For Official Use **NEA/CSNI/R(2001)12**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

20-Jul-2001

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

REQUALIFICATION PROBLEMS OF SAFETY RELATED EQUIPMENTS FOLLOWING OUTAGES

PWG1

JT00111063

NEA/CSNI/R(2001)12
For Official Use

English - Or. English

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), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). 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 27 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

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

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 co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

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

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

OECD

PWG-1

Requalification Problems of Safety Related Equipments Following Outages

TABLE OF CONTENTS

Introduction

The Principal Working Group 1 (PWG 1) of the Committee on the Safety of Nuclear Installations (CSNI) agreed on its annual meeting September 1996 to initiate a generic study on requalification problems following outages. This generic study has been conducted by a task group led by France with participation of Belgium, Finland, Germany, Hungary, United Kingdom, Sweden and the United States of America. The French representative co-ordinated the work, collected the contributions from the participating countries and completed the report in close co-operation with the other representatives.

The main objective of the study is to gain insights and findings resulting from the lessons learned by the participating countries concerning the requalification process through their operational experiences in order to draw conclusions on requalification practices that may be useful for member countries.

In this study, the requalification or post-maintenance testing (operability verification) is defined as (following a description of Electricité de France - EdF, the french licensee) : “The requalification consists of a verification of the function of an equipment or system to guarantee that the performance required by design is maintained or restored after an intervention due to maintenance, due to modifications, or due to an operational occurrence”.

The requalification is a part of the general safety precautions of nuclear power plants. The aims of safety precautions in NPP operation are not only to maintain the designed safety level (as laid down in the Safety Analysis Report) but also to improve the safety by integrating lessons learned from operating experience feedback. In terms of the defence-in-depth concept, the first line of defence corresponds to maintaining the installation within the operating conditions stipulated in the Technical Specifications. The second line corresponds to monitoring and ensuring the operability of the safety related functions by means of surveillance tests and maintenance of safety related equipment and systems. This second line of defence explains the general safety significance of requalification.

The performance of requalification tests is described by EdF as follows :

In general, the requalification is performed in two successive steps. First, the equipment is requalified and afterwards the respective system or functional unit is tested. The requalification of equipment is called “intrinsic requalification”. The requalification of a system or functional unit is called “functional requalification”. The latter requalification is performed with the normal operating configuration or with a representative configuration.

The requalification is an integrated part of any intervention. It is planned before the beginning of an intervention and the scope of the requalification is reassessed after the intervention, when one knows what has been done and what has been the cause of malfunction. The preparation of the requalification defines the necessity of the

requalification, the type of the test to be performed, the respective mode of operation, the acceptance criteria, and the test conditions.

The documentation of the intervention should include the analyses performed during the preparation and the report of the test execution with the results of the requalification test. The achievement of the required requalification results and the successful treatment of possible deviations are prerequisites for an equipment or system to be declared operable.

This generic study describes the basic concept of requalification in different countries and lessons learned form operating experience feedback. 41 events (some of them are generic) from 7 countries have been evaluated in detail. They have been classified according to following aspects related to the main cause of the event:

- Deficiencies in the requalification programme content
- Deficiencies in the requalification test preparation
- Deficiencies during organisation and scheduling/rescheduling of requalification tests
- Deficiencies during test performance or post-test evaluation

It has to be taken into account that the events described have been specifically selected to demonstrate the main aspects of potential problems related to requalification. They definitely do not set up a basis for any meaningful statistical analysis. It has to be noted that another generic study of PWG 1 has been devoted to the specific problems of latent failures and of human factors (ref. ETF works).

The basic concept of requalification

Fundamentals of a requalification program specification

In order to be declared operable in terms of the Technical Specifications, all safety-related systems and components, which have been taken out of service for any reason (i.e. for maintenance or repair work or for modification), have to be subjected to formal and documented requalification tests in which the correct functioning of the equipment and system is verified. This test should establish that all the required safety functions, as determined at the design stage, can be performed by the tested component (or by the complete system) and that in case of repair, the original defect was corrected and no new defects have been introduced by the repair or maintenance work itself.

Requalification testing after maintenance and repair is a routine activity having a standard requalification documentation. Requalification tests are performed in accordance with procedures and instructions and properly documented in accordance with the QA programme. They make it possible to measure the performance of the equipment, to compare measured values with acceptance criteria and to document test data. Depending

on the work that took place, new working characteristics might be established in the requalification process such as reference values for further in service testing.

In defining requalification tests, maximum use is made of existing periodic test procedures. They may be applied in part or in full depending on the details of the work carried out. Requalification tests after modifications may include some additional non-routine tests to be defined on a case by case basis. Depending on the nature of the modification, requalification tests might in this case be equivalent to those used in the commissioning phase of the plant. Decisions as to the adequacy of the requalification program are taken by authorised plant staff responsible for the work in agreement with the staff of the division responsible for operation activities. Assistance might be provided by a technical support division.

