-basis accident</td>
</tr>
<tr>
<td>DRIRE</td>
<td>Direction Régionale de la Recherche et du Dévelopement (France)</td>
</tr>
<tr>
<td>ECCS</td>
<td>emergency core cooling system</td>
</tr>
<tr>
<td>EDF</td>
<td>Electricité de France</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>EDG</td>
<td>emergency diesel generator</td>
</tr>
<tr>
<td>EOP</td>
<td>emergency operating procedure</td>
</tr>
<tr>
<td>ESF</td>
<td>emergency safety feature</td>
</tr>
<tr>
<td>ESFAS</td>
<td>emergency safety feature actuation system</td>
</tr>
<tr>
<td>FSAR</td>
<td>final safety analysis report</td>
</tr>
<tr>
<td>GE</td>
<td>General Electric</td>
</tr>
<tr>
<td>GL</td>
<td>generic letter</td>
</tr>
<tr>
<td>GOR</td>
<td>general operating rules</td>
</tr>
<tr>
<td>HHSI</td>
<td>high head safety injection</td>
</tr>
<tr>
<td>HPCI</td>
<td>high pressure coolant injection</td>
</tr>
<tr>
<td>HVAC</td>
<td>heat, ventilation and air conditioning</td>
</tr>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>IN</td>
<td>information notice</td>
</tr>
<tr>
<td>IPE</td>
<td>individual plant examination</td>
</tr>
<tr>
<td>IPSN</td>
<td>Institut de Protection et de Sûreté Nucléaire (France)</td>
</tr>
<tr>
<td>IRS</td>
<td>incident reporting system</td>
</tr>
<tr>
<td>IST</td>
<td>in-service testing</td>
</tr>
<tr>
<td>LCO</td>
<td>limited condition of operation</td>
</tr>
<tr>
<td>LDST</td>
<td>letdown discharge storage tank</td>
</tr>
<tr>
<td>LER</td>
<td>licensee event report</td>
</tr>
<tr>
<td>LOCA</td>
<td>loss of coolant accident</td>
</tr>
<tr>
<td>LOOP</td>
<td>loss of offsite power</td>
</tr>
<tr>
<td>LPCI</td>
<td>low pressure coolant injection</td>
</tr>
<tr>
<td>LPCS</td>
<td>low pressure coolant spray</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>MCB</td>
<td>miniature circuit breaker</td>
</tr>
<tr>
<td>MOV</td>
<td>motor operated valve</td>
</tr>
<tr>
<td>MSL</td>
<td>main steam line</td>
</tr>
<tr>
<td>MSLB</td>
<td>main steam line break</td>
</tr>
<tr>
<td>MSS</td>
<td>main steam system</td>
</tr>
<tr>
<td>NCCS</td>
<td>nuclear component cooling system</td>
</tr>
<tr>
<td>NEA</td>
<td>Nuclear Energy Agency</td>
</tr>
<tr>
<td>NER</td>
<td>nuclear experience review</td>
</tr>
<tr>
<td>NPP</td>
<td>nuclear power plant</td>
</tr>
<tr>
<td>NPRDS</td>
<td>Nuclear Plant Reliability Data System (US)</td>
</tr>
<tr>
<td>NPSH</td>
<td>net pressure suction head</td>
</tr>
<tr>
<td>NSSS</td>
<td>nuclear steam system</td>
</tr>
<tr>
<td>NUMARC</td>
<td>Nuclear Management and Resources Council (US)</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>PHWR</td>
<td>pressurised heavy water reactor</td>
</tr>
<tr>
<td>PRA</td>
<td>probabilistic risk assessment</td>
</tr>
<tr>
<td>PSR</td>
<td>probabilistic safety review</td>
</tr>
<tr>
<td>PWG-1</td>
<td>Principal Working Group No. 1</td>
</tr>
<tr>
<td>PWR</td>
<td>pressurised water reactor</td>
</tr>
<tr>
<td>RCIC</td>
<td>reactor core isolation cooling</td>
</tr>
<tr>
<td>RCS</td>
<td>reactor coolant system</td>
</tr>
<tr>
<td>RHR</td>
<td>residual heat removal system</td>
</tr>
<tr>
<td>RPS</td>
<td>reactor protection system</td>
</tr>
<tr>
<td>RSHX</td>
<td>recirculation spray heat exchanger</td>
</tr>
</tbody>
</table>
RW        raw water
RWST      radwaste storage tank
SALP      systematic assessment of licensee performance (US)
SG        steam generator
SGTR      steam generator tube rupture
SI        safety injection
SIRWT     safety injection recirculating water tank
SKI       Swedish Inspectorate
SOV       solenoid operated valve
SOIV      solenoid operated isolating valve
SQA       Safety Quality Approach (France)
SRV       safety relief valves
SSAR      standard safety analysis report
SSFI      safety system functional inspection
SSPS      solid state protection system
STUK      Sateilyturvakeskus (Finland)
SWS       service water system
TDP       turbine driven pump
TS        technical specification
TVO       Teollisuuden Voyma Oy (Finland)
UPS       uninterruptible power sources
VCT       volumetric control tank
LATENT FAILURES OF SAFETY SYSTEMS

A generic study performed by the Principal Working Group 1 on Operating Experience and Human Factors
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

************

The opinions expressed and the arguments employed in this document are the responsibility of the authors and do not necessarily represent those of the OECD.

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France
This volume contains copies of the full text of the reports provided by the participating countries. The French contribution has been directly incorporated in the main report.
CONTRIBUTION FROM BELGIUM
Belgian contribution to the PWG1 Generic Study on
Undetected Failures of Safety systems

by Marc Vincke

Contents
1. Introduction
2. Selected cases
   2.1 Non qualification of steam-line valve control organs to an environment with steam (DOEL 2, June 1980)
   2.2 Deviation of flow rate control system of reactor building cooling ventilators (DOEL 1, January 1986)
   2.3 Primary leak caused by thermal fatigue induced by a cyclic cold water discharge through a leaking closed ECCS valve (Tihange 1, June 1988)
   2.4 Improper operation of drain system causing damage on the auxiliary feedwater turbine driven pump (DOEL 2, August 1990)
   2.5 Possible unavailability of diesel generators in case of blackout following a safety injection signal due to an improper temporisation (DOEL 3, September 1991)
   2.6 Incomplete design basis accident qualification of electrical equipment (June 1992)
3. Summary and discussion
   3.1 Characterization of events
   3.2 Causes of undetection, means of discovery, safety significance
   3.3 Corrective and preventive means
4. Conclusion
1. Introduction

In the frame of its participation to the PWG1 generic study on "Undetected Failures of Safety Systems", AVN performed a search of such cases among the Belgian plants, using the proposed criterion: to find significant events where equipment remained inoperable, or would have been unable to fulfil correctly its safety function for an extended period of time until their condition was discovered. An extended period of time means one cycle duration or several test interval periods at least; if unknown, it has to be estimated w.r.t. plant lifetime. Note that non safety systems preventing safety systems to perform their function are to be included.

As a first information source, a screening of AVN's DIANE (Domestic Information About Nuclear Events) database, for undetected failures of safety systems was performed. This database is used to store and retrieve information on a selection of events which have occurred in the Belgian NPPs since 1985. The sources of information are the incident reports which AVN receives from the utilities, completed with the reports of our inspectors on site.

The coding system used within this database is based on the IRS Coding Manual. This coding system does not always allow for an easy retrieval of events related to a specific subject. In addition the DIANE-coding system does not allow for direct retrieval of undetected failures. In a first step, the following systems were scanned: reactor coolant system, reactor heat removal system, emergency core cooling system, chemical and volume control, containment spray, main and auxiliary feedwater, component cooling water, control rod drives. For each system, records were selected by examining their title. Careful reading of the 64 reports selected this way finally led to two cases compatible with the criteria.

The decennial revision studies formed a second set of information sources. An inquiry to AVN's engineers responsible for the decennial revision projects allowed to retrieve additional cases of interest.

The six selected cases are detailed below, including the source of selection, the plant(s) concerned, the (safety) systems and equipment involved, the context, the way failures were detected, the reason of late detection, corrective actions, safety significance and the period of time involved. In some cases, additional information could be found in AVN's ARIANE (Automatic Retrieval of Information on Abnormal Nuclear Events) database of international events. The coding of this database is also based on the IRS Coding Manual.

Finally, event characteristics are summarized, and discussed along the two proposed lines

1. try to understand the causes of late detection, the difficulty of detection, and specify the means of discovery and the safety significance of failures;

2. draw corrective and preventive means that would preclude or reduce the likelihood of such events.
2. Selected cases

2.1 Non qualification of steam-line valve control organs to an environment with steam (DOEL 2, June 1980)

2.1.1 Selection source
DOEL 1-2 decennial revision studies - ARIANE record no. 0678.

2.1.2 Plant concerned
DOEL 2.

2.1.3 Affected system / equipment
Main steam / several steam-line valves, including the main steam isolation and the atmospheric relief valves.

2.1.4 Statement of the problem
A. CONTEXT

At full power, it was decided to repair a leak on the atmospheric dump control valve 2MS1004 of the SG-B 5% relief line; to this end, the isolation valve 2MS1068 was closed by closing the compressed air inlet. But no valve depressurization was performed, because it was wrongly assumed as “Fail Closed”. Progressive pressure drop led to gradual valve opening, which was effective after about one hour. Superheated vapour went out of the valve in repair. The staff had just the time to escape.

Manual power decrease was performed after turbine runback, and finally manual trip. A rapid cooldown (= 150°C/h) occurred due to the steam line break; at 282 °C, safety injection was actuated on high steam flow and low primary temperature signals. After isolation of the SG-B auxiliary feedwater line, vapour discharged until the SG-B was empty. Further cooling was ensured with SG-A (DOEL 2 is a two-loop plant) until shutdown cooling conditions were met.

B. PROBLEM IDENTIFICATION

During the incident, the cooling was made difficult because several valves (SG-A main isolation and atmospheric relief valves for example) turned out to be unavailable. The transient fortuitously brought to the fore the non-qualification of their control organs for an environment with steam.
C. WHY DID THE DEFICIENCY REMAIN UNDETECTED

Only breaks occurring inside the reactor building were accounted for in the design. In particular, for other buildings, steam conditions were not considered for the qualification of valve control organs in the design basis review.

D. OTHER ANOMALIES

The auxiliary feedwater control valves showed a residual flow rate of 40 t/h in their completely closed position, making them unable to control the flow rate; this problem was known for a long time, so that manual valves were used instead, but a high temperature made their access difficult during the accident.

Too many people were present in the control room, and some recorders and the computer were deficient.

E. CORRECTIVE ACTIONS

- Qualification of the main isolation and atmospheric relief valves to environmental conditions typical of steam line break.

- New layout of the main steam and atmospheric relief lines.

- Physical separation of measurement lines.

- Building and foundation reinforcement.

- Review of procedures for valve closing before intervention.

- NOT DONE: physical separation of auxiliary feedwater with respect to main steam and normal feedwater.

2.1.5 Safety significance

The insufficient cooling resulting from valve unavailability may be a core melt precursor.

2.1.6 Period of time involved

Since the first commercial operation of the plants (1975).

2.2 Deviation of flow rate control system of reactor building cooling ventilators (DOEL 1, January 1986)

2.2.1 Selection source

DOEL 1-2 decennial revision studies.

2.2.2 Plants concerned

DOEL 1 and DOEL 2.

2.2.3 Affected system / equipment

Containment cooling / ventilators.
2.2.4 Statement of the problem

A. CONTEXT

In the DOEL 1 and 2 plants, the containment ventilation is part of the containment cooling safety system, in the same way as the containment spray. For the related ventilators, the decennial revision requires to perform a full load test during the containment leaktightness test of “A type”, which corresponds to a pressure value (2.18 bar a) typical of design basis accidents.

B. PROBLEM IDENTIFICATION

The test showed power overconsumption for 3 (1V1B, 1V1C, 1V1D) out of the 4 ventilators, leading after half an hour to trip by thermal protection.

Further measurements performed at atmospheric pressure confirmed the mutual proportions of the ventilator power consumptions, although the values were smaller, so that no trip occurred. Moreover, flow rate measurements also showed differences between ventilators, distributed accordingly.

It was deduced that this deficiency found its origin in (maybe manual) setting modifications of the flow rate control acting on the ventilator obturators.

C. WHY DID THE DEFICIENCY REMAIN UNDETECTED

Tests are usually performed at atmospheric pressure. Ventilators then consume less power, so that trip is less probable. High pressure tests are only required every ten years.

D. CORRECTIVE ACTIONS

The flow rate was adjusted to reach the atmospheric pressure nominal power (60 kW), leading to flow rates a bit below the nominal value (80000 m3/h). Later, the ventilators were adjusted to a power below 50 kW (operating alone at atmospheric pressure), and the control mechanism was fixed to that value with a weld, in Doel 2 first, and thereafter in Doel 1. Since then, three ventilators must operate together for rightly fulfilling their cooling function.

2.2.5 Safety significance

Less containment cooling in case of a design basis accident may lead to a higher peak pressure, increasing the risk of loss of containment integrity.

2.2.6 Period of time involved

Since the first commercial operation of the plants (1975).

2.3 Primary leak caused by thermal fatigue induced by a cyclic cold water discharge through a leaking closed ECCS valve (TIHANGE 1, June 1988)

2.3.1 Selection source

DIANE record no. 189.
2.3.2 Plant concerned
TIHANGE 1.

2.3.3 Affected system / equipment
Safety injection / isolation valve and downstream line.

2.3.4 Statement of the problem

A. CONTEXT
At full power, a sudden increase of containment activity measurements occurred, simultaneously with a level decrease in the volume control tank (1300 l/h leak). The leak, not isolable, was visually localized after shutdown, on an elbow between the primary hot leg no. 1 and a safety injection check valve, itself situated downstream an isolation valve.

Liquid penetrant and ultrasonic tests showed inner cracks in the elbow, near the underside. The check valve and the piping downstream the elbow also revealed cracks on the underside.

B. PROBLEM IDENTIFICATION
The underside locations of the cracks led to the assumption of a thermal fatigue induced by a cyclic cold water discharge through the check valve, after pressurization by the volume control pumps of the line upstream the check valve through the leaking closed isolation valve (the volume control pumps also play the role of high head safety injection pumps). This was confirmed by a micrographic examination of the elbow.

C. WHY DID THE DEFICIENCY REMAIN UNDETECTED
- Risk of thermal fatigue not accounted for in the design.
- Lack of inservice inspection.

D. CORRECTIVE ACTIONS
- Replacement of the check valve, elbow and downstream piping.
- Replacement of the elbows for all the other legs, and of the check valves showing fatigue cracks (1989 outage).
- Installation of a permanent common pressure measurement downstream the possibly leaking valves, with alarm and possibility to create a depressurization controlled leak, automatically isolable in case of safety injection (1989 outage).
- Leaktightness tests will be performed on the isolation valves during each reload.

2.3.5 Safety significance
The risk of LOCA is increased, in particular in case of safety injection actuation. This safety problem seems to be generic for all plants with dual purpose charging pumps. A similar event was observed in FARLEY Unit 2 (December 1987).
2.3.6 Period of time involved
Since the first commercial operation of the plant (1975).

2.4 Improper operation of drain system causing damage on the auxiliary feedwater turbine driven pump (DOEL 2, August 1990)

2.4.1 Selection source
DIANE records no. 327 and 393.

2.4.2 Plants concerned
DOEL 1 and 2.

2.4.3 Affected system / equipment
Auxiliary feedwater / turbine driven pump drain system

2.4.4 Statement of the problem
A. CONTEXT
The drain system of the auxiliary feedwater turbine driven pump is equipped with steam traps on the turbine steam supply main line, to avoid the presence of water in the turbine, which might be a source of damage.

B. PROBLEM IDENTIFICATION
As the DOEL 2 plant was in critical hot shutdown status, requalification test of the turbine driven pump revealed heavy damage of the bearing (gear box side) and the turbine blading caused by the presence of water. As a result of a bad operation of the drain system, the condensate water had not been evacuated properly.

C. WHY DID THE DEFICIENCY REMAIN UNDETECTED
A design deficiency of the drain system introduced a probability of improper operation.

D. CORRECTIVE ACTIONS
- Pump repair.
- Provision of a temporary permanent drain before improvement of the drain system.
- Replacement of some of the steam traps.
- Shift of the steam traps from the turbine steam supply main line to the bypass line.
- Same modification of the DOEL 1 drain system.
2.4.5 Safety significance

There is a risk of improper working of the drain system, so that the turbine driven pump may be unable to work in case of need. The auxiliary feedwater system provides then less cooling capacity.

2.4.6 Period of time involved

Since the first commercial operation of the plants (1975).

2.5 Possible unavailability of diesel generators in case of blackout following a safety injection signal due to an improper temporisation (DOEL 3, September 1991)

2.5.1 Selection source.
TIHANGNE 2 - DOEL 3 decennial revision studies.

2.5.2 Plant concerned
DOEL 3.

2.5.3 Affected system / equipment

Diesel generators (DG) / temporisation of DG coupling with electrical boards.

2.5.4 Statement of the problem

A. CONTEXT

In the plant concerned, a second protection level has been designed in order to face external accidents. The involved systems are contained inside a bunkered building, the "bunker".

When a safety injection signal appears ("S" signal), DGs (first and second level) are started but remain uncoupled. The electrical boards keep their usual voltage and the utilizers are not unloaded.

In case of a subsequent loss of offsite power, a blackout signal ("B" signal) is generated and asks for unloading of these electrical boards and their utilizers, which then coast down and build up a residual voltage.

After temporisation, the DGs are coupled to the electrical boards and the needed utilizers are sequentially switched on.

B. PROBLEM IDENTIFICATION

As a result of the design review of the system, it was realized that the DG coupling temporisation corresponded to a 1" delay introduced between the order of breaker opening for the offsite power supply to electrical board, and the order of DG coupling to the electrical board. If the breaker opens slowly, DGs may couple to a hardly or even a not unloaded electrical board. The presence of still important residual voltages, out of phase with the DGs, may lead to an overpower condition, resulting in a prioritary order of DG shutdown.
C. WHY DID THE DEFECT REMAIN UNDETECTED

The DG load increase under the conditions described above, and in particular the risk of DG shutdown, had never been tested. It has to be noted however that the safety equipment involved (pumps and ventilators) require low powers, and work without flywheel, so that the coastdown period is small and that residual voltages develop over a very limited period.

D. CORRECTIVE ACTIONS

- Addition of a 1" delay for the DG coupling, starting at the moment when the opening of all board supply breakers is detected.

- Preoperational testing of the loss of offsite power following a safety injection signal scenario.

2.5.5 Safety significance

DG availability was not guaranteed after safety injection signal actuation in case of loss of offsite power, which is postulated in condition 4 accident studies. Moreover, the introduction of the additional delay improves the protection of safety equipment against overpower.

2.5.6 Period of time involved

Since the first commercial operation of the plant (1982).

2.6 Incomplete design basis accident qualification of electrical equipment (June 1992)

2.6.1 Selection sources

DOEL 3 / THINAGE 2 decennial revision studies - Event rated at level 2 on the INES Scale for the DOEL 3 plant (rating date : 92/09/29).

2.6.2 Plants concerned

Generic.

2.6.3 Affected system / equipment

Instrumentation and control / containment penetrations; connectors; terminal blocks.
2.6.4 Statement of the problem

A. CONTEXT

Some of the electrical equipment located inside containment needs qualification to demonstrate that it is compatible with the harsh environment created by design basis accidents. Standards to this effect exist since the '70's, notably the IEEE-323. Many tests have been performed during the construction phase of the DOEL and TIHANGE units. Whenever possible, existing test results were reviewed to ensure compatibility with the pressure-temperature profile calculated.

B. PROBLEM IDENTIFICATION

During an attempt to prove the overall functionality of essential equipment like motor-operated-valves and instrumentation sensors, considering the globality of the electrical connections up to the primary containment, it was found that the minimum requirements for the insulation resistance may not be met.

It was thus decided to assemble prototype circuits and to submit them to a LOCA profile (after suitable ageing and irradiation) in a large vessel (the KALI loop in CADARACHE) in June 1992. A variety of configurations were tested: terminal blocks, connectors, RAYCHEM sleeves, AUXITROL penetrations with KAPTON or PEEK.

The results confirmed the adequacy of some circuits, but also the excessive losses of insulation resistance when unsealed terminal blocks were used.

C. WHY WERE POTENTIAL DEFICIENCIES LEFT UNDETECTED

Most initial qualification test campaigns had been performed on single components; the important parameters had not always been measured, in particular, the loss of insulation resistance.

D. CORRECTIVE ACTIONS

The plants modified progressively their equipment accordingly; short term procedures alleviated in the meantime the lack of full qualification.

2.6.5 Safety significance

In case of a design basis accident, leak currents may result in drifts of measuring channels, leading to undesirable effects, like a pressurizer safety valve opening. Moreover, recirculation switching, hydrogen recombinor start-up, and availability of temperature, pressurizer pressure and level measurements, are not guaranteed.

2.6.6 Period of time involved

Since the first commercial operation of all plants.
3. Summary and discussion

There are 7 plants in Belgium, among which two twin plants. As a result, the few (6) selected events are not expected to form a significant set. However, their analysis, presented below, may be helpful in the global discussion on undetected failures of safety systems.

3.1 Characterization of events

Table 1 lists the main characteristics (plant, date of discovery, affected system, brief description of failure) of the Belgian selected cases detailed in § 2 and referenced in the discussion below.

Table 1. Brief description of selected Belgian events.

<table>
<thead>
<tr>
<th>Plant</th>
<th>Date</th>
<th>Affected system</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 DOEL 2</td>
<td>6/80</td>
<td>Main steam / steam line valves</td>
<td>Non qualification to steam of control organs</td>
</tr>
<tr>
<td>2 DOEL 1, 2</td>
<td>1/86</td>
<td>Containment cooling / ventilators</td>
<td>Deviation of flow rate control system</td>
</tr>
<tr>
<td>3 TIHANGE 1</td>
<td>6/88</td>
<td>Safety injection / isolation valve and downstream line</td>
<td>Thermal fatigue induced by cyclic cold water discharges</td>
</tr>
<tr>
<td>4 DOEL 1, 2</td>
<td>8/90</td>
<td>Auxiliary feedwater / turbine driven pump drain system</td>
<td>Design deficiency of the drain system</td>
</tr>
<tr>
<td>5 DOEL 3</td>
<td>9/91</td>
<td>Diesel generators / temporization of coupling with electrical boards</td>
<td>Delay starts at breaker opening order, not detection</td>
</tr>
<tr>
<td>6 Generic</td>
<td>6/92</td>
<td>I&amp;C / containment penetrations; connectors; terminal blocks</td>
<td>Incomplete design basis qualification</td>
</tr>
</tbody>
</table>

3.2 Causes of undetection, means of discovery, safety significance

Table 2 summarizes for the Belgian selected events the causes of late detection, usually explaining the difficulty of detection, the way failures were discovered, and their safety significance.

For several cases, discovery is related to decennial revision studies. Decennial revisions (DR) are periodical safety reassessments, occurring every ten years of plant operation and which may lead to plant modifications connected to safety enhancements.
Table 2. Causes of undetection, means of discovery and safety significance for the selected Belgian events.

<table>
<thead>
<tr>
<th>Why undetected</th>
<th>How discovered</th>
<th>Safety significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Not in design; undetectable out of incident</td>
<td>fortuitous (incident)</td>
<td>Insufficient cooling, possible core melt precursor</td>
</tr>
<tr>
<td>2 Containment high pressure test: rare</td>
<td>DR containment high pressure test</td>
<td>Risk of loss of containment integrity in case of design basis accident</td>
</tr>
<tr>
<td>3 Not in design; lack of inservice inspection</td>
<td>fortuitous (incident)</td>
<td>Risk of LOCA increased</td>
</tr>
<tr>
<td>4 Drain design deficiency; slow evolution of effects</td>
<td>Requalification test of turbine driven pump</td>
<td>Risk of less cooling capacity</td>
</tr>
<tr>
<td>5 Inadequate implementation; no test</td>
<td>Questioning attitude during DR</td>
<td>Risk of diesel generator unavailability</td>
</tr>
<tr>
<td>6 Deficiency in environmental qualification; undetectable out of accident</td>
<td>Questioning attitude during DR</td>
<td>Risk of drift of measurement channels</td>
</tr>
</tbody>
</table>

3.3 Corrective and preventive means

Table 3 presents the corrective actions introduced to cope with the failures after their detection for the Belgian cases. It also shows the possible impact of DR studies on failure discovery, and gives information on the subsequent implementation of methodologies or guidances (M/G) when applicable.

It should be noted that

1. among other possible regulatory requirements, the DR studies have proven to be effective for several presented cases (4/6); event 1 was not effectively detected in the frame of a DR, but DR studies led to a refined, more in depth solution;

2. apparently, studies in the category “Findings and insights...” did not play a role;

3. in some cases (3/6), appropriate methodologies were introduced; for event 6, implemented procedures were only transitional, in order to cope with a temporary lack of full qualification.

In all cases, the failures collected for Belgium appear to be related to design and component qualification, and / or to phenomena not well known at the design stage, but not on testing and maintenance practices.
Table 3. Corrective actions, impact of decennial revision (DR) studies and implementation of methodologies or guidances (M/G) for the selected Belgian events.

<table>
<thead>
<tr>
<th>Corrective actions</th>
<th>DR</th>
<th>M/G</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Hardware modifications</td>
<td>(Y)</td>
<td>N</td>
</tr>
<tr>
<td>2 Hardware modifications</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>3 Hardware modifications; leaktightness tests at each reload</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>4 Hardware modifications</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>5 Setting modification; preoperational test</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>6 Hardware modifications; transitional procedures</td>
<td>Y</td>
<td>(Y)</td>
</tr>
</tbody>
</table>

4. Conclusion
The few selected cases of undetected failures of safety systems in Belgium mainly bring to the fore the importance of decennial revisions. They allowed to discover failures

- through more severe testing procedures;
- through a questioning attitude in the studies.

In addition, they provide the opportunity to find more refined solutions to problems which may have been detected in another context.

However, the observed weight of the role of decennial revisions in failure discovery (3/6) may be misleading. Indeed, the set of events is too small to be significant. In addition, decennial revision studies were one of the two sets of information sources used.

All failures found cover the whole period between the first commercial operation and the failure discovery.

They involve design and component qualification only, not testing and maintenance practice.
CONTRIBUTION FROM FINLAND
LATENT FAILURES OF SAFETY SIGNIFICANT SYSTEMS AT FINNISH NPP'S

Lasse Reiman, STUK

1. Introduction

In considering the human contribution to accidents, Reason /1/ distinguishes two kinds of errors: (1) active errors, whose effects are felt almost immediately, and (2) latent errors, whose adverse consequences may lie dormant within the system for a long time. Active errors are associated with the performance of the "front-line" operators of a complex system. Latent errors are most likely made by designers, decision makers or maintenance personnel.

Reason /2/ has analyzed the nature and variety of latent errors through case study analyses of six major accidents, two of which took place at a nuclear power plant (Three Mile Island and Chernobyl). An important lesson learned from this analysis is that the term error does not capture all the ways in which human beings contribute to major accidents. Reason concludes that an adequate framework requires a distinction to be made between errors and violations. Violations can be defined as deliberate deviations from those practices deemed necessary to maintain the safe operation of a system. He defines further routine violations which are largely habitual, forming an established part of an individual's behavioural repertoire.
Accidents happen when latent failures combine with local triggering events to breach or incapacitate the system defences. Of the two primary accident-causing ingredients usually only the former, latent failures, can be detected before an accident sequence is initiated. They exist during normal plant operations and are amenable to various auditing procedures. Local triggers are often extremely difficult to foresee.

Reason's accident causation model is closely related with Turner's model of disaster development /3/. The study of disasters merges with the study of accidents, although for an accident to be labelled a disaster, it will probably need to be an unusually large-scale, costly or otherwise unexpected accident. Turner concluded that disasters rarely come about for any single reason, and that the conditions for failure do not develop instantaneously. Instead, there is an accumulation over a period of time of a number of events. The incubation period, in which the gradual degradation takes place, is brought to a conclusion either by performing preventive actions to remove dangerous preconditions or by a trigger event, which brings the latent factors to light in unpredictable ways.

Mosey and Weaver /4/ call latent failures related to organizational accidents institutional failures and define them as the absence or impairment of a corporate function which is necessary for the safety of an installation. Mosey /5/ has reviewed a number of selected high-consequence events, both nuclear and non-nuclear, and this review identified some of the principal characteristics of organizational failures. They include a dominating "production imperative", inappropriate allocation of safety-related resources, failure to recognize or acknowledge a deteriorating safety situation, lack of clearly defined and assigned safety responsibilities and lack of understanding at the management level of the technical safety envelope of the technology involved.

2. Latent failures of safety significant systems

Undetected or latent failures include events where components remained inoperable, or would have been unable to fulfil correctly their safety function for an extended period of time until their condition was discovered. An extended period of time means a period equivalent or greater to one production cycle duration or to several test periods.
A study was performed in STUK the purpose of which was to understand, why deficiencies remain undetected during a long period, and to collect measures that would preclude or reduce the likelihood of such events.

The selection of incidents at Finnish nuclear power plants for this study was made based on the quarterly operating experience reports published by STUK and the incident data base of STUK. When the selected incidents were analyzed in details, also the incident reports of the utilities were studied. The quarterly reports and the incident data base were reviewed from the beginning of 1985 until the end of 1995. Nine incidents with latent failures of safety significant systems were selected for this study. In addition to latent failures, which were not discovered during an extended period of time, also latent failures which were not discovered during regular tests and could have stayed undiscovered for a long time but were discovered by chance (for example during a transient) were included in the analysis. Descriptions of the incidents are presented in the next chapter.

3 Latent failures at Finnish NPP's

3.1 Loviisa 1, Inadvertently closed manually operated valves in the boron supply system, July 1986

For increasing the boron concentration in the primary circuit the boron supply system is equipped with two high-capacity centrifugal pumps and four smaller piston pumps. Only two of the piston pumps can be controlled from the emergency control room. These pumps are also needed in the event of a containment isolation for feeding sealing water to the main circulation pumps.

A decision was made to increase boron concentration in the primary circuit of Loviisa 1 unit by means of the two piston pumps on July 25, after the trip of the other turbine had caused a displacement of the control rods from the normal position range. Both pumps stopped, however, immediately after the start. This was caused by high pressure in the pumping line due to closed manually operated shut-off valves. The pumps had been tested on July 18, at which time the shut-off valves remained, contrary to the procedures, in
closed position in spite of having been acknowledged as open. The pumps were operated also on July 24 in connection with the testing of the emergency control room signals. During the tests an alarm indicating high pressure was neglected, because the alarm activates also during normal tests. The pumps did not stop because the pressure switch is automatically by-passed during the testing.

The incident was caused by a human error in restoring the manual valves to open position after the testing on July 18. After the incident testing procedures were modified.

3.2. Loviisa 1, Erroneous removal of protections for two primary circuit make-up water pumps, March 1987

In order to compensate for minor primary circuit leakages and discharges, water is pumped back to the primary circuit by the normal make-up water system. The system comprises two high-capacity centrifugal make-up pumps and three smaller piston pumps, which can feed into either of the two make-up water collectors.

It was noted on March 31, during a random check-up of instrument connections, that the high capacity make-up water pumps had almost all their protection signals switched off at Loviisa 1 plant unit. One of the protection signals is used to stop the make-up pumps due to high pressure in the primary circuit in cold shutdown conditions, since the pressurization of the primary circuit by the pumps might jeopardize reactor pressure vessel tightness. The switched-off protections also serve to protect the pumps against damages resulting from minor operational transients.

It became obvious during the investigations, that the protection signals had been erroneously switched off already during the plant start-up on September 10, 1986. As a result of a transient, which occurred during the plant start-up, a decision had been made to switch off the protection signal related to high pressure in the make-up water deaerator, from where the pumps take their suction. Instead of this signal conductor, as a result of an erroneous interpretation of the schematic diagram, the conductor which couples all the
protections of the pumps had been removed. This kind of an error does not usually disclose itself during the periodic tests performed on pumps.

3.3 TVO I, Inoperability of the reactor pressure control valves, October 1987

The reactor overpressure protection and pressure control system (314) of TVO I and II units comprises ten relief valves and two quick-opening and control valves.

A turbine trip occurred at TVO I on October 6, as a result of which, owing to a partial inoperability of the turbine bypass valves, reactor scram followed as well as the opening of the 314 system valves and the transfer of reactor pressure control to the control valves of the 314 system. The motor protection switches of the control valves tripped during pressure adjustment. The valves switched on to manual control and remained in an about 15% open position. This position did not suffice to maintain the reactor pressure constant but it rose slowly. By restoring several times the motor protection switches after a trip, the valves could gradually be driven into the open position.

The cause for the inoperability of the control valves was a modification made during the annual maintenance outage in 1987, during which the motor protection switches of the control valves had been set to trip at a too low electrical current value. The original setting of the manufacturer was not modified because the work plan was not checked by the experts of the TVO electrical office as it should have been done. The error was not discovered, because the valves were not tested in transient flow conditions after the modification.

3.4 Loviisa 2, Faulty states of the primary shut-off valves of the impulse lines of certain pressure measurements of the plant protection system, June 1988

At Loviisa 2 it was noted on June 14 that certain (15 pcs) so called primary shut-off valves of the impulse lines of some pressure measurements were in closed position. These pressure measurements are related to the plant protection system (YZ) signals, the function of which
is to identify a leaking steam generator on the basis of a pressure difference and to close the auxiliary feedwater lines which are connected to it.

The situation was discovered in connection with the settlement of the reason for the comparison signal of pressure measurements. The valves were closed in refuelling shutdown 1986 due to a modification of the impulse lines. The correct positions of the valves were not checked after the work as they should have been done. All the pressure measurements, with the exception of the aforementioned comparison alarm, had continuously been giving normal indications which was due to the untightness of the shut-off valves.

3.5 Loviisa 1, Feedwater pipe rupture, May 1990

At the Loviisa 1 plant unit a main feedwater line pipe rupture occurred on May 28, 1990. At the Loviisa plant there are four main feedwater pumps running and one on stand-by during operation at full power.

One of the operating feedwater pumps tripped and the stand-by feedwater pump started immediately. The starting of the stand-by pump brought about a pressure shock in the feedwater lines. This resulted in a pipe rupture of one feedwater line during which about 70 m³ of water from the secondary circuit was discharged into the turbine hall. Pressure decrease in the feedwater collector tripped all operating feedwater pumps. Reactor operator in the control room brought about a reactor scram manually as presupposed in the procedures concerning loss of feedwater. A scram would have occurred automatically after some time upon the decreasing of steam generator water levels below the safety limit. Auxiliary feedwater pumps started operation when steam generator water level decreased. Furthermore, a supplemental auxiliary feedwater system independent of other systems was available. In addition to these systems, water could be supplied to the steam generators by the primary circuit make-up water pumps. The auxiliary feedwater pumps operated according to plans and it was not necessary to undertake the two last mentioned options during this event. Nobody was injured in connection with the event and no radioactive discharges occurred.
The feedwater pipe rupture was downstream of a feedwater pump in the flange of an orifice plate used for flow measurement close to a welded seam. The rupture was attributed to heavy erosion corrosion which had reduced pipe wall thickness to 1–2 mm circumferentially in the rupture point. The outside diameter of feedwater line piping is 325 mm and nominal wall thickness 18 mm.

Erosion corrosion of pipings, as well as other phenomena due to wear, are monitored by means of inservice inspection programmes. Programmes have been drawn up based on experience. They were not so comprehensive, however, that the thinning of the flanges of the orifice plates used for flow measurement could have been detected in the inspections. The error was of a type organizational failure (failure to recognize a deteriorating safety situation).

A corresponding feedwater pipe rupture had occurred in the USA in 1986. Due to the rupture also the scope of the inspection programme for pipings at the Loviisa plant units had been extended significantly e.g. concerning pipe bends and flow reduction points. Additional inspections of the flanges of orifice plates were not introduced, however. After the event inservice inspection programmes were complemented. The flanges of orifice plates and certain other items were added to the programme.

A second feedwater pipe rupture occurred at the Loviisa 2 plant unit on February 25, 1993. After the feedwater line break at the Loviisa 1 unit in 1990, several corrective actions were taken. In spite of these actions, a break occurred again. In connection with the 1991 and 1992 refuelling outages, the pipelines in question were inspected in accordance with an extended programme.

The broken pipe section's proneness to erosion was known. Also, based on an analysis made using the WATHEC computer-aided condition evaluation system, an inspection was recommended to be conducted during the 1992 refuelling outage. During a review of these recommendations, the inspection was given up, however, since piping wall thickness after the check valve had been measured and ascertained as sufficient in the 1991 refuelling outage. In actual fact, the end of the inspected area was at about 20 mm's distance from the
broken point. The broken connecting flange, located after the check valve flange, was lacking entirely from the inspection protocol diagram and was thus not measured in 1991. The incorrect inspection protocol diagram contributed for its part to the drawing of an erroneous conclusion.

3.6 Loviisa 1, Unsatisfactory functioning of the check valve of the discharge line of an emergency core cooling system, August 1991

During the Loviisa 1 annual maintenance a discharge test of a pressurized water tank of the emergency core cooling system was performed on August 21. It was discovered that the check valve located between the tank and the reactor pressure vessel did not open sufficiently at the tank's hydrostatic pressure. During an actual loss-of-coolant event, the force opening the valve would have been essentially greater but it remains uncertain, whether the valve would then have opened sufficiently.

In the passive part of the emergency core cooling system there are four pressurized emergency water tanks from which borated water is injected to the reactor pressure vessel. In the tanks 54 bar pressure is maintained by means of nitrogen. Water is injected from two tanks to the lower part of the reactor pressure vessel and from two tanks to the space above the core. A discharge test of the emergency water tanks was performed on each tank on alternate years at four years' intervals. The test is performed at hydrostatic pressure with the reactor pressure vessel open.

After the test the check valve was dismantled. It was found out that the gaps of the axle sleeve of the valve disc are too narrow axially and prevent the disc's movement. The sleeves were removed and machined so that a generous gap (2 mm) was introduced between them and the disc. In a repeated post-repair discharge test the valve functioned faultlessly. Corresponding discharge tests were conducted also on three other tanks at Loviisa 1 and all emergency water tanks at Loviisa 2. The valves of these tanks functioned correctly.

In the 1988 annual maintenance, modifications had been made in the housings of the axle seals of the valve in question to enhance structural reliability. Components had been
dimensioned according to the design drawings since all valves were assumed to have identical dimensions. It was probably individual differences between valves that caused the gaps of the axle sleeve of the valve in question to become too narrow. The first post-modification tank discharge test was performed as late as in the 1991 annual maintenance outage.

The incident was caused by insufficient testing after modification work. Based on the event, all tanks will be tested once in every two years instead of the previous interval of four years. Furthermore, a tank discharge test is always performed after extensive repairs and modifications of the components of this system.

3.7 Loviisa 1, Inoperability of the fire extinguishing system of the containment inner intermediate ring, October 1992

A periodic inspection of the fire extinguishing system of the Loviisa 1 reactor containment inner intermediate ring was performed on 27 October 1992. Water flow from the system and fire hydrants was observed to be nonexistent. This was caused by two valves of the system's collection pipelines having been left closed during annual maintenance outage work. The system was inoperable for one month from the end of the annual maintenance outage.

The system in question serves to extinguish potential cable fires in the space between the steel containment and crane wall, i.e. the so called inner intermediate ring. All cables to the containment building come through this intermediate ring. The spreading of fire in this space has been restricted by means of 7 m high walls dividing the space into four compartments.

In order to modify a test assembly in the annual maintenance outage of 12 August 1992, the fire extinguishing system of the reactor containment building was separated by closing the system's collection pipeline valves. The closing of the valves was marked in the auxiliary control room log, but not in the work order. When the work was finished, the valves remained closed, as there was no mention of them in the work order. In addition, the closed state of the valves went unnoticed in the fire prevention inspection conducted at the end of
the annual maintenance outage, as the valves in question were not mentioned in the check lists.

The incident was caused by inadequate work order and inadequate fire prevention inspection procedures.

3.8 TVO I/II, Shut-down service water system reliability was impaired, July 1994

At both Olkiluoto plant units, an error was made when installing shut-down service water system strainer pressure difference switches. Consequently, automatic back-flushing of the strainers would not have started immediately on potential blockage.

The shut-down service water system has four parallel lines supplying service water to the shut-down secondary cooling system heat exchangers and to the heat exchangers, which cool emergency diesels. Potential service water cooling circulation blockage would have direct safety significance to i.a. back-up diesels, which require cooling to function.

The shut-down service water systems had been improved at both plant units in 1992 – 1993 by installing strainers to prevent clogging of cooling water circulation. The clogging may occur if mussels or other impurities end up in heat exchangers. The strainers were equipped with a back-flushing function which activates, when pressure difference resulting from clogging exceeds the set point. Also, when the service water system is operating, back-flushing activates automatically every 40 minutes. Back-flushing can be manually activated on the spot. The correct functioning of the strainers is, according to the latest PSA studies, of high safety significance. Erroneous installations were detected on 14 July, 1994.

The strainer back-flushing function, which activates automatically on pressure difference, was inoperational in all four cooling water lines at TVO I and in two lines at TVO II. Due to a human error, the pressure difference measurement was installed in the reversed direction. The wrong direction was not discovered in the commissioning and functional tests performed after the modification, because they were only simulated tests.
3.9 TVO, Insufficient supply of suction air to diesel generators during load tests, February 1995

During back-up diesel load tests conducted at TVO plant units, the filters of the air intake ducts of the diesels emergency began to clog due to a strong wind and a snow storm.

Both TVO plant units have four emergency diesels subjected to load tests every four weeks. Suction air for the diesels is drawn from the outside of the building. Besides the air-intake grid in the outer wall, there is a filtering unit in the air-intake duct of the diesel turbochargers. During a diesel's operation, the condition of the filter is monitored by measuring the pressure difference between the air-intake duct and the diesel room. If the pressure difference deviates from its normal range of fluctuation, it appears an alarm in the control room based on which necessary measures can be taken.

Diesel load tests were carried out on 1 February, 1995. There was a heavy snow storm in the Olkiluoto site at that time and a strong, turbulent wind was blowing, lifting snow in the air. During the test at TVO I, so much snow ended up in the filters of the air intake duct of the diesels that an alarm on pressure difference actuated in the control room. A decision was made to stop the test although there was nothing out of the ordinary in the operation of the diesels. The filter was partly blocked by a compact layer of snow which had accumulated in its lower part. The filter was replaced and the load test was completed. A diesel load test was also carried out at TVO II during which an alarm on a blocked filter actuated in the control room. This blocking was not serious and there was nothing unusual in the diesel's operation, so the test was completed.

This being a test, the plant unit's safety was not affected. The event identified deficiencies in the supply of suction air to the emergency diesels.