The acceptance criteria which are applied in general are based on the Technical Specifications and on in service test criteria when applicable. In the case of non routine requalification activities such as in the case of modifications, special requalification procedures may be established based on design criteria, manufacturer requirements, codes and analyses. Requalification tests are normally performed under conditions which are representative for normal operating conditions. In some cases it can be necessary to apply more stringent conditions which have to be defined on an ad hoc basis (if this is not possible for practical reasons, such as the weather conditions, test results may be extrapolated to the design conditions).

The necessity to perform a requalification test is indicated as soon as a work permit request is issued (in the case of maintenance or repair) or a modification proposal is submitted for approval. The scope of components to be included in the requalification test will depend on the impact of the work on the system and will include all components rendered inoperable by the work. In principle, requalification testing is applied to all safety-related equipment for which the work involves an activity which may degrade its safety function (if performed inadequately) or of which electrical supplies have been racked out during the work (requalification of the breaker). Requalification may include the tests of connected systems and other systems in the work area that may have been disturbed by the work. In case of a modification, the requalification test should include checking of the correct functioning of neighbouring components and systems which might be indirectly affected by the modification itself or by its installation.

In some countries like Finland [1,2] and Germany [3], regulatory guidelines have been established related to the procedure for maintenance, repair and modification work at nuclear facilities. Such guidelines impose obligations on the utilities in general and more specifically with regard to the performance and documentation of requalification tests. They

[1] STUK Guide YVL 1.8 Repairs, modifications and preventive maintenance at nuclear facilities

[2] STUK Guide YVL 2.5 Pre-operational and start-up testing of nuclear power plants

[3] BMI Guideline Relating to the Procedure for the Preparation and Implementation of Maintenance Work and Modifications at Nuclear Power Plants

may also stipulate the involvement of the Regulatory Body or its technical support organisation in terms of the approval of test programmes and test results.

The types of requalification tests

Requalification tests after repair or maintenance are mainly standardised activities based on normal surveillance test procedures. The type and extent of the requalification test will therefore be dictated by its objective (requalification of a specific component or of a system), the type of components to be tested and the nature of the previous work on that component or system (routine maintenance activity, non-routine maintenance activity, repair or component made inoperable).

Some examples are given below:

- for motorised valves, testing includes systematic checking of Technical Specifications and in service test criteria by measuring opening and closure times and, in addition, remote position indications will be checked; the test may cover automatic and/or manual actuation depending on its objective; when the work involves a maintenance or repair activity, a torque signature may be requested; in addition to opening or closure times, other safety functions such as leaktightness (typical for containment penetration valves) may be checked;

- requalification testing of pumps is based on Technical Specifications and in service test criteria if the work involves the mechanical parts of the pump or its motor (temperature of bearings and motor, pump vibrations, fluid pressure and flow; if the impeller has been replaced or modified, several points of the pump's performance curve are measured and the reference curve is modified for further in servive testing); if the work is limited to its electrical part, the test might cover cabling, breakers and fuses as well as current and voltage protections;

- requalification programs after work on diesel generators are mainly based on Technical Specification surveillance requirements and include, as a minimum, start-up, coupling and load tests; in some cases, especially after a modification or a major overhaul, endurance tests are required as well; if the work also covers the alternator part, tests similar to those of pump motors are required (see above);

- requalification tests of pumps and diesel generators may include specific checks of support systems such as lubrication and cooling circuits as well as the instrumentation, if these systems are part of the work;

- requalification tests of analog and digital protection and actuation channels are typically not different from the functional tests which are performed on a periodic basis;

- requalification of reactor protection instruments involves checking of control panel and process computer indications and alarms and checking of status indications on the entries of the reactor protection cabinets.

The details of the tests to be performed, in the case of requalification after a modification, are documented in the modification file. This file is submitted for inspection and approval to the regulatory body. Also in these cases maximum use is made of functional tests in accordance with existing test procedures. Specific tests may be specified on an ad hoc basis depending on the nature of the modification and the impact of its execution on the system (i.e. performance of blank tests in case of re-cabling, reiteration of initial commissioning tests). Sometimes specific checklists are used which support the specification of requalification tests after modification.

For requalification activities after an outage, specific standardised requalification programs and procedures, which cover the whole system, are established and applied by the operations division before or when the system is put back in operation and before it is declared operable. It includes systematic checking of the line-up of the system (checking locally the position of all valves, this is exceptionally important for the systems which cannot be functionally tested), checking the availability of the instrumentation and the position and status of breakers, verifying the status and position indications of valves on the control panels and performing functional tests of motorised valves and pumps. These programs can be supplemented by specific tests on demand of the maintenance division.

lessons learned from experience feedback

Findings and lessons to be learned from these events might be very different, not only when looking at the failures during the preparation phase of the requalification tests, but also when looking at the phases of carrying out of tests and monitoring after the requalification.