As an immediate measure to prevent recurrence and to ensure the supply of the suction air, the operating personnel was advised about the quick removal of the filter unit once it begins to show signs of blocking. Afterwards, a modification has been made at the plant, which
makes it possible to take the suction air also from the inside of the diesel generator room. A similar modification has been made at the Loviisa plant, too.

4. Findings

An important issue in analysing human errors is the dependence of actions i.e. how the success or failure on one task may be related to the success or failure on some other tasks. The dependence of errors between tasks performed in redundant subsystems of a safety system is the most important issue, when the safety significance of test and maintenance errors at NPP's is considered. The impact of the dependence is that it reduces the gain in system reliability achieved by the use of redundant subsystems.

It can be seen that in six of the nine cases a dependent human error had occurred. The dependent errors were classified using the scheme of Lucas /6/ in a slightly modified way /7/. The results of the classification of dependent failures are presented in Table 1. In two cases two different dependent errors occurred.

<table>
<thead>
<tr>
<th>Class</th>
<th>Cases (chapter of the paper)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skill-based errors</td>
<td></td>
</tr>
<tr>
<td>- mistake among alternatives</td>
<td>3.8</td>
</tr>
<tr>
<td>- omission</td>
<td>3.1, 3.4</td>
</tr>
<tr>
<td>- carelessness</td>
<td>3.2</td>
</tr>
<tr>
<td>Rule-based errors</td>
<td>3.3</td>
</tr>
<tr>
<td>Knowledge-based errors</td>
<td>3.3, 3.9</td>
</tr>
<tr>
<td>Violation</td>
<td>3.4</td>
</tr>
</tbody>
</table>

It was analyzed, which was the method of discovery of the latent failures described in ch. 3. The results are presented in Table 2.
<table>
<thead>
<tr>
<th>Case</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Real need of the system (operative action)</td>
</tr>
<tr>
<td>3.2</td>
<td>Random inspection</td>
</tr>
<tr>
<td>3.3</td>
<td>Real need of the system (plant transient)</td>
</tr>
<tr>
<td>3.4</td>
<td>Alarm (comparison signal of the measurements)</td>
</tr>
<tr>
<td>3.5</td>
<td>Transient (pipe break)</td>
</tr>
<tr>
<td>3.6</td>
<td>Periodic test</td>
</tr>
<tr>
<td>3.7</td>
<td>Periodic inspection</td>
</tr>
<tr>
<td>3.8</td>
<td>Maintenance work</td>
</tr>
<tr>
<td>3.9</td>
<td>Periodic test (in extreme weather conditions)</td>
</tr>
</tbody>
</table>

It is important to notice that none of the dependent human errors was detected in normal periodic tests, but were discovered in a real need or in a random way. Only in two cases the latent failure was discovered by periodic testing, in one of these cases during abnormal weather conditions.

The effectiveness of other defensive barriers was also analyzed. It was noted that in two cases (3.1, 3.2) there were no defensive barriers at all. In two cases (3.3, 3.4) an independent check, either after the work planning or the actual work, should have been performed but was not made. In all the other cases some kind of independent review was done, but this could not prevent the latent failure.

5. Conclusions

Based on an analysis of the nine incidents some conclusions can be presented. Six cases of the nine incidents were related to modifications performed at the plant, which shows the importance of clearly defined and strictly followed modification processes. A study has been started by STUK to define the requirements for different phases of the modification process and to evaluate the modification procedures in use at NPP's.
More attention should be paid at the plants to the determination of the functional tests after modification works so that the tests would cover adequately the possibilities for latent failures. Especially the testing of valves in real flow conditions is important.

The need for independent inspections should be reviewed every time with care, especially if there are doubts concerning the effectiveness of the tests, which are always the primary defensive mechanism against latent failures.

Increased attention should be paid to the motivation of maintenance staff so that the likelihood of dependent errors would be minimized. Attention should be given to work orders and work procedures in general to avoid omissions in routine tasks. A more detailed study financed by STUK is in progress concerning dependent errors in maintenance tasks at TVO and Loviisa nuclear power plants.

References


CONTRIBUTION FROM SPAIN
ANALYSIS OF OPERATING EXPERIENCE AND SYSTEMS AT TRILLO NPP:
A PROGRAM INTENDED TO ELIMINATE ALL UNDETECTED FAILURES OF SAFETY SYSTEMS

July 1996

Report of Spain for The
Generic Study on Undetected Failures of Safety Systems
Organized by The PWG 1 of The CSNI/NEA

Javier Zarzuela
Head, Area of Operational Experience and Training
CONSEJO DE SEGURIDAD NUCLEAR

Justo Dorado 11
Tel: 34-1-346 01 02
Fax: 34-1-346 05 88
jzj@csn.es

SPAIN
E-Mail:

ANALYSIS OF OPERATING EXPERIENCE AND SYSTEMS AT TRILLO NPP:
A PROGRAM INTENDED TO ELIMINATE ALL
UNDETECTED FAILURES OF SAFETY SYSTEMS

SPAIN

1. BACKGROUND

Several events consisting of safety system deficiencies occurred at Trillo\(^1\) NPP from 1992 to 1994 related to discovery of design and/or construction deficiencies. These deficiencies remained hidden after the commissioning process, and their discovery took place as result of activities not intended to discover them.

The most safety significant were: a) Crossed redundancies at the Protection System, b) Operability degradation in safety systems due to internal leaks in valves, and c) Excessive voltage drop in Emergency 24 V DC System.

Each deficiency, after discovery, was submitted to detailed analysis, and a plan for individual resolution, including short term actions and definitive solution. Besides, the root cause analysis performed in these cases, and in other ones of less significance which also happened by these years, identified weak points related with important features of design, construction and commissioning process, such as:

- Safety basic requirements implementation in the detail design.
- Commissioning test execution, scope and acceptance criteria.
- Identification of applicable codes and standards, and implementation of them in the design process.
- Interface between basic design (NSSS supplier) and detail design (architect engineer).

Subsequently, the licensee perceived the need to carry out a systematic, overall program to identify other possible hidden deficiencies of similar origin and to ensure the capability of safety systems to adequately fulfill their safety functions. The aim of the program was extended to a wide review of plant design, construction and commissioning.

The program was named "Operating Experience and Systems Analysis" (AOES) and it was unveiled before the Regulatory Authority in late 1994.

\(^1\) Trillo is a 3 loop PWR designed by KWU, 974 Mwe, in commercial operation since 1988.
2. **SHORT DESCRIPTIONS**

The most safety significant events that led Trillo NPP to undertake the AOES program are described in this part, all of them were reported to the Incident Reporting System (IRS) as report No. 1307, 1354 and 1506. Additionally, these events represent the biggest contribution to shape the scope and content of the program.

2.1. **1307 Crossed redundancies at the Protection System**

On January 31, 1992, the licensee, by investigating a minor event, discovered that some actuations of the Emergency Core Cooling System (ECCS) were crossed at the Protection System between trains, i.e. the high level in sector 3 of the annulus produced "permissives" and "interlocks" to actuations of train 1 of TH, instead of train 3 as designed. This happened in three out of four trains and the safety feature affected was the inhibition, in certain conditions, of ECCS automatic switching from injection to recirculation phase during a postulated LOCA.

Safety significance is that in certain scenario, included in the design bases of the plant Safety Analysis, the unique train of ECCS suctioning from the containment sumps would be that of the broken line, so that discharging coolant out from the containment to the annulus, where it is not possible to recover it. In such a case the plant safety would have relayed on the skills of the operators to understand the contradictory and confusing information offered by several monitoring systems, as well as their ability to investigate the real situation timely and take measures not described by any emergency procedure.

The origin of this crossing was caused by a design error made by the NSSS supplier, not discovered by neither start up nor surveillance tests after four years of performance.

Corrective measures consisted of:

- Reviewing all Protection System design and installation in search of other similar mistakes. None else was discovered, instead some other minor errors were found, with no significant impact and due to installation mistakes.

- Improving of assembling control procedures, to prevent new assembling errors unnoticed in design modifications, maintenance works, etc.

- Demanding the NSSS vendor to review and stress internal controls and supervision.
Licensee was currently reviewing its Technical Specifications (TS) for other reasons. It took notice of the causes of this event to improve the surveillance program, in order to lower the probability of not detected inoperabilities of safety systems.

2.2. 1354 Operability degradation in safety systems due to internal leaks in valves.

In 1993, leaks were detected through two check valves belonging to two different trains of the Essential Service Water System (ESW), a system constituted by 4 trains with the design criteria of N + 2, i.e., just two trains can face any anticipated accident. All four trains have some interconnections, but they isolate each other upon certain protection system signals.

Technical Specification require a minimum flow of 720 Kg/s per train, the leaks were estimated in 125 kg/s in a line and 34 kg/s in another one, being the regular flow 800 Kg/s at each of three trains and 730 Kg/s at the fourth train.

After discounting the leak amounts, the system did not had enough flow for safety functions; moreover in the event of certain scenarios related with LOCA, plus a single failure of a train interconnection isolation valve, two ESW trains would remain connected all over the accident, what constitutes a design principle break. Presumably, the system had been operating that way for years.

The cause of the leaks was disk misalignments respect to the seats, leaving gaps of 25 and 10 mm respectively.

Short term corrective measures were to fix the valves, to rebalance system flows to different components as required and to start considering a redesign of the complete system, as well as set up a comprehensive surveillance program for the system.

2.3. 1506 Excessive voltage drop in Emergency 24 V DC System

A service test of the Emergency 24 V DC System carried out in October 1994 found that in certain conditions postulated in the design basis of the plant, the Reactor Protection cabinets received 19.2 V, i.e., 2.3 less than the design requirement of 21.5 V.

In those conditions, such as one out of four Emergency 24 DC System buses in maintenance and single failure in another, it is not guarantied that in case of loss of off-site power the emergency batteries had been able to start up the emergency diesel generators. Therefore, the core cooling safety function had not been guarantied.

5
The excessive voltage drop in Emergency 24 V DC System was caused by design error and lied in elements such as cables, fuses, breakers, etc. whose voltage drop at higher voltage systems is usually negligible, and so it was in this case by the designer. In addition, the batteries of the system had been down-sized to fit them in the allotted room.

The root causes are a) the applicable standards/specifications were not used to the extent necessary, and b) the design control did have neither the scope nor the strength required. Scope of surveillance tests is also under scrutiny.

System oriented corrective measures have been: increase section of many cables; performance of a "real black out" test; introduction of operating restrictions; restrict inoperability of AC and DC emergency trains more than allowed by TS, and a complete design modification of the system is under way.

3. DETECTION OF THESE EVENTS

Event of IRS No. 1307 was discovered by analyzing a minor in-house experience, not even reaching the threshold of Licensee Event Report reporting criteria: small leakage of borated water to the annulus during refuelling outage. When checking out the computer alarms, it was noticed that the annulus high level alarm corresponded to a sector different to that of the leakage.

The event was not detected over the start up tests because at that phase the goal of the tests is to check out that systems have been assembled according to design, so that, being a design deficiency it was not detected.

Besides, it remained undetected for 4 years of operation because the approach of functional tests, both during start up phase and during operation, in german regulations is "step by step", i.e., at first step it is tested the analogic section from the sensor to the logic cabinets verifying coherence among electrical trains, disregarding verification of sensors location. This is so because tests are carried out at one electrical redundancy at a time. Other parts of the Protection System are tested at separate steps to check out as well coherence among electrical trains.

Upon analyzing this event, it was realized that only an integrated test, real increase of water level at the sector of the annulus or just at the sensor well, would have detected the error. However, the design of this type of tests to other systems would have departed from the KWU surveillance philosophy and procedures and the licensee did not undertake such a task; in the other hand, at the time it was not fully justified, as no significant similar events were known. Instead, it was just taken into account for the revision of the TS then under way.

Event of IRS 1354 was detected by an indirect way. In July 1992 the licensee noticed some leaks in the ESW system, whose amount was estimated and it was
scheduled for the coming refuelling outage, in autumn that year, to repair them. Following repair works, system rebalances were carried out with and a campaign of flow measures initiated and after that it was found out that ESW train flows were much smaller than expected and concluded that the system had been bellow Technical Specifications requirements all over the period when the leaks were present.

Flow decreases had not been detected because of lack of system flow meters. The cause originating the deficiency was insufficient scope of the commissioning tests and the root cause plant surveillance program insufficient scope and mismanagement.

As for event of IRS No. 1506, in the course of a functional inspection, an inspection team of the regulatory body (CSN) witnessed a periodic test of Emergency DC batteries at Trillo and analyzed the system design report, concluding that voltage drop across the system could be excessive. Therefore, upon CSN requirement a new service test of the battery was carried out in October 1994 and the problem was discovered.

The event was caused by design errors motivated by insufficient use of applicable regulations and inadequate design control, remaining undetected because:

i) There was no measure of actual voltage drops.

No regulation requires these measures, therefore it is not expectable from the Engineering Company to have made them.

ii) No real functional tests were carried out, i.e., disconnection of Emergency 24 V DC System train from the AC power and check out whether or not the battery is able to take the loads and start up DGs. Such tests, although not aimed to measure voltage drops, provide confidence in system operability.

What all three events reveal, as well as others taken place at Trillo NPP, is a pattern of design deficiencies degrading safety functions, that remain unnoticed because the surveillance program is short of scope and frequently focused on component ("step by step") rather than complete system ("real test") operability.

4. **AOES PROGRAM**

The response of the plant to the above mentioned events, and some others, was the AOES program. The program was defined to apply to all plant safety systems or systems included in plant Technical Specifications. The goal of the program was to ensure, by systematic design, construction, and commissioning review, the adequacy of safety systems, structures and components to fulfil their safety functions.
As a result of the program, it was decided to perform a reconstitution of the plant design basis, consisting of a complete, unambiguous, systematic, design basis definition and a complete documental review of the plant design.

The program had a very important specific feature: it would be carried out in an operating plant, so there were important related considerations:

- The program findings should be adequately and timely assessed with respect to their impact on operability status of safety systems, and subsequent Technical Specifications requirements application.

- Corrective action, both in the short term and in the long term, should be implemented to resolve issues resulting from the program. The corrective action implementation plans should be commensurate with the safety significance of the issues.

4.1. Scope and content

In the program scope definition there were used as references diverse existing review procedures defined for similar purposes, such as NSAC 121, NUREG 1397 and NUMARC 90-12, specially for the design basis review area.

The program was structured in seven main areas of review: Design Basis, Commissioning Tests, Reactor Protection System, Operating Experience, Plant Specific Design Features, Adequacy and Completion of Construction "Open Items", Design Changes.

- Design Basis.

The aims of this review area are: a) to compile and clearly define the design basis requirements of all safety systems, and b) to assess the efficient implementation of these design basis requirements in the design of the different systems. Additionally, a wide documental review of the design should result from this area. The design basis requirements compilation should start from a review of functions to be performed by each safety system in the different postulated scenarios.

- Commissioning Test Review.

In this review area the purpose is: a) to define in complete detail the requirements (scope and subject of different tests, acceptance criteria) of a commissioning test program, b) to compare this commissioning program with the commissioning test actually performed, identifying differences, evaluating them and, if applicable, to define additional test to carry out. Finally, a complete
verification of the commissioning test results (versus procedures requirements) is to be performed within this review area.

Reactor Protection System.

This area includes: a) complete, in-depth review of Reactor Protection System (RPS) design and b) implementation, including instruments, electronic cards and cabinets. Part b) had been partially performed before the issuance of the program, as one of the corrective actions resulting from the event of RPS crossed redundancies referred to before.

Operating Experience

This area consists of a review of all reported events looking for possible repetitive design/construction related root causes, as well as all external applicable experiences; from this analysis would result the definition of new specific review areas.

Plant Specific Design Features

It is mainly focused on the adaptation from a standard four loop to a three loop plant. Trillo is an adaptation of a standard 4 loop plant to a 3 loop plant. The 4 loop plant has 4 trains of ECCS, Nuclear Components Cooling System (NCCS), Essential Service Water System (ESW), etc., physically, hydraulically and electrically separated. Trillo has 3 independent trains of ECCS, NCCS, plus a fourth train of ESW, emergency AC -with 4 Diesel Generators (DG)- and DC power, and other systems, that can be connected to any of all other three, in such a way that is able to substitute any of the other 3 trains, under some rules. Besides, each train of NCCS contains valves, interlocks, etc. fed from different electrical buses of AC and DC power. The multiple combinations of inoperabilities and/or single failures of any electrical bus produce multiple scenarios not always covered by the plant design. Therefore, severe operating restrictions have been required much stiffer than those allowed by Technical Specifications.

Additionally, there have been included some other specific areas of review suggested by licensee technical staff personnel, according to their experience; in this way, several specific areas of review were recommended (e.g., motor operated valves actuators setting, surveillance requirements related procedures scope, etc.) and incorporated to the program.

Adequacy of Completion of Construction "Open Items".

The aim of this review area is to ensure the adequacy of completion of plant construction works, specially in aspects of small detail. To accomplish this, and
using the "Open Items" Data Banks generated in the different stages of construction and commissioning, a review is to be carried out to ensure the effective resolution of every "Open Item".

Design Changes.

The goal of this area is: a) to review all design changes introduced since plant start-up in order to ensure that no unresolved deficiencies are underlying these design changes. Should any significant deficiency of this kind arise, a corresponding specific review area would be defined. b) to review implementation adequacy of design changes defined during construction and commissioning phase.

Due to the high number of these design changes, part b) review is performed by sampling. Depending on the results, the possible extension of the initial sampling would be considered. This specific area is mainly related with piping support and snubbers, subject of most of design changes issued during the construction and commissioning phases.

This revision process is generating a high figure of detailed design basis changes, system descriptions, etc, therefore by the end of the process several documents are going to be written down anew and it is expected to obtain:

- Complete design basis definition for all safety systems. For each safety system, an specific study will be issued describing in detailed the basic design requirements and safety functions accomplished by the system in all different design scenarios.

- Complete redefinition of commissioning tests required scope and acceptance criteria. Complete review of commissioning tests results.

- Complete updating of plant design documents.

The program started in January 1995 and it is expected to be completed by the end of 1996, however definitive resolution of some issues resulting from the program will be deferred from this date, e.g., design modifications of the electrical distribution system is planned to be designed by October 1996, its actual implementation is scheduled for at least one year later though. A very important effort has been dedicated to the program execution, including the corrective measures to cope with the program findings. The main organizations engaged in the program are Trillo NPP, Siemens KWU -NSSS supplier- and Empresarios Agrupados -the architect engineer.

4.2. Program results
Around half of design/construction/commissioning deviations identified so far consist just of documental deficiencies. About one third are referred to minor deviations not relevant for safety functions, related with diverse design, construction or commissioning issues.

The remaining topics, about one sixth of the identified deviations, involve some degree of safety relevance. Many of these safety-relevant findings refer to piping support and snubbers and seismic design.

Most safety significant findings of the AOES program identified so far are:

- Deficiencies of Residual Heat Removal Chain (ECCS/CCW/ESW).

  Several cases were identified where Residual Heat Removal Chain did not fulfil the design criterion "N + 2" (this criterion requires that the system shall have enough redundancy to fulfil its safety function assuming the worst single failure and one train unavailable for maintenance). The necessary design changes were identified and recently implemented, in the interim the allowed unavailability of every train of the chain was severely limited.

- Deficiencies in Emergency Feedwater System.

  A deficiency was related with no compliance of "N + 2" criterion in certain scenarios. Design changes were introduced to cope with this issue, in the interim administrative compensatory countermeasures were required. Another one included wrong setting of flow control valves of the system, because commissioning process mistakes. The required changes were implemented right after the discovery of the deviation.

- Deficiencies in A.C. Plant Systems.

  A complete in depth A.C. systems review has been started, as result of diverse detail deficiencies shown in the design. According to the conclusions gathered so far, safety functions are not jeopardized by these deficiencies, but divers design changes will be recommended to cope with weaknesses of the A.C. systems, such as very little power margin of some big transformers and some cable sections.

- Deficient HVAC design in Emergency Feedwater Building

  The specified temperature for the HVAC design of Emergency Feedwater Building, where most of the RPS cabinets are located, is 40°C, a figure apart from the design temperature required by applicable codes and the temperature used for HVAC design in similar plants: 35°C. This point is
important to ensure adequate electronic components behaviour in case of an accident involving loss of offsite power. A complete review of the affected HVAC system has been started to incorporate the required design temperature; meanwhile, an evaluation has been carried out to assess the power dissipated by the electronic devices of the cabinets and whether or not they would overpass or not the manufacturer temperature specification.

As mentioned before, a relatively high number of deficiencies have been identified in piping supports and snubbers (22 cases of deviations in this area). Some deviations have been accepted after new piping calculations, some others required changes in the supports and snubbers involved. Because of the relative high number of the deficiencies, a complete on field review of piping support and snubbers has been started.

A remarkable feature of the program is that it may open up new revision areas, although these have narrower scope. E.g., upon completion of the Operating Experience review, 11 new areas were opened up, such as review of primary coolant system thermal isolation regarding its design of thermal efficiency or review of the design interphase between two specific manufacturers of certain valves and their actuators.

4.3. Program follow-up by the Regulatory Authority

As mentioned earlier, the overall program scope and methodology were subjected to regulatory approval and the regulatory staff reviewed and required some changes to be included in the program-related procedures. Periodic and "on line" ("hot") information is sent to and commented with the regulatory staff.

From the Regulatory Authority point of view, a critical point was the timely, adequate assessment of findings, specially systems operability status and Technical Specifications compliance, as well as adequacy of corrective action plans defined for these findings.

As the plant is operating while the program is on going, so that a very important point was the need for additional measures to cope with:

- Uncertainties associated with the program, i.e., issues under evaluation, the possibility of additional deficiencies which may arise from a certain finding, etc.

- Short term corrective actions for safety deficiencies discovered, as well as insurance of plant safe operation until definitive countermeasures (i.e., design changes) have been implemented.
These additional measures were implemented as operational restrictions (additional to Technical Specifications requirements) that were adopted by the licensee on a voluntary basis, looking for maximum safety systems availability. These operational restrictions were discussed with and accepted by the Regulatory Authority and included points like:
Safety systems design has been considered, to any practical extent, as N + 1, instead of N + 2 as licensed. The main impact of this consideration is on preventive maintenance of safety systems during power operation, that used to be a common practice at Trillo NPP before the beginning of the program and has been banned as long as the program continues.

Further limitations to those included in the Technical Specifications, to allow unavailability of safety systems.

Line-up of standby systems in the event of certain predefined safety systems unavailability.

Within these operational restrictions, some of them are general, applicable up to the end of the program, some other have been issued as interim solution to cope with an specific finding.

5. LESSONS LEARNT

No matter how proven and reliable is the design, the grade of redundancy of safety devices provided (e.g., Trillo NPP has 4 Safeguards DG for emergency AC power, plus 4 Emergency DG dedicated to the Emergency Feedwater System), etc., what is essential to guarantee operability of the safety systems is:

- An integrated, comprehensive programme of surveillance tests, both for certifying the acceptance of safety systems during construction and for functional test at commercial operation.

- Test conditions shall reproduce real conditions as much as reasonably achievable.

- Step by step tests are acceptable for functional tests at power and verification of individual components, but a set of those tests should not substitute integrated tests (sensor to final device actuation), because, much more often than anticipated, system deficiencies remain unnoticed to component tests.

At Trillo NPP a vast design revision program has been undertaken as response to operating experiences taken place at the plant. It evidences that available operating experience, if analyzed rigorously and in depth, shows the root causes that produce events at a plant, that those root causes may pervade all across plant systems and organization. Likewise, AOES program of Trillo NPP shows that such a rigorous root cause analysis is an excellent tool to shape as ambitious a design revision program as
desired that may lead to major design modifications, significant revisions of procedures and other documents.
CONTRIBUTION FROM SWEDEN
Undetected failures in safety systems

Swedish contribution to the PWG1 of the OECD Nuclear Energy Agency

Jean-Pierre Bento

July 1996
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>3</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2 Design deficiencies</td>
<td>4</td>
</tr>
<tr>
<td>2.1 Emergency core cooling system / Re-analysis of design basis accidents</td>
<td>4</td>
</tr>
<tr>
<td>2.2 Containment integrity</td>
<td>5</td>
</tr>
<tr>
<td>3 Inadequate or incomplete testing</td>
<td>5</td>
</tr>
<tr>
<td>3.1 Pressure control system / Inadequate calibration and instrumentation set-points evaluation</td>
<td>5</td>
</tr>
<tr>
<td>3.2 Inadequate calibration and instrumentation set-points evaluation</td>
<td>6</td>
</tr>
<tr>
<td>4 Improper installation</td>
<td>7</td>
</tr>
<tr>
<td>4.1 Quality organisation deficiencies / inappropriate component selection</td>
<td>7</td>
</tr>
<tr>
<td>5 Inadequate control of modifications to safety-related systems</td>
<td>8</td>
</tr>
<tr>
<td>5.1 Inadequate design control and post-modification testing / component cooling system</td>
<td>8</td>
</tr>
<tr>
<td>5.2 Inadequate post-modification testing</td>
<td>8</td>
</tr>
<tr>
<td>5.3 Inadequate design control and post-modification testing / residual heat removal system</td>
<td>9</td>
</tr>
<tr>
<td>5.4 Inadequate design control of post-modification testing / core cooling system</td>
<td>9</td>
</tr>
<tr>
<td>6 Conclusions</td>
<td>10</td>
</tr>
<tr>
<td>Appendix: Information about the Swedish projects</td>
<td>12</td>
</tr>
<tr>
<td>&quot;BOKA&quot;, &quot;REDA&quot;</td>
<td>12</td>
</tr>
</tbody>
</table>
Summary

The present report represents the Swedish contribution to the Nuclear Energy Agency (NEA) project with the same title. This project is done within the activities of the Principal Working Group 1 on operating experience and human factors.

The scope of the study has been to review the last five years of operating experience of all Swedish nuclear units with the aim to identify, select and understand why deficiencies in safety systems (components, logic circuitry and structures) remained undetected during long time periods. With long time periods means here latent failure or unavailability time of one year or longer.

The scope of the study also encompasses the description of the corrective actions that would preclude or reduce the likelihood of similar events according to the identified causes.

The analysis of the Swedish operating experiences has been performed based on the review of on the one hand all Licensee Event Reports (LERs) reported during the last five years and on the other hand of the IRS data base. These experiences exhibit a broad safety spectrum, from safety insignificant events to one event (strainer clogging event of 1992) of world-wide safety implication for most LWRs.

The selected events have been chosen with consideration taken to the limitation regarding safety systems and to the classification scheme agreed upon by the project group. Accordingly, the events described in the present report represent a sub-group of a somewhat wider experience base.

1 Introduction

As learned from operating experiences, latent failures in nuclear plant systems have remained undetected for many years, in some cases since the unit(s) started commercial operation. Most often these latent failures are discovered through expanded control, testing and/or design review, or by the occurrence of unexpected events.

The present review of the last five years of operating experience from all Swedish nuclear units with respect to undetected failures in safety systems has been performed by selecting event reports related to failures hidden during times longer than one year. Furthermore the study has been limited, in accordance with the NEA-PWG1 project’s scope, to the following systems:

- pressure control system
- emergency electrical power sources
- auxiliary feedwater system
- fire prevention and protection system
- component cooling system
- residual heat removal system
- containment
- service water system
- emergency core cooling system.

In addition, in order to make easier the finding of specific conclusions, the events have been categorised according to the following, and within the project agreed, overall causal categories:
• design deficiencies
• inadequate or incomplete testing
• improper installation
• inadequate maintenance
• inadequate control of modifications to safety-related systems.

2 Design deficiencies

2.1 Emergency core cooling system / Re-analysis of design basis accidents

Barsebäck 2 - Clogged pump suction strainers in the wet well pool after spurious opening of a safety valve of the pressure control system (IRS 1294.00-04)

This event which occurred during start-up of Barsebäck 2 (ASEA BWR, 600 MWe, 1977) after the annual refuelling outage in July 1992 is one of the most interesting event considering its generic implication for the vast majority of LWRs. Even if this event has already been largely discussed within the international community, it has however to be handled in the present report.

The initiating event was the spurious opening of a safety relief valve on a main steam line inside the containment. When the valve opened, steam blew directly on adjacent piping and an unexpected large amount of mineral wool pipe insulation was dislodged and subsequently flushed down to the condensation pool (wet-well). Approximately one hour after the spurious valve opening, high differential pressure over the suction strainers to the containment spray pumps was observed in the main control room. This was apparently caused by clogging of the strainers by insulation material. The operators initiated the backflushing of the strainers to remove the insulation material from the strainers.

The original plant safety analysis estimated the time to clogging of these strainers and of the suction strainers of the low pressure core spray pumps to be, based among other on small scale tests, not less than 10 hours for a design basis LOCA. The Barsebäck incident demonstrated that clogging could de facto occur much earlier.

The preliminary analysis performed after the incident estimated that clogging could occur within the first 20 minutes. Subsequent analysis indicated even shorter times for clogging, down to a couple of minutes. The implication of the event analysis was that a fundamental safety principle for the design basis accident was violated, i.e. the Swedish "30-minutes rule" (the reactor safety should not depend on manual actions during the first 30 minutes after an event). The event indicated also that some of the assumptions in the NUREG guidelines (2988 & 0897) were not conservative, e.g. the pressure drop due to clogging and the time for strainer clogging.

Six weeks after the incident, the Swedish Nuclear Power Inspectorate (SKI) decided to revoke the operating licences for the five oldest Swedish BWRs with external circulation pumps. All five units had then already been shut down, after decisions made by the utilities.

Following these shutdowns the Swedish utilities initiated vast projects including tests, experiments (some full scale), simulation models and analysis in order to redesign the related parts of the plants and to fulfil the requirements in the FSAR. As a condition for restart of the units, these efforts resulted in the installation of new suction strainers with much larger areas, replacement of a
major part of the mineral wool insulation with metallic or glass fibre insulation, and improved backflushing arrangements.

2.2 Containment integrity
Barsebäck 2 - Corrosion of the containment steel liner (IRS 1390.00)

During the 1993 refuelling outage, leakage rate testing of the containment (at 0.3 MPa overpressure) was carried out. The test result indicated a 0.7% leakage per 24 hours, to be compared with the maximum permissible level of 0.35%, according to the Technical Specifications. Leakage rate testing is performed yearly according to different schemes. The previous similar leakage rate testing was performed in 1988 and indicated that the leakage rate was then below permissible level.

Subsequent inspection revealed a leak near a containment penetration in the wet-well. After drilling from the inside, towards the leaktight steel liner embedded in the concrete, corrosion attack was detected on the outside surface of the liner. The attack had led to cavities in the 7 mm thick steel plate.

Following this discovery, all the containment pipe penetrations were investigated by drilling small holes near the upper part of respective penetration. The liner was afterwards also investigated with ultrasound testing. When damage was found, part of the concrete was removed in order to perform additional testing. All damages (30 spots) had in common that they were located in the wet-well, no damage was found in the dry-well. Most of the corrosion attacks were minor, meaning the liner was still tight and with good margin to leakage.

The cause of the corrosion was assessed to be incorrect grouting during the initial erection of the containment. The grouting had not been performed according to construction specifications. Small air evacuation pipes were placed too far from the outside surface of the liner resulting in the presence of cavities in the upper part of the defective penetrations. High humidity from the concrete caused with time the liner to corrode.

The defective parts of the liner were replaced with new material and all cavities filled with concrete. Inspection of the other unit at Barsebäck did not reveal similar defects. At the other Swedish plants, the grouting technique has been different.

3 Inadequate or incomplete testing

3.1 Pressure control system / Inadequate calibration and instrumentation set-points evaluation

Ringhals 2-4: Incorrect setpoint of main steam safety relief valves (IRS 1550)

Ringhals 2 is a 875 MWe three loop W PWR with two turbines. Commercial operation started in 1975. There are six main steam safety valves on each one of the three main steam lines.

The analysis of the scram which occurred in October 1994 at Ringhals 2 showed that the main steam safety valves should have opened because the design opening pressure was exceeded for a short time. After that assessment Ringhals 2 was then shut down for safety valve inspection and testing. Ringhals 3 and 4 (915 MWe W PWR, 1981 and 1983) which have similar safety valves and use the same test equipment, were shut down 2 days later in December
1994 for similar actions. After analysis and corrective valve adjustments the units were restarted December 17, 1994.

The testing of the main steam safety valves is carried out with the unit in hot standby with operating pressure and temperature in the reactor coolant systems. During testing the valve stem is lifted by a pneumatic device which is mounted on the valve. The opening of the valve is identified by listening to the change in sound when the valve disc lifts from the valve seat. Thereafter the opening pressure is determined by converting the applied air pressure to a lift force which is exerted on the valve stem. The conversion is done with help of a conversion factor. The lift force represents the difference between the main steam line pressure and the opening pressure of the safety valve.

Detailed analysis showed that the incorrect setpoint was less than 10% too high at Ringhals 2 and less than 5% too high at both Ringhals 3 and 4. The main cause of the incorrect setpoint was an incorrect conversion factor. The locally pressure measurement in the main steam line while testing the valves has also contributed to adjustment errors: the steam pressure was determined from pressures gauges mounted on the main steam lines, and which are less accurate than the pressure transmitters located in the main control room. An hypothesis that the safety valves were delivered with incorrect set-points has not been ruled out. This situation has existed since initial commercial start-up of respective unit.

The main steam safety valves at Ringhals 2 were subsequently tested before the refuelling outage in May 1995. Their adjustment was assessed to be still deficient. The test equipment and methods being shared commonly by all three units, it was assumed that the opening pressure of unit 3 and 4 also were incorrectly adjusted. Shutdown of and testing at unit 3 confirmed the assumption. Unit 4 was also shutdown for a renewed testing and adjustment of the main safety valves. All adjustments were still found too high.

After these repetitive incorrect adjustments, extra testing devices have been purchased and calibrated against full scale laboratory testing of the safety valves. The testing procedure includes today:

- new constants unique for each pneumatic lifting device and with known accuracy intervals
- measuring the lifting pressure only when the pressure increases to the lifting device in order to avoid hysteresis
- determining the steam pressure with the average of three pressure transmitters which are read from the control room
- regularly calibration of the lifting devices.

3.2 Inadequate calibration and instrumentation set-points evaluation

Ringhals 4 - Pick-up voltage of diesel generator field breaker outside limits

Ringhals 4 is a 915 MWe W PWR which started commercial operation in 1983. During the refuelling outage 1995, maintenance activities of diesel generator #410 (DG) were performed. It was then noted that a voltage of 115 V DC was required to obtain function of the DG's field breaker.

If the manoeuvring voltage on the supplying bus had be lower than 115 V DC, then the breaker had not closed, resulting in the DG being not able to pick-up designed voltage (6 kV). Because the voltage on the supplying bus has been 118 V DC, the deficiency has not been observed during previous testing.
According to design specification, the field breaker must be able to close down to 85% of the nominal manoeuvring voltage (93.5 V DC).

The cause for the malfunction has been too early connecting up of the coil load reduction resistance. The resistance is connected, after the closure of the breaker, in series with the breaker coil in order to prevent overheating of the coil. This deficiency has most probably existed since the start of commercial operation, and was in its turn due to wrong adjustment of the auxiliary contactor in the field breaker.

The field breaker was properly adjusted and tested without remark. Correct pick-up function was verified at 92 V DC. The decision was also taken to perform preventive yearly maintenance of the field breaker on all DGs during the coming three years. This will be done in order to identify eventual changes or ageing effects. If no special problems are detected, the maintenance period will be increased to two years, which corresponds to the stipulated maintenance of each DG.

4 Improper installation

4.1 Quality organisation deficiencies / inappropriate component selection

Ringhals 3 - Boric acid pump #2 stops spuriously on thermal overcurrent protection during boration to cold shutdown

Ringhals 3 is a 915 MWe W PWR which started commercial operation in 1981. During power reduction to cold shutdown for the annual refuelling outage 1994, the control room operator started both boric acid pumps on "high speed". After about 10 minutes operation pump #2 stopped spuriously and an alarm for electrical failure was received. Activated thermal overcurrent protection was identified. This was reset and pump #2 was started again. The pump stopped again after about 10 seconds. The above checks and restarts were performed a couple of more times, all with the same result. The boric acid pump #2 was declared inoperable.

There are two 100% redundant boric acid pumps, so failure of one means that there is no redundancy at the pump level.

Functional testing of all boric acid pumps at Ringhals 3 and 4 showed that pump #2 had higher pressure head and higher current level than the other three pumps. The defective pump was replaced. During replacement it was noticed that the pump wheel had wrong dimension. Its diameter was 249 mm, meanwhile the correct dimension for this type of pumps at Ringhals 3 and 4 is 230 mm.

Further investigations of the maintenance records identified that the wrong pump was installed most probably in 1979 (before commercial start-up of the unit) as spare for the original one which had been removed from Ringhals 3 and installed in Ringhals 2 for replacement of a boric acid pump which had failed due to burned motor winding.

After the occurrence of this event, information has been provided to the mechanical staff to test pumps under fully realistic conditions and flows.
5 Inadequate control of modifications to safety-related systems

5.1 Inadequate design control and post-modification testing / component cooling system

Ringhals 3 & 4 - Temperature protection alarms for two out of four component cooling pumps not reconnected after modification

Ringhals 3 & 4 are both W PWR (915 MWe, 1981, 1983). In January 1993 it was found out in Ringhals 4 that the alarm for low temperature in the component cooling system did not actuate despite the temperature had decreased below the set-point 9 °C. Subsequent examination indicated that both pumps #3 and #4 were without alarm function for both low and high temperature in the system. Similar deficiencies existed in Ringhals 3.

The safety implication of these deficiencies is very limited, because redundant parameters in connecting systems will alert operators if out of limit temperatures are reached.

The cause of the latent deficiencies was assessed to be modification works during the annual refuelling outages 1988, when the alarm function in both units was disconnected and not restored after the completion of the modifications.

The pumps were used as stand-by pumps from the time for discovery to the respective unit’s annual refuelling outage 1995, when correct connection of the alarm function was made.

5.2 Inadequate post-modification testing

Ringhals 2 - Periodical testing of the charging pump rooms cooling not performed after modification

In January 1995, during the writing of a document for control of operational functionality of safety related components to be made during the coming refuelling outage, it was found that periodical testing of the charging pump rooms cooling in accordance with the Technical Specifications had not been performed since the refuelling outage 1988.

This testing had earlier been part of the testing of the charging pumps, because start of the actual room cooling automatically resulted in charging pump swap. After implementation of an improved fire separation of the charging pump rooms, and installation of separate room cooling, made during the refuelling outage 1988, the above automatic function had been replaced by thermostat control of the cooling. The modification resulted in the automatic testing of the cooling function, earlier part of the charging pump testing, to cease. This modification had not been reflected into similar modification of the operating and test instructions.

The safety implication could have been a delay in identification of malfunctions in the cooling system. In case of safety injection, this event could have resulted in a reduced, but not insufficient, cooling of the charging pump motors.

After the verification of correct function of the cooling fans, the actual test instruction was updated. Included is the annual calibration of the controlling thermostats.
5.3 Inadequate design control and post-modification testing / residual heat removal system

Ringhals 1 - Spurious stop of RHR-pump #2 due to poor adjustment of relay protection

Ringhals 1 is a 795 MWe BWR from ABB Atom which started commercial operation in 1976. During the 1995 refuelling outage RHR pump #2 was started and short thereafter the short circuit protection activated. The pump stopped. After control of the pump was performed locally and without any finding, the pump was restarted successfully. The electrical maintenance department received a work order on the pump, but could not under testing identify any failure neither on the engine itself nor in the relay protection.

During subsequent root cause analysis it was identified that the pump main breaker had one short circuit protection, assumed earlier to be blocked because adjusted in blocked position, which probably had been activated when the pump was started. The analysis showed that the protection was not blocked in spite of its adjustment, but received a signal which, considering the protection inaccuracy, could be activated by the start current and thus stop the pump.

RHR pump #2 is one of two 100% redundant pumps. Since refuelling outage 1990 pump #2 had been started one or two times a month without any problem. The same has been valid after the reported event. It is thus confident that it had been possible to restart the pump after the spurious stop, should a real demand have existed.

The failure mode could have an effect also on RHR pump #1 availability to start on demand.

The cause of the event has been assessed to date from 1989 and 1990 when preventive replacement of old breakers for several components was performed. The new breakers have "built-in" protection device. At the time of the replacement, the proper function of the device had not been identified which explains the poor adjustment of the protection relays.

As corrective action the protection trip set-point was increased to 320 ms in order to get enough margin compared with the start current. Both RHR pumps were then tested without remark. Other components with similar protection have been controlled and their protection relays adjusted to the same value. These components belonging to the containment cooling system, reactor component cooling system and service water system were later tested without remark.

5.4 Inadequate design control of post-modification testing / core cooling system

Oskarshamn 1 - Incorrect setting of pressure vessel water level transmitters

Oskarshamn 1 is a 445 MWe BWR from ABB Atom which started commercial operation in 1972. The unit has been shutdown as a consequence of the Barsebäck event in July 1992. Oskarshamn 1 resumed operation in December 1995. An almost total verification of the condition of the unit has been carried out, as well as extensive modernisation work. The decontamination of the reactor pressure vessel and its inspection from the inside represent pioneering work.
The reactor being defueled, in May 1993 the water level in the reactor pressure vessel was decreased as preparation for cutting and replacement of piping. Alarm for L4 low water level was obtained at -2.3 m on two out of four level transmitters. This value deviated from the L4 set-point which is -1.75 m.

The hypothetical consequence was that if a large LOCA was postulated, the reactor protection condition H8 which isolates the emergency primary condensor had been triggered somewhat later than provided in the FSAR. Forced blow-down (TB2) via the pressure control system was however available at the correct water limit (-1.75 m). The assessment is that when TB2 is activated, the water level in the reactor pressure vessel drops very fast to -2.3 m, thus also actuating the L4 alarm. The safety implication of the event was thus judged to be relatively insignificant.

The cause of the latent failure was a calculation error for the theoretical calibration signal for the level transmitter. In 1989 the water level monitoring system of the reactor pressure vessel was improved by density compensation of the reference legs. The error has been latent because of the assumption that the calculated calibration signal was correct. The event shows that the post-modification test program was not complete. Should simulation listings of the process computer have been examined, then had the error been discovered.

The actual level transmitters were adjusted and calibrated to the correct set-point.

6 Conclusions

As a result of an in-depth screening of the Swedish LER data base including more than 2000 events for the last five years of plant operation, the present report describe 13 events with latent failures in safety systems and according to the classification agreed upon within the PWG1 project group.

All events selected in the present report have human and organisational performance as root causes. A smaller percentage of these undetected failures was initially introduced during unit construction, meanwhile the majority of events has occurred during maintenance and modification works during refuelling outages. Considering these two aspects one has however to put the actual number of latent failures in the context that more than 50 000 maintenance and modification tasks have been performed at the Swedish units during the actual time period of five years.