In fact, problems discovered after inadequate, incomplete or non-representative requalification tests result from one or a combination of the following factors:

- lack of identification of the need to perform a requalification test
- inadequate analysis of the impact of test conditions (causing system or equipment unavailability, I don't understand this otherwise?)
- inadequate specification of the required test conditions
- inadequate specification of the required test procedure or inadequate definition of applicable acceptance criteria
- inadequate selection or qualification of tools used (i. e. measuring apparatuses)
- inadequate analysis of the ongoing work in order to define the most appropriate and comprehensive requalification test

Therefore, the progress has to be made during the following phases of the processus of performing of requalification tests :

1. Definition of the content of requalification programme
2. Preparation of the requalification tests
3. Organisation and Scheduling / rescheduling of the requalification tests
4. Execution of the tests and post test Evaluation

Definition of the content of requalification programme

The phase of definition of a requalification test program includes the identification of the need to perform a test (objective), the selection of a representative test (type of the test, acceptance criteria and tests conditions). Problems during the definition of the requalification program may stem from : the lack of identification of the need to perform the test, the inadequate specification of the required test conditions and/or the inadequate definition of applicable acceptance criteria. Following events illustrate potential deficiencies :

In France (generic design fault), during draining of the spray additive (soda) tank associated with the containment spray system (EAS), to allow maintenance work to be carried out on a mixing pump, the low-level alarm in the spray additive tank failed to trip. This alarm initiates isolation of the spray additive tank from the rest of the EAS system. In the event of an accident requiring actuation of the containment spray system, there would be a potential risk to safety in that failure of the low-level alarm to trip could lead to damage to the EAS pumps as a result of air being entrained from the spray additive tank once the latter had been emptied. This malfunction was attributable to the design of the bottom instrument tap connection for the level detector column, which creates a trap for a residual amount of sodium hydroxide. The presence of this residual volume of sodium hydroxide prevents the low-level sensor from generating the signal indicating that the tank is empty which is used to initiate isolation of the tank. This design fault proved to be generic and thus common to all 1300 MWe reactor units. It had remained undetected during both start-up and periodic tests due to the fact that such tests consist simply in simulating a low level in the tank by isolating the tank from level-sensing instrumentation lines. As a result, the fault was only discovered once the tank had actually been drained. The main lesson learned from this fault is the need to analyse whether tests are properly representative. In cases where standard operating conditions cannot be reproduced during a test, a careful assessment must be made of the differences between standard and test conditions, and measures drawn up to compensate for such differences.

During a series of in service tests at nominal and 110% nominal power level of an emergency diesel generator (DG), high oil and cooling water temperature alarms occurred after a few minutes of operation, resulting in respectively manual and automatic trips of the DG. The tests occurred during a period of warm days with outside temperatures going up to 28°C, which is rather unusual for the plant location. The root cause was

determined to be an inadequate design of the capacity of the DG cooling system, which according to design should be qualified for operation with outside temperatures up to 30°C. The design deficiency was a common mode problem because redundant trains were affected as well. The lack of cooling capacity was explained by the fact that the DGs had been modified a few months before with the objective to increase its nominal power level. The design deficiency had not been detected during the post-modification requalification tests which had been performed with success but at lower ambient temperatures. In the establishment of acceptance criteria for the post-modification tests insufficient attention had been given to the influence of ambient temperatures on the operability of the DGs. During the review of the post-modification test results operating parameters such as increase of oil and cooling temperatures had been insufficiently analysed as well.

After the plant outage during the first performance of a periodic partial stroke test of the feedwater isolation valves at full power, a fast full closure of one of the valves occurred instead of the foreseen slow partial closure, resulting in a reactor trip. The hydraulic circuit of each feedwater isolation valve is equipped with 3 separate solenoid valves: 2 for fast closure which are separately actuated by 2 different reactor protection signals, protecting the plant against internal and external accidents, and 1 solenoid valve for slow closure only used during testing. The failure was explained by the inversion of the cable connections to 2 of these solenoid valves. The consequences of this failure were not only an increased risk of reactor trip during testing, but also the inoperability of a fast isolation function of the feedwater line (needed in case of a feedwater line break as a consequence of an external event). The cable connection error had not been detected during the post-outage requalification test of the valve performed shortly before start-up of the plant. The scope of this test and the periodic test procedures used for this test were inadequate to detect the cabling error: only full closure tests were performed to qualify the protection channels and valve closure time was only verified by actuating one of the fast closure solenoid valves. The origin of the cable connection error could not be traced back because no intervention had been planned on this valve during the previous outage.