Another aspect worth mentioning is that a significant percentage of these events exhibit Common Cause Failure character, in the meaning that two or more redundant components, systems or even two units have been exposed to the same latent deficiency(ies).

The event at Barsebäck, July 1992, with potential for clogging strainers in the core and containment cooling systems represents, because of its implication for western LWRs, the most significant event in the present study. This event has been widely discussed within the international nuclear community.

The event chain connected to the incorrect setpoint of the main safety relief valves in Ringhals 2-4 represents another event worth deeper considering. Generally speaking, the testing activities which take place at the plants are both numerous and extensive. Furthermore they are for safety related components and systems in most cases performed in accordance with periodic schemes. If
the test procedures are such that some failure mode in the equipment utilised for
the tests can not be revealed during the performance of the tests, then can latent
failures in the tested components exist for significant time periods. The Ringhals
2-4 event underlines the importance of a questioning attitude, from one time to
another, towards deep rooted or since long time used routines. In that particular
case, test routine and equipment keep to the same old beaten track, i.e. since
respective unit start-up.

Outgoing from the present study, it can be asserted that the most effective
single corrective action category to prevent the occurrence of undetected
failures in safety systems is a more systematic, thorough and realistic
operational readiness control and testing after maintenance and modification
activities. Such testing and control represent often the last barrier after
performed maintenance or repair to detect component and system deficiencies,
and prevent events. Operational readiness control should accordingly
encompass not only the modified or repaired component(s), but should also
include integral system testing and even be extended, on a case by case basis, to
testing of the complete relevant safety function.

Finally the present report identifies the occurrence of several latent deficiencies
originating in deficient work packages for tasks performed during refuelling
outages. In this respect, it is obvious that a well prepared work package
represents the first barrier and a prerequisite for the performance of failure free
maintenance and repair tasks. Apparently this obvious prerequisite has not
always been taken into full consideration by the staff responsible of the
preparation of the actual work packages. Such inaccurate or incomplete work
packages result often in latent failure(s) being implicitly implanted in the
component(s) and system(s) already in the task preparation stage. As efficient
corrective actions, plant management should re-emphasise for the concerned
personnel the primary importance of careful work package preparation, which
presuppose that enough time has been allocated before the annual refuelling
outages for the preparation and an independant checking of these work
packages.
Appendix: Information about the Swedish projects "BOKA", "REDA"

Following the event which occurred at Barsebäck 2 in July 1992, the Swedish utilities initiated comprehensive projects for the systematic assessment of the safety criteria to be fulfilled by the nuclear power units and of how well the units fulfill these requirements. (BOKA project is an acronym for the studies performed at Barsebäck and Oskarshamn, meanwhile REDA is performed at Ringhals. A similar project, RAK, is on-going for the Forsmark’s units).

All these exhaustive projects encompass furthermore the eventual identification of safety weaknesses in the plant’s design. The results of each project will be documented in a unit specific Safety Analysis Report (SAR) which will supersede today’s Final Safety Analysis Report (FSAR). The new acronym SAR has been chosen in order to underline that SAR will be a living document as far as new rules and regulations are developed, the unit(s) modernised, etc.

The most important idea with SAR is that all information which impact on or is related to the unit’s safe operation has to be included in the SAR. SAR must also clearly and distinctly demonstrate that each unit fulfil today’s requirements for the operation license.

Significant efforts in the development of the SAR are spend considering how the SAR is aimed to be utilised in the daily safety work of the unit operation, in addition to the fact that it represents an important document to provide the regulatory bodies with.

These studies are performed by the vendor(s) in close co-operation with the utilities. Existing safety reports, background reports, experiment results and design and construction reports are reviewed at depth by multi-disciplinary groups. These reviews are made in the light of today’s safety requirements. After the group(s) agreed upon the correct content of a specific report, each such report is approved for further use within each unit’s specific project. Each "approved" report is then part of the SAR or part of the background material for the resolution of a specific issue.

If, during the review process, the assessment is made that a requirement is not fulfilled by the present FSAR, then a discrepancy or a significant discrepancy is identified and classified as such for resolution within the project.

The actual projects represent together an impressive amount of work. They were initiated in 1994-95 with a reporting time set to year 1998. The efforts devoted within these projects are more than 300 person-years of studies.
CONTRIBUTION FROM THE UNITED STATES
ADDITIONAL INFORMATION IN SUPPORT OF PWG1 STUDY OF 
UNDETECTED FAILURES OF SAFETY SYSTEMS

General Notes on the Content and Organization of Appendixes:

1. The 33 events were selected for this study from the Accident Sequence Precursor 
(ASP) data base for 1991 through 1993. These events are listed in Appendix A, 
Section I, by their plant name, Licensee Event Report (LER) number, and LER 
description. Note that same event, if applicable to different units at multi-unit sites, is 
counted as multiple events, thus counting a total of 33 events.

2. The ASP data base provided the values of the conditional core damage probability 
(CCDP) of these events, as well as the CCDP of a set of certain postulated events. 
This provided a qualitative reference for comparison of CCDP of the events under 
study to the CCDP of the postulated events. The span of CCDP of the set of 
postulated events is usually about three decades. The span could be divided into three 
parts: upper, middle, and lower, each about a decade. The CCDP of 3 of the 33 
events under study exceeded the span of the postulated events, the remainder of the 33 
events falling into one of the three parts. Thus, the 33 events studied are classified 
into 4 groups (Groups 1: exceeding the span, Group 2: Upper, Group 3: Middle, and 
Group 4: Lower part of the span), as shown in Appendix A, Section I.

3. In Appendix A, Section I, alpha- numeric codes are used for categorization of failure 
cause, discovery method, and corrective/ preventive actions. Appendix B contains a 
complete list of all codes used. All categories listed in AEN/NEA letter dated 
December 4, 1995 are included in Appendix B. Where a specific situation does not 
match any of the categories listed by AEN/NEA, additional categories are included in 
Appendix B. Descriptions of codes associated with the 33 events analyzed are also 
given in Appendix A, Section II, for easy reference.

4. The distribution of the 33 events under various codes (ranked in the order of 
decreasing frequency) is given in Appendix A, Section II.

5. The categorization is based on the description found in the actual LERs associated 
with these events and/or the event summaries included in Appendix C. The relevant 
parts of the write-up are extracted and included in Appendix C, along with appropriate 
codes, to provide the reader the basis and context of this categorization.

Enclosure
6. In addition to summary of each event, Appendix C includes writeup on failure cause, method of discovery, and corrective/preventive actions (licensee's actions and regulatory actions). The regulatory actions included are limited to Augmented Inspection Team (AIT), Incident Investigation Team (IIT), NRC Generic Communications (Information Notice, Generic Letter, and Bulletins). The AIT and IIT information is obtained by searching the AIT/IIT reports and AEOD Annual Reports. The NRC Generic Communication information is obtained by searching the data base in NRC's Event Tracking System (ETS). Please note that certain regulatory actions such as Enforcement Actions (Notice of Violation, Enforcement Conference, Civil Penalty, etc.) are not included. Please also note that, due to limited time, certain other items discussed in the enclosure to the AEN/NEA December 4, 1995 letter are not included in Appendix C (e.g., Factors Contributing to Difficulty of Discovery, Safety Significance, and Insights from Licensee and Regulatory Efforts to Resolve Safety Issues), although attempts were made in a few cases to get a feeling of the extent of work involved.

7. Some of the licensee's corrective actions were incomplete when the original LER was written. These actions are identified by an asterisk (*) by the side of their codes, as shown in Appendixes A and C. These actions are now verified by the licensee contact as complete, except as specifically noted otherwise.
APPENDIXES

Appendix A  Categorization of 33 Events Involving Undetected Failures of Safety Systems

Appendix B  Codes Used for Categorization of Failures

Appendix C  Summary, Causes, Method of Discovery, Corrective/Preventive Actions for Events Involving Undetected Failures of Safety Systems
APPENDIX A
CATEGORIZATION OF 33 EVENTS INVOLVING
UNDETECTED FAILURES OF SAFETY SYSTEMS

I. Categorization (by code) of Failure Cause, Discovery Method, and Corrective/Preventive Actions:

LER#/Descr. | Plant Name | Failure Cause | Discovery Method | Corrective/Preventive Actions | Licensee's | Regulatory Actions |
-------------|------------|---------------|------------------|-------------------------------|------------|-------------------|
|             |            |               |                  |                               |            |                   |

1. Events with CCDP > Any Postulated Event (Group 1 Events):

400/91-008: HPI unavailability for one refueling cycle because of inoperable miniflow lines
Harris 1 [CC1],[CE1] [D15] [A39] [A18]

423/91-011: Both trains of HPSI inoperable due to relief valve failures
Millstone 3 [CE1] [D15] [A39]

278/91-017: Control wiring for ADS/relief valves found damaged
Peach Bottom 3 [CC1] [D16] [A46],[A48]

2. Events with CCDP in Upper Third of Its Span (Group 2 Events):

336/91-009: Both diesel generators unavailable and unit shutdown
Millstone 2 [CB1],[CC1] [D15] [A43]*,[A39]*,[A40]

440/91-009: Two EDGs inoperable
Perry 1 [CB1] [D15] [A43],[A39]

269/91-010, 270/91-010, 287/91-010: Potential for hydrogen entrainment in HPI pumps
Oconee 1,2,3 [CA1] [D17] [A40],[A42]*

265/93-010 and -012: Emergency Power System Unavailable
Quad Cities 2 [CE1] [D15] [A39]
313/93-003: Both Trains of Recirculation Inoperable for 14 h
Arkansas 1 [CC1] [D17] [A43]

413/93-002, 414/93-002: Essential Service Water Potentially Unavailable
Catawba 1,2 [CA1], [CA2], [D15] [A34]*, [A39]
 [CB1]

3. Events with CCDP in Middle Third of Its Span (Group 3 Events):

483/92-011: Loss of Main Control Board Annunciators
Callaway [CB1], [CE2] [D16] [A39]*, [A40], [A16], [A18]
 [A43]

261/92-013: Safety Injection Pump Out of Service
Robinson 2 [CC5] [D18]* [A44]*, [A45] [A18]

269/92-018, 270/92-018, 287/92-018: Both Keowee Emergency Power Hydro Units Potentially Unavailable
Oconee 1,2,3 [CE1] [D15] [A39]

301/92-003: Plugged Safety Injection Pump Suction
Point Beach 2 [CC5] [D15] [A44], [A45], [A46]

213/93-006 and -007: Degradation of Motor Control Pressurizer Power-Operated Relief Valve, and Emergency Diesel Generators
Haddam Neck [CE1] [D05], [A39] [A16], [A18]
 [D15]

4. Events with CCDP in Lower Third of Its Span (Group 4 Events):

206/91-014: Inoperable volume control tank level transmitters
San Onofre 1 [CB1], [D17] [A40], [41],
 [A46]*, [A47]

445/91-012: Potential charging pump unavailability due to hydrogen void expansion
Comanche Peak 1 [CA2] [D08], [A40]*
 [D09]

A-2
272/91-030: Both PORVs failed due to leaking actuators
Salem 1  [CB1]* [D15] [A39]*,[A41]

281/91-017: Both emergency diesel generators for Unit 2
inoperable for 13 h
Surry 2  [CE2],[CC1] [D17] [A41],[A45]

328/92-010: Emergency Diesel Generator and Residual Heat
Removal Pump Inoperable
Sequoyah 2  [CE2],[CC1] [D15],[A43],[A46]
[D17]

269/92-008, 9/92-008, 9/92-008: Both Keowee Emergency Power
Hydro Units Unavailable
Oconee 1,2,3  [CB1] [D17] [A40]*,[A46]

286/92-011: Multiple EDGs Inoperable
Indian Point 3  [CA2],[CE2] [D15] [A40],[A46]*,
[A48]

289/93-002: Both Residual Heat Removal Heat Exchangers
Unavailable
TMI-1  [CE3],[CE4] [D19], [A40]*,[A46]*

412/93-012: Failure of Both Emergency Diesel Generator Load
Sequencers
Beaver Valley 2[CB1],[CE1] [D15], [A39],[A49]* [A16],[A18]

498/93-005 and -007: Unavailability of One Emergency Diesel
Generator and the Turbine-Driven Auxiliary Feedwater Pump
STP-1  [CC1],[CC2], [D15], [A41],[A43]*, [A16],[A18]
[CE5]
[A46]*

*  See the Enclosure, Note 7.
II. Distribution (by code) of Failure Cause, Discovery Method, and Corrective/Preventive Actions:

Note: The number of events which fall under each code, as categorized in Section I above, are counted and their distribution, ranked in the order of decreasing frequency, is given below:

Failure Cause Codes:

[CB1] Component failure: 11 events
[CE1] Design deficiency: 10 events
[CC1] Inadequate testing or maintenance procedures: 7 events
[CA2] Conditions not previously considered in design basis reviews: 4 events
[CE2] Maintenance error: 4 events
[CA1] Inadequacies in design basis studies: 3 events

[CC5] Foreign bodies left in piping: 2 events
[CC2] Ineffective operating experience feedback: 1 event
[CE3] Operator error: 1 event
[CE4] Deficiencies in operating procedure: 1 event
[CE5] Deficiencies in communication: 1 event

Discovery Method Codes:

[D15] Testing: 19 events
[D17] Analysis/evaluation of operational problems: 10 events
[D16] Preventive/Corrective maintenance: 2 events
[D05] Individual Plant Examination (IPE): 2 events
[D08] Response to NRC Information Notice (IN), Generic Letter (GL) and Bulletins (BL): 1 event
[D09] Response to NSSS Vendor's information notices: 1 event
[D18] Operational problems (plant startup, normal operation, or shutdown): 1 event
[D19] System line-up verification: 1 event

Corrective/Preventive Actions Codes:

Licensee's Actions:

[A39] Design change/plant modification: 16 events
[A40] New or change in operating procedure: 11 events
[A46] Additional training/guidance to plant personnel: 8 events
[A43] Change to maintenance procedure: 6 events
[A41] Corrective maintenance, repair/replace failed component: 4 events
[A42] Change to Design Basis: 3 events
[A45] Post-maintenance verification testing/
<table>
<thead>
<tr>
<th>Event</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A34] Assessment of modifications' implementation and subsequent requalification:</td>
<td>3 events</td>
</tr>
<tr>
<td>[A44] Removal of foreign material by flushing:</td>
<td>2 events</td>
</tr>
<tr>
<td>[A48] New or change in Administrative Procedure/Management Directives:</td>
<td>2 events</td>
</tr>
<tr>
<td>[A47] New or change to Technical Specifications:</td>
<td>1 event</td>
</tr>
<tr>
<td>[A49] New or change in Engineering/Design procedure:</td>
<td>1 event</td>
</tr>
</tbody>
</table>

Regulatory Actions:

<table>
<thead>
<tr>
<th>Event</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A18] NRC Generic Communication (Information Notice (IN), Generic Letter (GL), or Bulletins (BL)) issued included the event:</td>
<td>7 events</td>
</tr>
<tr>
<td>[A16] NRC Augmented Inspection Team (AIT) investigated the event:</td>
<td>5 events</td>
</tr>
</tbody>
</table>
APPENDIX B
CODES USED FOR CATEGORIZATION OF FAILURES

Codes for Failure Cause and Type (Based on Cause)

Codes for items in groups a), b), c), and d) of part A) of the enclosure to the AEN/NEA Letter dated December 4, 1995 and others not specifically listed (group e):

Causes in Group a):

[CA1] Inadequacies in design basis studies
[CA2] Conditions not previously considered in design basis reviews

Causes in Group b):

[CB1] Component failure
[CB2] Deficiencies in environmental qualification
[CB3] Deficiencies in fabrication and installation
[CB3] Unforeseen interaction between systems
[CB4] Aging

Causes in Group c):

[CC1] Inadequate testing or maintenance procedures
[CC2] Ineffective operating experience feedback
[CC3] Inadequate implementation of modifications
[CC4] Improper review or implementation of vendor recommendations
[CC5] Foreign bodies left in piping

Causes in Group d):

[CD0] Combination of different failures

Causes in Group e (Others):

[CE1] Design deficiency
[CE2] Maintenance error
[CE3] Operator error
[CE4] Deficiencies in operating procedure
[CE5] Deficiencies in communication

Codes for Discovery methods

Codes for items under "Mean or method of discovery" section of part A) of the enclosure to the AEN/NEA Letter dated December 4, 1995 and other categories not specifically listed in that section:

[D01] Design review
[D02] Safety Assessment
[D03] Periodical Safety Reassessment (PSR)
[D04] Probabilistic Risk Assessment (PRA)
[D05] Individual Plant Examination (IPE)
[D06] Fortuitous (i.e., by chance)
[D07] National or international operating experience feedback
[D08] Response to NRC Information Notice (IN), Generic Letter (GL) and Bulletins (BL)
[D09] Response to NSSS Vendor's information notices
[D10] Functional inspections
[D11] Augmented Team Inspections (AITs) subsequent to significant events
[D12] Inservice inspections
[D13] Walkdowns
[D14] Questioning attitude

Other Categories:
[D15] Testing
[D16] Preventive/ Corrective maintenance
[D17] Analysis/ evaluation of operational problems
[D18] Operational problems (plant startup, normal operation, or shutdown)
[D19] System line-up verification

Code for Corrective and Preventive Actions

Codes for items under categories 1), 2), and 3) in part B) of the enclosure to the AEN/NEA Letter dated December 4, 1995 and other items not specifically listed in that part:

Regulatory Actions (Category 1)

[A11] Periodic safety reassessment
[A12] Decennial inspections (specific to France)
[A13] Probabilistic Risk Assessment
[A14] Individual Plant Examination (specific to US)
[A15] Implementation of clearer Technical Specification surveillance requirements and limiting conditions of operation

Others:
[A16] NRC Augmented Inspection Team (AIT) investigated the event
[A17] NRC Incident Investigation Team (IIT) investigated the event
[A18] NRC Generic Communication (Information Notice (IN), Generic Letter (GL), or Bulletins (BL)) issued included the event
[A19] NRC Enforcement Actions (Notice of Violation, Enforcement Conference, Civil Penalty, etc.) issued

Insights from Licensee and Regulatory Efforts to Resolve Safety Issues (Category 2)

[A21] Design Basis Reconstitution studies

B-2
[A22] Engineering evaluation studies
[A23] Generic studies reports
[A24] Operating experience feedback reports
[A25] Assessment of significant operating events (e.g., Salem, ...)

Licensee's Actions (Category 3)

[A31] Inservice testing procedure
[A32] Preventive maintenance programs
[A33] Post-maintenance procedures
[A34] Assessment of modifications' implementation and subsequent requalification
[A35] Trending specific parameters affecting component operation, and use of appropriate diagnostic tools
[A36] Premature aging anticipation policy
[A37] Inspection guides
[A38] Quality assurance

Others:

[A39] Design change/ plant modification
[A40] New or change in operating procedure
[A41] Corrective maintenance, repair/ replace failed component
[A42] Change to Design Basis
[A43] Change to maintenance procedure
[A44] Removal of foreign material by flushing
[A45] Post-maintenance verification testing/ examination
[A46] Additional training/ guidance to plant personnel
[A47] New or change to Technical Specifications
[A48] New or change in Administrative Procedure/ Management Directives
[A49] New or change in Engineering/ Design procedure
APPENDIX C

SUMMARY, CAUSES, METHOD OF DISCOVERY, CORRECTIVE/ PREVENTIVE ACTIONS FOR EVENTS INVOLVING UNDETECTED FAILURES OF SAFETY SYSTEMS

1. Events with CCDP > Any postulated Event (Group I Events):

1. Event Summary

LER No.: 400/91-008
Event Description: HPI unavailability for one refueling cycle because of inoperable miniflow lines
Date of Event: April 3, 1991
Plant: Harris 1

Summary

Harris is equipped with three charging/safety injection pumps (CSIPs) that provide charging and seal flow during normal operation and provide high-pressure injection (HPI) during accidents. Each pump is provided with a normal minimum flow path and an alternate minimum flow path for pump protection. During normal operations, the minimum flow path is via the seal water heat exchanger back to the pump suction. During safety injection (SI) operation, this path is isolated, and two alternate paths via relief valves to the reactor water storage tank (RWST) are aligned. Tests conducted during a refueling outage revealed that both relief valves were failed, as well as associated piping. Had HPI been demanded during the operating cycle, sufficient flow would have been diverted via the alternate miniflow system to fail the injection function. Under some circumstances, pump runout and failure could also have resulted.

The conditional core damage probability estimated for this event is 6.3 x E-3. This event CCDP was greater than that calculated for any of the postulated events.

2. Failure Cause and Type (Based on Cause)

The cause of this event was water hammer that apparently occurred because of an air void that remained in the alternate miniflow lines following previous testing and maintenance [LER 400/91-008]. The causes of air void were a design deficiency [CE1] (i.e., having no provision for venting) and inadequate maintenance procedure [CC1].

3. Method of Discovery

Tests conducted during a refueling outage revealed that both relief valves were failed, as well as associated piping [D15].

C-1
3.1 Factors Contributing to Difficulty of Discovery

The normal minimum flow path is the one normally used during normal plant operation. The alternate minimum flow path is used only while testing during refueling outages or during an accident. Water hammer in these lines which occurred while testing during the previous refueling outage had damaged both relief valves and associated piping. The failure remained undetected until the testing was done again, during the next refueling outage.

3.2 Safety Significance

Had HPI been demanded during the operating cycle, sufficient flow would have been diverted via the alternate miniflow system to fail the injection function. This was a common mode failure, affecting components in both trains of the system.

4. Corrective and Preventive Actions

4.1 Regulatory Actions

- NRC Information Notice 92-61, Loss of High Head Safety Injection, issued. [A18]

- Enforcement Conference was conducted on October 14, 1992 (see Letter to NRC, November 5, 1992). [A19]

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To determined by AEN/NEA)

4.3 Licensee's Actions

Supports were added [A39] to the test connection lines to prevent pipe cracking. The relief valve installation instructions were changed to require both filling the pipe prior to relief valve installation and venting the pipe through the relief valve after installation to eliminate the air void [temporary fix]. Later, plant modifications [A39] were made in 1992, replacing relief valves with orifices and changing the MOV logics [see the letter to NRC dated November 5, 1992].
I. Events with CCPD > Any postulated Event (Group I Events) (Cont.):

1. Event Summary

LER No.: 423/91-011
Event Description: Both trains of HPSI inoperable due to relief valve failures
Date of Event: April 10, 1991
Plant: Millstone 3

Summary

During testing of the high-pressure safety injection (HPSI) system while in Mode 3, the "A" HPSI relief valve lifted and would not reseat until the running HPSI pump was stopped. Flow loss through the stuck-open valve was 79 gpm. An investigation determined that the incident occurred because the design relief valve set pressure was too close to system operating pressure. A similar condition existed with the "B" HPSI relief valve; however, it was "gagged shut" during the test to prevent it from lifting, and therefore no failure of the "B" valve was noted. Had both valves lifted during accident conditions, the system would have been unable to perform its safety function.

The conditional core damage probability for this event is conservatively estimated to be 8.1 x E-4. This event CCPD was greater than that calculated for any of the postulated events.

2. Failure Cause and Type (Based on Cause)

The root cause of the event is design deficiency [CE1]. The setpoint for the relief valves was too close to the operating pressure of the system.

3. Method of Discovery

During testing of the high-pressure safety injection (HPSI) system [D15]

3.1 Factors Contributing to Difficulty of Discovery

The failure would not have been identified unless the required testing was done.

3.2 Safety Significance

Had both valves lifted during accident conditions, the system would have been unable to perform its safety function.
4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To determined by AEN/NEA)

4.3 Licensee's Actions

A test procedure was written, approved, and performed that utilized the appropriate steps of the surveillance procedure to duplicate the conditions that existed when the relief valve lifted. Instrumentation was installed on the safety injection system to provide a trace of the actual pressure seen by the relief valve. The testing verified that the pressure in the system exceeded the relief valve setpoint pressure. The test procedure verified that other combinations of valve and pump manipulations did not subject the relief valves to pressures higher than their new lift setpoint [A39] of 2250 psia.
I. Events with CCDP > Any postulated Event (Group I Events) (Cont.):

1. Event Summary

LER No.: 278/91-017
Event Description: Control wiring for ADS/relief valves found damaged
Date of Event: September 24, 1991
Plant: Peach Bottom 3

Summary

Improperly installed insulation on the automatic depressurization system (ADS) / safety relief valves (SRVs) resulted in damage to SRV control wiring. This condition existed throughout the refueling cycle. The high-pressure coolant injection (HPCI) system was also unavailable for periods of time during that interval. The conditional core damage probability estimated for this event is 3.3 x E-4. This event CCDP was greater than that calculated for any of the postulated events.

2. Failure Cause and Type (Based on Cause)

The cause of this event has been determined to be that the MSRV insulation was improperly installed. The maintenance procedure [CC1] used to remove and reinstall the MSRV thermal insulation did not provide the necessary level of detail to ensure that the insulation was properly installed.

3. Method of Discovery

On 9/24/91 at 1300 hours, during the performance of routine preventive maintenance [D16] on the Main Steam Relief Valve (MSRV) solenoid valves (SV) associated with the present Refueling Outage, the MSRV SV wiring insulation was discovered to be degraded. An investigation revealed that the MSRV thermal insulation was improperly installed (see attached drawing) during the previous Refueling Outage in 1989. This caused an unusually high temperature environment in the immediate vicinity of the SVs and associated wiring. This high temperature condition caused the MSRV SV wiring insulation to degrade. [LER 278/91-017]

3.1 Factors Contributing to Difficulty of Discovery

(To determined by AEN/NEA)

3.2 Safety Significance

On 11/8/91, it was determined by engineering analysis that there was no longer a reasonable assurance that the Automatic
Depressurization System (ADS) (EIIS: RV) relief valves were operable.

4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To determined by AEN/NEA)

4.3 **Licensee's Actions**

The main steam relief valve thermal insulation was removed and reinstalled properly and the solenoid valves were replaced. Administrative procedure A-25, "Plant Work Process," [A48] was revised to include sufficient detail to properly control installation and removal of thermal insulation [see Rev.1 of the LER]. Additional training was given to maintenance personnel [A46] [see Rev.1 of the LER].
II. Events with CCDP in Upper Third of Its Span (Group II Events):

1. Event Summary

LER No.: 336/91-009
Event Description: Both diesel generators unavailable and unit shutdown
Date of Event: August 21, 1991
Plant: Millstone 2

Summary

Both emergency diesel generators (EDGs) were found to exhibit erratic load control, a result of either a resistance change in the "droop" potentiometer in the electronic governor controls or contaminated oil in the hydraulic actuator units. This second cause would result in EDG inoperability under all circumstances; the first cause would only impact paralleled operation. Assuming, for the purposes of this analysis, that the EDGs would be inoperable following a postulated loss of offsite power (LOOP), a conditional core damage probability of $2.1 \times 10^{-4}$ is estimated. This event CCDP was in the upper third of CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The failure of both EDGs was caused by erratic operation of each EDG’s Woodward Governor EG-A electronic control unit. Two potential causes were identified. The first involves large resistance changes [CB1] in the EG-A "droop" potentiometer, which can result in large load swings while the EDG is running paralleled to the grid. The "droop" potentiometer is not used when the EDG alone is supplying power to the safety-related buses, and its failure would not affect EDG operability during emergency operation. The second potential cause, which would impact EDG operability under all circumstances, involved contaminated hydraulic oil [CC1] in the hydraulic actuator unit—foreign material was found when the unit was disassembled.

3. Method of Discovery

On August 21, 1991, with the plant at 90% power and EDG 13U out of service for maintenance, redundant EDG 12U was running loaded and paralleled to offsite power to demonstrate operability [D15]. At the end of a 1-h run, the EDG load control became erratic. EDG 12U output breaker was opened, and the EDG was reparalleled, but erratic speed control caused load swings that prevented reloading.
3.1 Factors Contributing to Difficulty of Discovery

(To determined by AEN/NEA)

3.2 Safety Significance

(To determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To determined by AEN/NEA)

4.3 Licensee's Actions

The governor units on each diesel generator were replaced [A40]. The maintenance department was directed to modify the maintenance procedure [A43]* [not complete as 2/96] to include flushing the hydraulic operator fluid to preclude oil contamination. Planning was initiated to upgrade the diesel generator controls with a replacement system of a newer design [A39]*.
II. Events with CCDP in Upper Third of Its Span (Group II Events) (Cont.):

1. Event Summary

LER No.: 440/91-009
Event Description: Two EDGs inoperable
Date of Event: March 14, 1991
Plant: Perry

Summary

Perry was operating at 100% power on March 14, 1991, when the Division 2 emergency diesel generator (EDG) failed a surveillance test. Subsequently, the Division 1 EDG also failed its surveillance test. It took 11 h and 55 min to restore one EDG to operable status. It was later determined that one EDG had been inoperable for over 28 d, and the other EDG was potentially unavailable for 15 d. The conditional core damage probability estimated for this event (assuming both EDGs were unavailable for 15 d) is 5.3 x E-4. This event CCDP was in the upper third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The root cause of both events was equipment malfunction. The Division 2 DG field contact or K1 failed to close due to a component failure [CB1], which occurred at completion of the last successful diesel surveillance run during engine shutdown on February 14, 1991. The Division 1 DG equipment malfunction was isolated to the governor control circuit, which was serviced and tested prior to declaring the DG operable.

3. Method of Discovery

Perry was operating at 100% power on March 14, 1991, when the Division 2 emergency diesel generator (EDG) failed a surveillance test. Subsequently, the Division 1 EDG also failed its surveillance test. [D15]

3.1 Factors Contributing to Difficulty of Discovery
(To determined by AEN/NEA)

3.2 Safety Significance
(To determined by AEN/NEA)
4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To determined by AEN/NEA)

4.3 **Licensee’s Actions**

Implemented design changes [A39] to enhance reliability of the field contact or by monitoring critical component position and addition of an electrical seal-in feature. Revised the periodic maintenance instruction [A43] to incorporate specific inspection criteria and service.
II. Events with CCDP in Upper Third of Its Span (Group II Events)  
(Cont.):  

1. Event Summary  
LER No.: 269/91-010, 270/91-010, 287/91-010  
Event Description: Potential for hydrogen entrainment in HPI pumps  
Date of Event: September 19, 1991  
Plant: Oconee 1, Oconee 2, and Oconee 3  

Summary  
During an analysis of the letdown storage tank (LDST) high-pressure alarm set point, it was determined that the potential existed for hydrogen entrainment in the high-pressure injection (HPI) pumps during small-break loss-of-coolant accident (LOCA) scenarios involving failure of either of the borated water storage tank (BWST) isolation valves to open. LDST hydrogen over pressure is normally adjusted so that the BWST will provide flow to the HPI pumps during a safety actuation. In this situation, the higher BWST pressure seats the LDST outlet check valve and prevents hydrogen from expanding into the HPI pump suction piping. During review of a 1971 Babcock & Wilcox curve of maximum LDST pressure as a function of inventory, it was determined that the curve was based on an assumption that the LDST would be isolated within 6.5 min for certain scenarios. This action is not specified in the procedures. In addition, the single valve provided for this purpose is not safety-related nor is it provided with safety-related controls or power.  

Subsequent analyses by the utility, which considered flow-related pressure drops, indicated that hydrogen entrainment would only occur if one of the BWST isolation valves failed to open. In this case, the additional pressure drop in the single operating line would allow hydrogen to expand into the HPI pump suction lines and damage the pumps.  
The conditional core damage probability estimated for this event is 1.2 x E-4. This event CCDP was in the upper third of the CCDP span for the postulated events.  

2. Failure Cause and Type (Based on Cause)  
The 1971 curve was based on calculations that addressed static head differences, but did not consider pressure drops due to flow. [CALC] Calculations performed by the utility after this problem was discovered, which addressed flow-induced pressure drops, indicated the existing LDST hydrogen pressure curve was adequate for most scenarios without closure of HP-23. The one exception
was a small-break LOCA during which one of the two BWST isolation valves fails to open. In this case, all HPI injection flow would pass through one suction supply line, which would lead to higher pressure losses and lower pressure in the suction supply header, and would result in hydrogen entrainment from the LDST and HPI pump damage.

3. **Method of Discovery**

During an analysis [D17] of the letdown storage tank (LDST) high-pressure alarm set point, it was determined that the potential existed for hydrogen entrainment in the high-pressure injection (HPI) pumps during small-break loss-of-coolant accident (LOCA) scenarios involving failure of either of the borated water storage tank (BWST) isolation valves to open.

3.1 **Factors Contributing to Difficulty of Discovery**

(To determined by AEN/NEA)

3.2 **Safety Significance**

(To determined by AEN/NEA)

4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To determined by AEN/NEA)

4.3 **Licensee’s Actions**

The operating procedure was revised [A40] to incorporate new letdown storage tank pressure and level curves. The emergency procedure was revised [A40] to include requirements for an immediate line up change in the event of a single failure of certain valves during a small break LOCA. Planned action includes development of a more restrictive curve [A42]* so that operator action will not be required.
II. Events with CCPD in Upper Third of Its Span (Group II Events) (Cont.):

1. Event Summary

LER Nos.: 265/93-010 and -012
Event Description: Emergency Power System Unavailable
Date of Event: April 22, 1993
Plant: Quad Cities 2

Summary

During a surveillance test on April 22, 1993, the Quad Cities swing diesel generator cooling water pump (DGCWP) breaker locked-up on antipump protection. The licensee determined that the potential for lock-up existed since the initial plant startup if the pump power source was aligned to Unit 2. A 1992 modification ensured that the cooling water pump would be powered from Unit 2 if a loss-of-offsite power (LOOP) occurred on that unit. Unavailability of cooling water for 5 to 10 min is sufficient to damage the DG.

About one month earlier, inadequate bearing oil level had been found in the Unit 2 dedicated diesel cooling water pump, the result of an incorrectly reassembled oiler. The pump would have been expected to fail if it had been required to run for more than a short period of time. The Unit 2 emergency power system was vulnerable to failure for a 7-month period beginning in August 1992.

The conditional core damage probability estimated for the event is 6.0 E-005. This event CCPD was in the upper third of the CCPD span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The root cause for the 1/2 DGCWP not starting is a design deficiency [C61] in the Bus 28 breaker close logic that has existed since the plant was originally designed. This design deficiency would prevent the 112 DGCWP from auto-starting if it was running on Bus 28, received a Bus 28 undervoltage trip and subsequently power was restored to Bus 28.

The problem was introduced into the Bus 18 pump control logic during the installation of modification M04-1/2-83-014 in 1985. This modification added the 1/2 DGCWP Feed Power Selector Switch to address Appendix R concerns. However, the problem only exists for the Bus 18 feed if the selector switch is placed in the Bus 18 position. The Bus 18 position of the switch is not the normal lineup for the 1/2 DGCWP.
3. **Method of Discovery**

During a surveillance test [D15] on April 22, 1993, the Quad Cities swing diesel generator cooling water pump (DGCWP) breaker locked-up on antipump protection.

3.1 **Factors Contributing to Difficulty of Discovery**

(To determined by AEN/NEA)

3.2 **Safety Significance**

(To determined by AEN/NEA)

4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To determined by AEN/NEA)

4.3 **Licensee's Actions**

Designed and installed modifications to the undervoltage contacts in the trip logic and close circuit [A39]. Procedures were changed and drawing deficiencies were corrected. [A training session was held to assure mechanics understood assembly procedures for the DG cooling water pump.] [A46]
II. Events with CCDP in Upper Third of Its Span (Group II Events) (Cont.):

1. Event Summary

LER No.: 313/93-003
Event Description: Both Trains of Recirculation Inoperable for 14 h
Date of Event: September 30, 1993
Plant: Arkansas Nuclear One, Unit 1

Summary

On September 30, 1993, an engineering evaluation was completed at Arkansas Nuclear One, Unit 1, which indicated that the B decay heat removal/low-pressure injection (DHR/LPI) pump might have been incapable of performing its recirculation mode function following a loss-of-coolant accident (LOCA). This condition existed from May 24, 1993, while that plant was at power, until the plant shutdown on September 9, 1993. In addition, the A DHR/LPI pump was also inoperable for 14 h during this time period for routine maintenance and surveillance. The estimated conditional core damage probability for this event is 5.1E-005. This event CCDP was in the upper third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

In order to prevent thrust loading of the motor bearing, it is necessary to couple the motor to the pump with the motor in its magnetic center. Magnetic center is the position the motor would naturally seek if running uncoupled. The best way to determine magnetic center is to run the motor uncoupled. The plant procedure governing maintenance [CC1] of P-34B instructs the craft to "scribe the motor shaft to mark magnetic center" prior to disassembly. At this point, the pump and motor are still coupled, but not running, and there is no guarantee that the motor is actually at its magnetic center. The assembly portion of the procedure directs the craft to set the motor shaft to magnetic center before coupling. The procedure did not provide the necessary guidance for accurately determining the motor's magnetic center. Therefore, the root cause of this condition was inadequate procedural guidance [CC1].

3. Method of Discovery

On September 30, 1993, an engineering evaluation [of an operational problem] [D17] was completed at Arkansas Nuclear One, Unit 1, which indicated that the B decay heat removal/low-pressure injection (DHR/LPI) pump might have been
incapable of performing its recirculation mode function following a loss-of-coolant accident (LOCA).

3.1 Factors Contributing to Difficulty of Discovery
(To determined by AEN/NEA)

3.2 Safety Significance
(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions
(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues
(To determined by AEN/NEA)

4.3 Licensee’s Actions

The maintenance procedure [A43] was revised to incorporate guidance on how to correctly identify the motor magnetic center and couple the pump to the motor.
II. Events with CCDP in Upper Third of Its Span (Group II Events) (Cont.):

1. Event Summary

LER No.: 413/93-002, 414/93-002
Event Description: Essential Service Water Potentially Unavailable
Date of Event: February 25, 1993
Plant: Catawba 1 and 2

Summary

On February 25, 1993, with Catawba Unit 1 at 100% power and Catawba Unit 2 in a refueling shutdown, three of four essential service water (ESW) pump discharge valves failed to open during surveillance testing. Four ESW pumps serve both units. During normal operation, only one pump is used. If the pump with the operable valve tripped, it would result in the loss of ESW to both units. The conditional core damage probability estimated for this event is 1.5 E-004. This event CCDP was in the upper third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

Failure of the RN pump discharge valves to open has been attributed to a lack of detailed information in the motor operated valve (MOV) torque switch setup procedure, sizing variables that are possibly inadequate for these specific applications [CA1], [CA2] and/or a potentially degraded valve subcomponent [CB1].

3. Method of Discovery

On February 25, 1993, with Catawba Unit 1 at 100% power and Catawba Unit 2 in a refueling shutdown, three of four essential service water (ESW) pump discharge valves failed to open during surveillance testing [D15].

3.1 Factors Contributing to Difficulty of Discovery

3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

(Nothing identified)
4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To be determined by AEN/NEA)

4.3 **Licensee’s Actions**

The discharge butterfly valves which failed to open were adjusted to 20 degrees open and the torque switch was adjusted to provide maximum opening torque [A39]. Planned actions include continued analysis of test data obtained with use of diagnostic equipment and additional tests to identify causes of higher than expected loads [A34]*.
III. Events with CCDP in Middle Third of Its Span (Group III Events):

1. Event Summary

LER Number: 483/92-011
Event Description: Loss of Main Control Board Annunciators
Date of Event: October 17, 1992
Plant: Callaway

Summary

Callaway was at 100% power on October 17, 1992. At 0100 hours a replacement power supply for the annunciator system was being placed into service. Failure of this power supply had caused 198 main control board (MCB) annunciator windows to fail and caused 76 to light. During this replacement process, a short circuit caused logic power supply fuses to blow, lighting 371 of 683 MCB annunciator windows and thus causing the annunciator system to fail. Blown fuses in the four field contact power supplies were found and replaced about 1 h later. The operators assumed that this fuse replacement would return the annunciator system to normal operation, although anomalous behavior was still being observed. Actually, 164 annunciator windows remained inoperable. The remaining failed fuses were found and replaced, and the annunciator system was tested and confirmed operable at 1937 hours. The conditional core damage probability estimated for this event is $1.3 \times 10^{-5}$. This estimate may be conservative; the analysis was performed using screening human error probabilities (HEPs) and with limited information concerning the activities that were in progress at the time of the event. This event CCDP was in the middle third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The cause of the initial failure of the power supply was a short in the power transformer internal to the field power supply [CB1]. During restoration following replacement of this power supply, a short occurred while removing jumpers [CE2], causing the fuses to blow.

3. Method of Discovery

Callaway was at 100% power on October 17, 1992. At 0100 hours a replacement power supply for the annunciator system was being placed into service. Failure of this power supply had caused 198 main control board (MCB) annunciator windows to fail and caused 76 to light. During this replacement process, a short circuit caused logic power supply fuses to blow, lighting 371 of 683 MCB
annunciator windows and thus causing the annunciator system to fail. [D16]

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

- An NRC Augmented Team Inspection (AIT) was conducted on this event (see AIT Report 50-483/92-018 for details).[A16]

- NRC Information Notice 93-47, Unrecognized Loss of Control Room Announciators, issued. [A18]

- An NRC Enforcement Conference was conducted in November 1992. [A19]

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

- The NRC Augmented Inspection Team (AIT) identified the root causes of the event as: 1. Poor Communications/Teamwork, 2. Lack of questioning attitude/complacency, 3. Inadequate knowledge of annunciator system, and 4. Less than adequate work performance (see AIT Report 50-483/92-018 for details).

4.3 Licensee’s Actions

The Operations Department procedures were changed [A40] to include detailed actions to be taken in case of annunciator failures. A possible modification [A39] will be evaluated concerning improved RK system field power supply reliability, DC power redundancy, and power supply failure detection capability for operating crews. Power supply replacement practices were revised [A43] to include guidance for retesting RK system power supplies, requirements for direct field supervision, requirements for pre-job briefings, and requirements to document work completion.
III. Events with CCDP in Middle Third of Its Span (Group III Events) (Cont.):

1. Event Summary

LER Number: 261/92-013, 261/92-014, and 261/92-018  
Event Description: Safety Injection Pump Out of Service  
Date of Event: June 18, 1992, through August 22, 1992  
Plant: H. B. Robinson, Unit 2

Summary

Both safety injection (SI) pumps were out of service for 1.5 h on July 10, 1992, while H. B. Robinson was at 100% power. The "B" SI pump was rendered inoperable because plastic sheeting material obstructed the pump’s recirculation line. The plastic material was believed to have been used during a design modification during the refueling outage that ended on June 18, 1992. The "A" pump was out of service for 1.5 h on July 10, 1992, because of a blown control power fuse in the pump’s breaker closing circuit. On August 22, 1992, with the plant operating at 100% power, the plant experienced a total loss of offsite power (LOOP) (See LER 261/92-017). Following the LOOP, on August 24, 1992, the "B" SI pump recirculation line was again found to be obstructed with the plastic sheeting material from the outage modification.

The conditional core damage probability for the 1.5 h that both SI pumps were inoperable (LERs 261/92-013 and -014) is 6.2 x E-8. This is below the precursor cutoff value of E-6. Therefore, this event is not a precursor but is included here since this is when the extended inoperability of the "B" SI pump began. The conditional core damage probability for the time period when the "B" SI pump was inoperable (LERs 261/92-013 and -018) is 3.5 x E-5. This event CCDP was in the middle third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The cause of this event is attributed to personnel error. Event investigation identified the cause of the "B" Safety Injection pump's reduced recirculation flow to be foreign material blockage [CC5] within the associated minimum flow recirculation check valve and flow orifice. This foreign material was subsequently identified as a plastic sheet material fabricated for use as purge dam material for welding operations associated with a recent modification to the RHR minimum flow recirculation system.

3. Method of Discovery

On July 8, 1992, at 2307 hours, H. B. Robinson Unit No. 2 entered a 24 hour Limiting Condition for Operation (LCO) due to
inadequate recirculation flow [D18] for "B" Safety Injection Pump.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

- NRC Information Notice 92-85, Potential Failures of Emergency Core Cooling Systems Caused by Foreign Material Blockage, was issued. [A18]

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To be determined by AEN/NEA)

4.3 Licensee's Actions

The debris was removed via extensive system flushing [A44]. The safety injection system was then operated at design basis flow rates with no blockage occurring [A45]. Subsequent testing under minimum flow conditions did not cause blockage [A45].
III. Events with CCDP in Middle Third of Its Span (Group III, Events) (Cont.):

1. Event Summary

LER Number: 269/92-018, 270/92-018, 287/92-018
Event Description: Both Keowee Emergency Power Hydro Units Potentially Unavailable
Date of Event: December 2, 1992
Plant: Oconee 1, 2, and 3

Summary

With all three Oconee units at 100% power, both emergency power sources, Keowee Hydro Units 1 and 2 (Keowee 1 and 2), were determined to be inoperable. A modification to the antipump relays in the Westinghouse (type DB) breakers at Keowee did not consider the reduced control circuit dc voltage which would exist following a loss of offsite power (LOOP), when the battery chargers are not supplying the dc buses. During emergency start testing 6 d after completion of the modification (which simulated a LOOP) and in subsequent testing, certain Keowee breakers did not close when required. Both Keowee units were potentially unavailable for 15 d. The conditional core damage probability estimated for this event is 3.2 x E-5. This estimate is a bounding estimate that assumes all impacted breakers fail following an actual LOOP and may be conservative for the observed event. This event CCDP was in the middle third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

A design deficiency [CE1] in the anti-pump relay scheme on DB-50 breakers associated with Keowee Hydro (KH) Units 1 and 2 Supply and Field Breakers resulted in both KH Units being inoperable.

3. Method of Discovery

During emergency start testing [D15] 6 d after completion of the modification (which simulated a LOOP) and in subsequent testing [D15], certain Keowee breakers did not close when required. Both Keowee units were potentially unavailable for 15 d.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)
4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To be determined by AEN/NEA)

4.3 **Licensee's Actions**

Westinghouse DB type breakers at Keowee were modified [A39] to remain energized for a longer time to ensure the breaker will close when the DC system voltage is degraded.
III. Events with CCDP in Middle Third of Its Span (Group III Events) (Cont.):

1. **Event Summary**

LER Number: 301/92-003  
Event Description: Plugged Safety Injection Pump Suction  
Date of Event: September 18, 1992  
Plant: Point Beach 2

Summary

Point Beach 2 was at 100% power on September 18, 1992 while performing the A train containment spray (CS) pump quarterly test. When the pump failed to pass the test, it was disassembled. A foam rubber plug, which had been installed in the RHR system 10 months earlier, was found in the suction line of the CS pump. This plug rendered the A train SI and RHR pumps inoperable for the 10 months it was installed. The conditional probability of subsequent core damage estimated for this event is 9.9 x E-6. This event CCDP was in the middle third of the CCDP span for the postulated events.

2. **Failure Cause and Type (Based on Cause)**

The spray pump impeller suction was blocked by a foam rubber plug [CC5]. The origin of the plug could not be conclusively identified by the incident investigation team formed to investigate and recommend corrective actions following this event. However, the investigation team determined that the plug was most likely installed in a portion of the piping between the Unit 2 RHR Pump P-10A discharge and the Containment Spray Pump P-14A and Safety Injection Pump P-15A suction as a temporary cleanliness barrier during system modifications performed during the Unit 2 Fall 1991 refueling outage, and subsequently not removed. This modification installed test lines allowing full flow testing of the RHR pumps. We committed to install this modification in response to potential concerns with operating pumps at less than manufacturer’s recommended minimum flows identified in NRC Bulletin 88-04, "Potential Safety-Related Pump Loss."

3. **Method of Discovery**

Point Beach 2 was at 100% power on September 18, 1992 while performing the A train containment spray (CS) pump quarterly test [D15].

3.1 **Factors Contributing to Difficulty of Discovery**

(To be determined by AEN/NEA)
3.2 Safety Significance
(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions
(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues
(To be determined by AEN/NEA)

4.3 Licensee's Actions

Full flow tests [A45], subsequent to removal of a foam rubber plug [A44], demonstrated the containment spray pump was operable. Other tests verified operability of the RHR system and safety injection system. During a subsequent refueling outage, boroscopic examinations and radiography [A45] were conducted on potentially affected piping to determine whether foreign material was present. Management emphasized the importance of foreign material controls and cleanliness concerns to supervisors, engineers, QA personnel, and maintenance planners [A46].
III. Events with CCDP in Middle Third of Its Span (Group III Events) (Cont.):

1. Event Summary

LER Nos.: 213/93-006 and -007
AIT No.: 213/93-80,
Event Description: Degradation of Motor Control Pressurizer Power-Operated Relief Valve, and Emergency Diesel Generators
Date of Event: June 27, 1993
Plant: Haddam Neck

Summary

In part as a result of the Haddam Neck Individual Plant Examination (IPE), a decision was made by the licensee to perform an integrated test of the automatic bus transfer (ABT) scheme for motor control center (MCC) MCC-5. Such a test had never been performed, although some of the individual components had been tested. Several important systems are directly dependent on MCC-5 for their operation, including both trains of high- and low-pressure safety injection (HPSI and LPSI) and both normally closed pressurizer power-operated relief valve (PORV) block valves. On June 27, 1993, the first test of the ABT scheme for MCC-5 was unsuccessful. MCC-5 was without power until an operator took local action to close a breaker. On May 25, 1993, one of the pressurizer PORVs was found to have an air leak that would drain the air receiver if feed-and-bleed were initiated. Also on May 25, 1993, the licensee was performing a 24-h endurance run of the -A- emergency diesel generator (EDG). After 22 h the EDG exhibited abnormal kilowatt, kilovar, and ampere indications that led to the termination of the test. Components in the exciter control cabinet had failed due to overheating. The exciter control cabinet for the -B- EDG was also susceptible to this failure mode. The conditional core damage probability of this combined event is 6.5 E-005. This event CCDP was in the middle third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The root cause of this event was lack of adequate cooling [CE1] inside the excitation cabinet, resulting in the failure of the selenium rectifiers which initially led to an abnormal field voltage condition and ultimately a loss of generator field. The failure mechanism is postulated to be the result of the combination of excessive heat generated due to the high electrical loading of the machine along with dust accumulation and loss of forced ventilation in addition to the age of the devices. It is uncertain whether both rectifiers failed together or one failed and overstressed the other until it failed as well.
3. **Method of Discovery**

In part as a result of the Haddam Neck Individual Plant Examination (IPE) [], a decision was made by the licensee to perform an integrated test of the automatic bus transfer (ABT) scheme for motor control center (MCC) MCC-5. Such a test had never been performed, although some of the individual components had been tested. Several important systems are directly dependent on MCC-5 for their operation, including both trains of high- and low-pressure safety injection (HPSI and LPSI) and both normally closed pressurizer power-operated relief valve (PORV) block valves. On June 27, 1993, the first test [D15] of the ABT scheme for MCC-5 was unsuccessful.

3.1 **Factors Contributing to Difficulty of Discovery**

(To be determined by AEN/NEA)

3.2 **Safety Significance**

(To be determined by AEN/NEA)

4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

- An NRC Augmented Inspection Team (AIT) investigated the event (see inspection report 50-213/93-80 for details). [A16]

- NRC Information Notice, 93-81, Revision 1, Problems with C-Relays in DB- and DHP- Type Circuit Breakers Manufactured by Westinghouse, issued (see 1993 AEOD Annual Report, page 68). [A18]

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

- The NRC Augmented Inspection Team (AIT) noted two issues regarding licensing basis of MCC-5 (see inspection report 50-213/93-80 for details).

4.3 **Licensee's Actions**

Several design changes [A39] that reduce dependence of the specific MCC were implemented. This included using another MCC as the power source for one residual heat removal charging pump suction valve, the main lube oil pump for charging pump A, and one PORV block valve. One PORV power source was changed from a semi-vital panel to a vital panel.

C-28
IV. Events with CCDP in Lower Third of Its Span (Group IV Events):

1. Event Summary

LER No: 206/91-014
Event Description: Inoperable volume control tank level transmitters
Date of Event: August 7, 1991
Plant: San Onofre 1

Summary

The automatic actuation for re-alignment of the charging pumps from the volume control tank (VCT) to the refueling water storage tank (RWST) on low VCT level was disabled. In the event of a small-break loss-of-coolant accident (LOCA), and if manual realignment failed, the charging pumps would become gas bound due to hydrogen from the VCT. This condition existed for ~17 h. The conditional probability of core damage associated with this event is 2.1x E-6. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The problems exhibited by LT-1100 were caused by loose fasteners in the transmitter which allowed some internal parts to bind and others (which should be locked together) to rotate [CB1]. An investigation has been initiated to determine why the level transmitter fasteners were loose. [This investigation revealed the vibration caused by welding and grinding done in the area caused the fasteners becoming loose.]

3. Method of Discovery

Operators observed differences in the indicated VCT level between the two level channels (LT-2550 and LT-1100) and erratic level indication by LT-1100. Due to the erratic behavior of LT-1100, a temporary design change was requested to switch the automatic VCT level control function from LT-1100 to LT-2550. During a feasibility review [D17] of the change request, it was recognized that operation with blocked charging pump protection on low VCT level was contrary to the TSs.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)
4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To be determined by AEN/NEA)

4.3 **Licensee’s Actions**

LT-1100 has been repaired, calibrated, and returned to service [A41]. Procedures were revised to preclude simultaneous disabling both trains of charging pump low volume control tank level protection [A40]. A proposed Technical Specification (TS) change [A47] providing a 72 hour allowable out of service time was submitted. Improved operator guidance [A46]* which will correlate ECCS components to the associated LCOs and action statements is planned.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER No.: 445/91-012  
Event Description: Potential charging pump unavailability due to hydrogen void expansion  
Date of Event: March 26, 1991  
Plant: Comanche Peak 1

Summary

Two hydrogen gas voids were identified in chemical and volume control system (CVCS) piping. One of the voids, in the boric acid tank (BAT) gravity feed line, was large enough to impact charging pump operation following use of the line or during safety injection (SI) when lower charging pump suction header pressures could result in expansion of the hydrogen void into the suction line. The conditional core damage probability estimated for this event is 6.2 x E-5. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

Evaluation of this event has identified the potential root cause to be hydrogen coming out of solution in the lower pressure CCP suction header and collecting in the vertical piping [CA2].

3. Method of Discovery

On October 29, 1990, Westinghouse sent a letter [D09] to CPSES regarding the formation and venting of hydrogen in the Chemical and Volume Control System (CVCS) (EIIS:(CB)) in response to Nuclear Regulatory Commission (NRC) Information Notice (IN) 90-64, "Potential for Common-Mode Failure of High Pressure Safety Injection Pumps or Release of Reactor Coolant Outside Containment During a Loss-of-Coolant Accident." [D08] In this letter Westinghouse, identified locations in the CVCS suction piping where gases would tend to accumulate. Westinghouse recommended ultrasonic examination to monitor the rate at which gas accumulates in these locations.

Ultrasonic examination of the Chemical and Volume Control System (CVCS) suction piping was performed on March 4, through March 15, 1991. These examinations revealed voids in the alternate boration line and the gravity teed line from the Boric Acid Storage Tank (BAT).
3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To be determined by AEN/NEA)

4.3 Licensee’s Actions

The gravity feedline from the boric acid tank was immediately vented. The feedline will be monitored for hydrogen accumulation and based on the data, venting requirements will be established [A40]°.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER No: 272/91-030
Event Description: Both PORVs failed due to leaking actuators
Date of Event: September 20, 1991
Plant: Salem 1

Summary

The power-operated relief valves (PORVs) at Salem 1 were inoperable because of leakage from the flange bolting area on the air-operated PORV actuators. It is assumed that both PORVs were inoperable for one half of their surveillance period (81 d).

The conditional probability of core damage estimated for this event is $4.4 \times 10^{-6}$. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

Investigation of this event's root cause is continuing. The initiating cause of both PORV valves failing to open is equipment failure [CB1]*.

3. Method of Discovery

On 9/20/91, a plant shutdown was in progress. The Pressurizer Pressure Operated Relief Valves (PORVs) are used to provide over pressure protection at low Reactor Coolant System temperatures. In accordance with Surveillance 4.4.9.3.1.1 the PORVs were functionally checked [D15]. Both valves failed to open.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)
4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To be determined by AEN/NEA)

4.3 Licensee's Actions

The diaphragm in each Copes-Vulcan actuator associated with the Unit 1 pressurizer was replaced [A41]. The diaphragm manufacturer was asked to certify a diaphragm material for elevated temperature service. It was determined that the actuator bolt pattern had been changed by the manufacturer and licensee staff is assessing whether current actuators need to be replaced [A39]*.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER No: 281/91-017
Event Description: Both emergency diesel generators for Unit 2 inoperable for 13 h
Date of Event: July 15, 1991
Plant: Surry 2

Summary

Both emergency diesel generators (EDGs) were inadvertently out of service at Surry 2 for 13 h. EDG 3, the dual-unit swing diesel, had been unavailable since May 7, 1991, because of inadequate post-maintenance testing. EDG 2 was removed from service for 13 h on July 15, 1991.

The conditional probability of core damage estimated for this event is 2.9 x E-6. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The reason for the EDG #3 not reaching its required speed and frequency range was attributed to a cognitive error [CE2] on the part of utility personnel in that an approved work order step which specified a fast start test of BW #3 was not performed. A contributing cause was that the post-maintenance testing follower associated with the work package did not specify an EDG fast start test be performed [CC1].

3. Method of Discovery

On August 9, 1991, with Unit 1 and Unit 2 at 100% power, it was determined that Emergency Diesel Generator (EDG) #3 had been inoperable since May 9, 1991. This determination was made while performing a root cause evaluation [D17] of the observed performance of EDG #3 during an August 2, 1991, Engineered Safeguards Feature (ESF) actuation on Unit 2.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)
4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To be determined by AEN/NEA)

4.3 Licensee’s Actions

EDG #3 was declared inoperable. The governor was adjusted [A41] and two consecutive fast starts [A45] were satisfactory. The governors for EDGs #1 AND 2 were adjusted [A41] and two fast starts [A45] for each EDG confirmed speed and frequency were within specification.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER Number: 328/92-010
Event Description: Emergency Diesel Generator and Residual Heat Removal Pump Inoperable
Date of Event: July 17, 1992
Plant: Sequoyah Nuclear Plant, Unit 2

Summary

During performance of a surveillance procedure on the 2B-B Residual Heat Removal (RHR) pump, it was found that the miniflow control valve continuously cycled open and closed when it should have remained opened. While the 2B-B RHR pump was inoperable, the 2A-A emergency diesel generator (EDG) was inoperable for 17 h and the 2A-A centrifugal charging pump was inoperable for 6 h. The conditional core damage probability estimated for this event is 1.9 x 10^-6. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

An investigation determined the problem to be an incorrectly terminated wire on the flow switch [CE2]. The wire was correctly terminated and the flow switch was functionally tested and returned to service. LCOs 3.5.2 and 3.6.2.1 were exited at 2249 EDT on July 17, 1992. A subsequent investigation into the event identified the root cause of the mislaid wire as being inattention to detail with an inadequate second-party verification. Maintenance personnel have been briefed on specific problems identified in this event. A less than adequate post maintenance test (PMT) also contributed to the event [CC1]. On July 28, 1992, during the review [D17] of the event by the Plant Event Review Panel (PERP), it was discovered that a potential issue existed involving the RHR systems being outside of design basis of the plant.

3. Method of Discovery

During performance of a surveillance procedure [D15] on the 2B-B Residual Heat Removal (RHR) pump, it was found that the miniflow control valve continuously cycled open and closed when it should have remained opened. See section 2. above for additional discovery method: [D17]

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

C-37
3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To be determined by AEN/NEA)

4.3 Licensee's Actions

The instrument preventive maintenance data packages for the RHR miniflow switches were revised [A43] to require independent verification for wire connections and jumpers. Maintenance craftsmen, planners, and procedure writers were briefed [A46] on the need to conduct an adequate post maintenance test or specify independent verification in lieu of such test.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER Number: 269/92-008, 9/92-008, 9/92-008
Event Description: Both Keowee Emergency Power Hydro Units Unavailable
Date of Event: July 16, 1992
Plant: Oconee 1, 2, and 3

Summary

With all three Oconee units at 100% power and emergency power source Keowee 1 unavailable because of maintenance, a failed fuse was discovered in the control power circuit for an auxiliary power breaker on Keowee 2. This rendered Keowee 2 also unavailable. Both emergency power sources were unavailable for 34 h. The conditional core damage probability estimated for this event is 2.8 x E-6. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The root cause of Keowee Unit 2's inoperability is Equipment failure [CB1]. With the failure of the "1B" positive 10 amp (OT10) fuse feeding ACB-8, one source of power available to the 2X Switchgear was lost, thus, rendering the CX Transformer and Keowee Unit 2 technically inoperable. It is not known exactly when the fuse blew, but it is assumed that on June 7, 1992, at approximately 1400 hours, the "1B" positive close fuse failed during the closure test performed on ACB-8 and the failure went unobserved until approximately 1200 hours on July 16, 1992.

3. Method of Discovery

On July 17, 1992, at 1330 hours, all three Oconee units were at 100 percent Full Power. With Keowee Unit 1 out of service for planned maintenance, it was discovered [as a result of an investigation [D17] for the cause of dim green and red indicating lights for the breaker position observed during an inspection of plant equipment] that the closing circuit fuse in ACB-8 breaker was blown causing an inoperability of Keowee Unit 2. With these conditions both onsite emergency power sources were technically inoperable.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)
3.2 Safety Significance
(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions
(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues
(To be determined by AEN/NEA)

4.3 Licensee’s Actions
The Keowee Breaker Status checklist was revised [A40] to include additional breaker and indicator status for each breaker. The checklist also contains directions on what to look for and who to call for guidance on other than normal conditions. Planned actions include developing a rounds and turnover procedure [A40]* to enhance monitoring Keowee Hydro equipment. Keowee personnel will receive training [A46] about the procedures, checklist, and Technical Specification time limit requirements.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER Number: 286/92-011
Event Description: Multiple EDGs Inoperable
Date of Event: July 6, 1992
Plant: Indian Point 3

Summary

During surveillance testing of 480-V engineered safety feature (ESF) bus 5A, it was discovered that a wire was not connected correctly in the relay circuits required to auto-start emergency diesel generator (EDG) 33. During the time that EDG 33 was not available to perform its safety function, the other two EDGs were inoperable at various times. Two EDGs were simultaneously unavailable for a total of 3.5 d, reducing onsite ac power supplies below the minimum assumed in the Final Safety Analysis Report (FSAR). Even though this event occurred while the unit was shut down, other similar modifications and tests have been conducted while Indian Point was at power (e.g., see LER 286/90-005, p. B-184, Vol. 14 of NUREG/CR-4674) that have resulted in more than one EDG being inoperable at the same time. Therefore, with no written policy indicating otherwise, it is credible that an EDG could be discovered inoperable during power operations coincident with the removal of another EDG from service for maintenance testing, or modifications. Consistent with the ASP methodology, this event was therefore modeled as if it occurred at power. The conditional core damage probability estimated for this event is $1.2 \times 10^{-6}$. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The most probable cause of the event was the electrical connection at a compression-type termination becoming loose due to thermal changes and vibration [CA2]. A possible contributing cause was the wire being inadvertently jarred by contractor electricians working in the area [CE2].

3. Method of Discovery

During surveillance testing [D15] of 480-V engineered safety feature (ESF) bus 5A, it was discovered that a wire was not connected correctly in the relay circuits required to auto-start emergency diesel generator (EDG) 33. During the time that EDG 33 was not available to perform its safety function, the other two EDGs were inoperable at various times. Two EDGs were simultaneously unavailable for a total of 3.5 d, reducing onsite power supplies below the minimum assumed in the Final Safety Analysis Report (FSAR). Even though this event occurred while the unit was shut down, other similar modifications and tests have been conducted while Indian Point was at power (e.g., see LER 286/90-005, p. B-184, Vol. 14 of NUREG/CR-4674) that have resulted in more than one EDG being inoperable at the same time. Therefore, with no written policy indicating otherwise, it is credible that an EDG could be discovered inoperable during power operations coincident with the removal of another EDG from service for maintenance testing, or modifications. Consistent with the ASP methodology, this event was therefore modeled as if it occurred at power. The conditional core damage probability estimated for this event is $1.2 \times 10^{-6}$. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The most probable cause of the event was the electrical connection at a compression-type termination becoming loose due to thermal changes and vibration [CA2]. A possible contributing cause was the wire being inadvertently jarred by contractor electricians working in the area [CE2].

3. Method of Discovery

During surveillance testing [D15] of 480-V engineered safety feature (ESF) bus 5A, it was discovered that a wire was not connected correctly in the relay circuits required to auto-start emergency diesel generator (EDG) 33. During the time that EDG 33 was not available to perform its safety function, the other two EDGs were inoperable at various times. Two EDGs were simultaneously unavailable for a total of 3.5 d, reducing onsite power supplies below the minimum assumed in the Final Safety Analysis Report (FSAR). Even though this event occurred while the unit was shut down, other similar modifications and tests have been conducted while Indian Point was at power (e.g., see LER 286/90-005, p. B-184, Vol. 14 of NUREG/CR-4674) that have resulted in more than one EDG being inoperable at the same time. Therefore, with no written policy indicating otherwise, it is credible that an EDG could be discovered inoperable during power operations coincident with the removal of another EDG from service for maintenance testing, or modifications. Consistent with the ASP methodology, this event was therefore modeled as if it occurred at power. The conditional core damage probability estimated for this event is $1.2 \times 10^{-6}$. This event CCDP was in the lower third of the CCDP span for the postulated events.
ac power supplies below the minimum assumed in the Final Safety Analysis Report (FSAR).

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

(None identified)

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

(To be determined by AEN/NEA)

4.3 Licensee’s Actions

Direction and guidance [A46]* [currently scheduled to be implemented during the 1997 refueling outage] for periodically checking the tightness of compression-type, clamp-down termination fittings will be developed. An administrative procedure [A48] was developed to control vendor activities at the site. The directive [A48] controlling preparation of work packages was revised to assure that all work packages prepared for contractor craftsmen use will include a precaution and limitation statement. This will alert craftsmen to review the work area before starting work, use caution around safety-related equipment, and report unintentional interactions with adjacent equipment to their supervisor.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER No.: 289/93-002
Event Description: Both Residual Heat Removal Heat Exchangers Unavailable
Date of Event: January 29, 1993
Plant: Three Mile Island 1

Summary

Three Mile Island 1 (TMI-1) was operating at 100% power on January 29, 1993, when an operator aligned river water system valves to bypass both decay heat service (DHS) coolers. The coolers remained unavailable for about 3 h. With the DHS coolers unavailable, it would not have been possible to remove heat from several safety-related systems had they been demanded. The conditional core damage probability estimated for this event is 3.1 E-006. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The root cause of this event was personnel error [CE3]. The AO bypassed both coolers at the same time in violation of established operator work practices. The AO failed to operate the equipment in accordance with Administrative Procedure (AP) 1029, "Conduct of Operations," which would have required authorization from the Shift Supervisor, Shift Foreman, or CRO prior to manipulating the valves. Additionally, operation of both trains of ESAS components was in violation of operator work practices. Further evaluation will determine to what extent communications, work preparation, and work control by the shift personnel contributed to this event.

To a lesser extent, clarity of the procedural guidance also contributed [CE4]. The instructions in OPS-S227 did not provide guidance for determining if a thermal transient would occur, did not specify that only one cooler at a time should be bypassed and that bypassing a cooler rendered the train out of service and started a TS time clock. However, the instructions in OPS-S227 that contributed to this event could have been eliminated entirely since they are not applicable to an operating station. If the guidance had been contained in the appropriate Operating Procedure, exposure to the biennial review process could have resulted in either enhanced presentation to clarify the use of this option or removed it entirely.
3. **Method of Discovery**

During the performance of OPS-S227 on January 29, 1993, the non-licensed Auxiliary Operator (AO) failed to follow established operator work practices and bypassed both DC-C-2A and DC-C-2B simultaneously at about 0100 hours. The DR System was not required to be in operation, so neither DR Pump was operating.

Control Room personnel were unaware that both coolers were bypassed until about 0330 hours when a licensed Control Room Operator (CRO) discovered this condition while attempting to determine the status of preparations for performing OPS-S227 [D19].

3.1 **Factors Contributing to Difficulty of Discovery**

(To be determined by AEN/NEA)

3.2 **Safety Significance**

(To be determined by AEN/NEA)

4. **Corrective and Preventive Actions**

4.1 **Regulatory Actions**

(None identified)

4.2 **Insights from Licensee and Regulatory Efforts to Resolve Safety Issues**

(To be determined by AEN/NEA)

4.3 **Licensee's Actions**

Operations surveillance procedures will be revised [A40]* to ensure that detailed procedural guidance for evolutions that can potentially affect safe plant operation are placed in approved Operating Procedures. Each operating crew will review [A46]* the event to ensure they understand the errors that were committed and how similar errors can be avoided. A comprehensive human performance review will include assessing the role of supervision, communications, and improvements in work practices and controls.

C-44
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER No.: 412/93-012
Event Description: Failure of Both Emergency Diesel Generator Load Sequencers
Date of Event: November 4-6, 1993
Plant: Beaver Valley 2

Summary

On November 4, 1993, the automatic loading capability of the 2-1 emergency diesel generator (EDG) on a safety injection (SI) signal failed during a test. Two days later, on November 6, 1993, the automatic loading capability of the 2-2 EDG on an SI signal also failed during a test. This failure would only occur when an SI signal was present coincident with a loss of the normal power supply to the engineered safety features (ESF) bus. The failure mechanism had existed since November 1990. Operator actions would have been necessary to allow manual loading of equipment on the ESF buses. The conditional core damage probability estimated for this event is 2.1 E-006. This event CCDP was in the lower third of the CCDP span for the postulated events.

2. Failure Cause and Type (Based on Cause)

The cause of the test failures was the misoperation of a digital (microprocessor based) solid state timer associated with the Load Sequencer circuitry. An inductive voltage surge [CE1] was produced by the de-energization of auxiliary relays within the Load Sequencer circuit during the SIS reset of sequencer operation. This caused the timer to misoperate resulting in the failure of the sequencer [CB1].

3. Method of Discovery

On November 4, 1993, the automatic loading capability of the 2-1 emergency diesel generator (EDG) on a safety injection (SI) signal failed during a test [D15]. Two days later, on November 6, 1993, the automatic loading capability of the 2-2 EDG on an SI signal also failed during a test [D15].

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)
3.2 Safety Significance

(To be determined by AEN/NEA)

4. Corrective and Preventive Actions

4.1 Regulatory Actions

- An NRC Augmented Team Inspection was conducted on this event (see AIT Report 50-412/93-81 for details). [A16]

- NRC Information Notice 94-20, Common-Cause Failure Due to Inadequate Design Control and Dedication, was issued. [A118]

- NRC Enforcement Actions, including Notice of Violation and Civil Penalty, were taken. [A19]

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

- The NRC Augmented Inspection Team (AIT) identified the root causes of the event as inadequate design control (see AIT Report 50-412/93-81 for details).

4.3 Licensee’s Actions

Voltage suppression diodes were added [A39] to the auxiliary relays for protection from voltage surges. The motor driven auxiliary feedwater pump was modified [A39] to ensure correct operation during emergency DG sequencer operation. Engineering requirements guidelines [A49] [this action still remain open] will be developed for the use of digital solid state components as replacements for electro-mechanical or non-solid state components.
IV. Events with CCDP in Lower Third of Its Span (Group IV Events) (Cont.):

1. Event Summary

LER Nos.: 498/93-005 and -007
Event Description: Unavailability of One Emergency Diesel Generator and the Turbine-Driven Auxiliary Feedwater Pump
Date of Event: December 29, 1992, through January 22, 1993
Plant: South Texas Project, Unit 1

Summary

For a period of ~ 25 d, South Texas Project (STP) Unit 1 operated with one emergency diesel generator (EDG) and the turbine-driven auxiliary feedwater (TDAFW) pump inoperable. The EDG was rendered inoperable because of binding of the fuel metering rods. The TDAFW pump was inoperable because of water intrusion into the turbine, which would have prevented the automatic start of the TDAFW pump. During this same period, a second EDG was removed from service for maintenance for a period of 61 h. The conditional core damage probability for this event is 1.2 E-005.

2. Failure Cause and Type (Based on Cause)

The primary cause of this event was the lack of proper work process control [CC1]. Contributing causes were inadequate implementation of lessons learned from industry operating experience [CC1] and inadequate verbal communications [CE5] which led to a lack of clearly defined responsibility for ensuring paint was not applied inappropriately.

3. Method of Discovery

On January 20, 1993, Unit 1 was in Mode 1 at 95% power. Standby Diesel Generator 13 failed to start during a monthly surveillance [D15], due to paint which had been applied to the fuel injection pumps. The paint ran into the fuel metering rod ports and caused binding of the fuel metering rods.

3.1 Factors Contributing to Difficulty of Discovery

(To be determined by AEN/NEA)

3.2 Safety Significance

(To be determined by AEN/NEA)
4. Corrective and Preventive Actions
4.1 Regulatory Actions

- An NRC Augmented Inspection Team (AIT) investigated the TDAFW pump event (see combined inspection report 50-498/93-07 and 50-498/93-07 for details). [A16]

- NRC Information Notice 93-51, Repetitive Overspeed Tripping of Turbine-Driven Auxiliary Feed Water Pumps, was issued. [A18]

4.2 Insights from Licensee and Regulatory Efforts to Resolve Safety Issues

- The NRC Augmented Inspection Team (AIT) identified weaknesses in the licensee's maintenance program and corrective action process (see combined inspection report 50-498/93-07 and 50-498/93-07 for details).

4.3 Licensee's Actions

The fuel metering rods were cleaned and lubricated [A41]. Efforts that have been or will be taken include revising work process control documents to include specific guidance on painting activities and pre-job briefings [A43]*, enhancing the Operating Experience Review program [A46]*, performing a case study of the event for training purposes [A46]*, and including the event in the Licensed Operators Requalification Program [A46]*.
INSIGHTS ON LICENSEE’S CORRECTIVE ACTIONS RELATED TO UNDETECTED FAILURES OF SAFETY SYSTEMS
1. **GENERAL BACKGROUND ON THE ENGINEERING EVALUATION**

Undetected failures of safety systems in nuclear power plants are of great safety concern, especially when the failures remained undetected for a long time. A set of 33 such events were identified by a search of the Accident Sequencer Precursor (ASP) database for selected period, 1991 through 1993. The failures were analyzed and evaluated with respect to their discovery methods, failure rate and trend, failure causes, corrective and preventive actions by the licensees, and regulatory actions. The purpose of the evaluation was to gain insights from such failures which could be useful in preventing or reducing the likelihood of such failures.

2. **SUMMARY OF EVALUATION FINDINGS**

The failures were more often discovered either by testing or analysis and evaluation of operational problems than other means. The failures were more often caused by component failure, design deficiency, and inadequate testing or maintenance procedures. The predominant corrective or preventive actions the licensees took were design change (plant modification), new or change in operating procedure, additional training or guidance to plant personnel, and change to maintenance procedure. Although the licensees' actions appear to be effective in correcting the individual failures discovered at each plant, their effectiveness in preventing or minimizing similar events in other plants appears to be doubtful, as substantial number of failures continues to occur.

3. **SPECIFIC FINDINGS RELATED TO LICENSEE’S CORRECTIVE AND PREVENTIVE ACTIONS**

Table 1 lists the actions for each event by their code, and Table 2 shows their distribution. For the 33 events, more frequent corrective or preventive actions the licensees took were: design change or plant modification (16 events), new or change in operating procedure (11 events), additional training or guidance to plant personnel (8 events), and change to maintenance procedure (6 events). Other corrective or preventive actions the licensees took were: corrective maintenance, repair or replace failed component (4 events), change to design basis (3 events), post-maintenance verification testing or examination (3 events), assessment of modifications' implementation and subsequent requalification (2 events), removal of foreign material by flushing (2 events), new or change in administrative procedure or management directives (2 events), new or change to Technical Specifications (1 event), and new or change in engineering or design procedure (1 event).

4. **SPECIFIC CONCLUSIONS RELATED TO LICENSEE’S CORRECTIVE AND PREVENTIVE ACTIONS**

The licensees’ analyses of events indicated that the failures were more frequently caused by component failure, design deficiency, and inadequate testing or maintenance procedures. All of these deficiencies could be reduced by appropriate corrective or preventive actions. The more frequent corrective or preventive actions the licensees took were design change (plant modification), new or change in operating procedure, additional training or guidance to plant
personnel, and change to maintenance procedure. Although the licensees' actions appeared to correlate to the failure causes and correcting the failures discovered, their effectiveness in preventing or minimizing similar events in other plants appears to be doubtful, as a substantial number of failures continued to occur.
TABLE 1
Categorization of Events

Note: This categorization is by codes in Appendix E for Failure Cause; Discovery Method, and Licensee’s Corrective/Preventive Actions, and Regulatory Actions.

<table>
<thead>
<tr>
<th>LER#/Descr.</th>
<th>Failure</th>
<th>Discovery</th>
<th>Corrective/Preventive Actions</th>
<th>Regulatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plant Name</td>
<td>Cause</td>
<td>Method</td>
<td>Licensee’s</td>
<td>Regulatory</td>
</tr>
</tbody>
</table>

1. 1991 Events:

206/91-014: Inoperable volume control tank level transmitters
San Onofre 1 [CB1], [D17] [A40],[A41],

269/91-010, 270/91-010, 287/91-010: Potential for hydrogen entrainment in HPI pumps
Oconee 1,2,3 [CA1] [D17] [A40],[A42]* [A46]*,[A47]

272/91-030: Both PORVs failed due to leaking actuators
Salem 1 [CB1]* [D15] [A39]*,[A41]

278/91-017: Control wiring for ADS/relief valves found damaged
Peach Bottom 3[CC1] [D16] [A46],[A48]

281/91-017: Both emergency diesel generators for Unit 2 inoperable for 13 h
Surry 2 [CE2],[CC1] [D17] [A41],[A45]

336/91-009: Both diesel generators unavailable and unit shutdown
Millstone 2 [CB1],[CC1] [D15] [A43]*,[A39]*,

* Some corrective actions identified by licensees were incomplete when the original LER was written and a status update via an LER revision was not submitted. These actions are identified by an asterisk (*). The status of these actions was confirmed with the licensees as complete, except as specifically noted otherwise.
<table>
<thead>
<tr>
<th>LER#/Descr.</th>
<th>Failure Description</th>
<th>Discovery Method</th>
<th>Licensee's Action</th>
<th>Regulatory Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plant Name</td>
<td>Cause</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harris 1</td>
<td>HPI unavailability for one refueling cycle because of inoperable miniflow lines</td>
<td>[D15]</td>
<td>[A39]</td>
<td>[A18]</td>
</tr>
<tr>
<td>Millstone 3</td>
<td>Both trains of HPSI inoperable due to relief valve failures</td>
<td>[D15]</td>
<td>[A39]</td>
<td></td>
</tr>
<tr>
<td>Perry 1</td>
<td>Two EDGs inoperable</td>
<td>[D15]</td>
<td>[A43],[A39]</td>
<td></td>
</tr>
<tr>
<td>Comanche Peak 1</td>
<td>Potential charging pump unavailability due to hydrogen void expansion</td>
<td>[D08],[D09]</td>
<td>[A40]*</td>
<td></td>
</tr>
</tbody>
</table>

*Some corrective actions identified by licensees were incomplete when the original LER was written and a status update via an LER revision was not submitted. These actions are identified by an asterisk (*). The status of these actions was confirmed with the licensees as complete, except as specifically noted otherwise.
LER#/Descr. Failure       Discovery       Corrective/ Preventive Actions
Plant Name Cause          Method         Licensee's Regulatory

2. **1992 Events:**

261/92-013: Safety Injection Pump Out of Service
Robinson 2 [CC5]          [D18]*         [A44]*,[A45]         [A18]

269/92-008, 270/92-008, 287/92-008: Both Keowee Emergency Power Hydro Units Unavailable
Oconee 1,2,3 [CB1]          [D17]         [A40]*,[A46]         

269/92-018, 270/92-018, 287/92-018: Both Keowee Emergency Power Hydro Units Potentially Unavailable
Oconee 1,2,3 [CE1]          [D15]         [A39]         

286/92-011: Multiple EDGs Inoperable
Indian Point 3[CA2],[CE2]     [D15]         [A40],[A46]*, [A48]         

301/92-003: Plugged Safety Injection Pump Suction
Point Beach 2 [CC5]          [D15]         [A44],[A45], [A46]         

328/92-010: Emergency Diesel Generator and Residual Heat Removal Pump Inoperable
Sequoyah 2 [CE2],[CC1]      [D15],[D17]     [A43],[A46]         

483/92-011: Loss of Main Control Board Annunciators
Callaway   [CB1],[CE2]       [D16]         [A39]*,[A40], [A16],[A18] [A443]

* Some corrective actions identified by licensees were incomplete when the original LER was written and a status update via an LER revision was not submitted. These actions are identified by an asterisk (*). The status of these actions was confirmed with the licensees as complete, except as specifically noted otherwise.

1-3
### 1993 Events:

<table>
<thead>
<tr>
<th>LER#/Descr.</th>
<th>Failure</th>
<th>Discovery</th>
<th>Corrective/ Preventive Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Plant Name</td>
<td>Failure</td>
<td>Licensee's Regulatory</td>
</tr>
<tr>
<td></td>
<td>Cause</td>
<td>Method</td>
<td></td>
</tr>
<tr>
<td>3. 1993</td>
<td>213/93-006 and -007: Degradation of Motor</td>
<td>[D05],[D15]</td>
<td>[A16],[A18]</td>
</tr>
<tr>
<td></td>
<td>Control Pressurizer Power-Operated Relief</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valve, and Emergency Diesel Generators</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Haddam Neck [CE1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>265/93-010 and -012: Emergency Power System</td>
<td>[D15]</td>
<td>[A39]</td>
</tr>
<tr>
<td></td>
<td>Unavailable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quad Cities 2 [CE1]</td>
<td></td>
<td>[A39]</td>
</tr>
<tr>
<td></td>
<td>289/93-002: Both Residual Heat Removal Heat</td>
<td>[D19],</td>
<td>[A40]<em>,[A46]</em></td>
</tr>
<tr>
<td></td>
<td>Exchangers Unavailable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TMI-1 [CB3],[CE4]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>313/93-003: Both Trains of Recirculation</td>
<td>[D17]</td>
<td>[A43]</td>
</tr>
<tr>
<td></td>
<td>Inoperable for 14 h</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arkansas 1 [CC1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>412/93-012: Failure of Both Emergency</td>
<td>[D15],</td>
<td>[A16],[A18]</td>
</tr>
<tr>
<td></td>
<td>Diesel Generator Load Sequencers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Beaver Valley 2[CB1],[CE1]</td>
<td></td>
<td>[A39],[A49]*</td>
</tr>
<tr>
<td></td>
<td>413/93-002, 414/93-002: Essential Service</td>
<td>[D15]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Water Potentially Unavailable</td>
<td></td>
<td>[A34]*,[A39]</td>
</tr>
<tr>
<td></td>
<td>Catawba 1,2 [CA1],[CA2], [CB1]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>498/93-005 and -007: Unavailability of One</td>
<td>[D15],</td>
<td>[A16],[A18]</td>
</tr>
<tr>
<td></td>
<td>Emergency Diesel Generator and the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Turbine-Driven Auxiliary Feedwater Pump</td>
<td>[A41],[A43]*,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STP-1 [CC1],[CC2], [CE5]</td>
<td></td>
<td>[A46]*</td>
</tr>
</tbody>
</table>

* Some corrective actions identified by licensees were incomplete when the original LER was written and a status update via an LER revision was not submitted. These actions are identified by an asterisk (*). The status of these actions was confirmed with the licensees as complete, except as specifically noted otherwise.
TABLE 2
Distribution of Event Categories

Note: The number of events which fall under each code, as categorized in the evaluation report, is counted and their distribution, ranked in the order of decreasing frequency, is given below:

Licensee's Corrective/ Preventive Actions Categories:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A39]</td>
<td>Design change/ plant modification:</td>
<td>16</td>
</tr>
<tr>
<td>[A40]</td>
<td>New or change in operating procedure:</td>
<td>11</td>
</tr>
<tr>
<td>[A46]</td>
<td>Additional training/ guidance to plant personnel:</td>
<td>8</td>
</tr>
<tr>
<td>[A43]</td>
<td>Change to maintenance procedure:</td>
<td>6</td>
</tr>
<tr>
<td>[A41]</td>
<td>Corrective maintenance, repair/ replace failed component:</td>
<td>4</td>
</tr>
<tr>
<td>[A42]</td>
<td>Change to Design Basis:</td>
<td>3</td>
</tr>
<tr>
<td>[A45]</td>
<td>Post-maintenance verification testing/ examination:</td>
<td>3</td>
</tr>
<tr>
<td>[A34]</td>
<td>Assessment of modifications’ implementation and subsequent requalification:</td>
<td>2</td>
</tr>
<tr>
<td>[A44]</td>
<td>Removal of foreign material by flushing:</td>
<td>2</td>
</tr>
<tr>
<td>[A48]</td>
<td>New or change in Administrative Procedure/ Management Directives:</td>
<td>2</td>
</tr>
<tr>
<td>[A47]</td>
<td>New or change to Technical Specifications:</td>
<td>1</td>
</tr>
<tr>
<td>[A49]</td>
<td>New or change in Engineering/ Design procedure:</td>
<td>1</td>
</tr>
</tbody>
</table>