A full load rejection capacity test failed due to the inadvertent actuation of the reactor flux variation protection channel as a result of moderate reactor coolant pump speed variations during the test. The failure was explained by an incorrect setting of gain factors for coolant pump speed in the electronic compensation module of the reactor protection channel. Previously performed full load rejection capacity tests had never shown this problem because they were systematically performed at the end of a cycle when reactor coolant pump speed compensation is hidden by the effect of the high negative reactor coolant temperature reactivity coefficient. The consequence of the incorrect adjustment of the protection channel was a loss of full load rejection capacity during a part of the cycle. The incorrect settings of the gain factors were not discovered during the periodic functional tests of the channel with an automatic testing console, because the latter had identical deficiencies in its design : these design deficiencies were not discovered due to a lack of global validation of the design.

On each of the 3 trains of the shutdown cooling system a tandem of almost identical pilot operated safety valves, but with different set-pressures, is installed to protect

both reactor coolant and shutdown cooling systems from over-pressurisation in intermediate and cold shutdown conditions. During the outage a maintenance activity occurred on the safety valves in 2 trains, in which replacement seals of the wrong type were installed in the actuators of the valves with the lower setting, which act as isolation valve in the tandem disposition. These valves are normally in open position when the shutdown coolant system is at nominal pressure. However the error resulted during post-outage pressurisation of the circuit in a progressive water ingress and additional downward force on the valve disc resulting in a progressive closure of the valve, which rendered both redundant safety trains inoperable for low temperature overpressure protection. The requalification of the safety valves had been of a generic nature and had been limited to a verification that the isolation valves opened correctly when the system was pressurised (verification of the setting pressure of the valve). It did not consider the particular nature of the maintenance intervention, which had been performed for the first time and by a specialised service contractor. As this particular failure mode was not expected, the position of the valves was not monitored any further. The problem was only discovered by chance a few days later by an operator on the basis of anomalous valve position indications on the electrical cabinet display. As corrective action a periodic surveillance of safety valve positions during the shutdown mode has been introduced and a study was launched to improve the current requalification procedure for these valves (possibilities sought to pressurise valves by test device instead of by system pressure).

Sometimes, intrinsic tests need to be completed by a whole functional test, as illustrated by the two following events.

A test carried out during pressure testing of the containment revealed that the orifice plates in the reactor building decompression system for units 1 and 2 had not been properly installed. This system had been installed in all PWR units in France and is designed to reduce pressure in the reactor building in the event of an accident. This anomaly meant that the line connecting the sand-bed filter to the reactor building had been closed off. Inspections carried out at all nuclear plants in France revealed similar anomalies at five other units. Remedial action was taken immediately. In the event of an accident, the anomalies detected would either have precluded use of the filter or would have resulted in the filter being used under abnormal conditions. The causes of the anomaly were a failure to comply with quality assurance rules, particularly during end of installation inspections, and the fact that no functional tests had been performed on the system.

At a Swedish plant the auxiliary condenser system consists of a condenser placed beneath the main steam lines near the reactor pressure vessel (outside containment). From the main steam lines, two steam lines are connected to the condenser. On the outlet side, two pipes with one control valve and one isolation valve in each line, lead the water back to the reactor pressure vessel, via the recirculation loops. Normally the isolation valves from the auxiliary condenser open on scram signal and the two control valves from the auxiliary condenser adopt reactor pressure control. The auxiliary condenser adds capacity and diversity to the reactor pressure relief system. On January 21, a reactor scram with steam dump block occurred. On this occasion, two high

temperature signals from the auxiliary condenser was obtained after six seconds and shortly afterwards the isolation valves from the condenser unexpectedly closed. Reactor pressure control automatically switched over to the pressure relief system and steam was blown down to the condensation pool. When the high flow alarm was cleared in the control room, the isolation valves opened again and reactor pressure was re-routed to the auxiliary condenser. The available systems for residual heat removal from the reactor was reduced as both the turbine condenser and the auxiliary condenser were unavailable. The temperature switches were redesigned so that they would actuate when de-energised. The cause of closure of the isolation valves from the isolation condenser was that the two temperature switches, that actuated after the scram, were set to actuate when energised (working current) instead of de-energised. Thereby the logic to the valves were supplied with false signals. The old temperature switches were replaced by new ones. The new ones were incorrectly designed resulting in a switch actuation when they were energised instead of when de-energised. The mistake in design was not discovered during the verification tests as these tests only included partial testing of the signals, not the complete signal chain. Because of the mistake in design and the insufficient verification of the new design, the event was classified as Level 1 on the INES.

The events selected by USA which appear in the appendix, related to the lack of testing after installation (IN 97-52) or after the replacement of equipment "like for like" (IN 93-13) or during the removal of a temporary device (IN 93-60) or after a benign painting operation (IN 93-76), to inadequate checking of a modification or design (LER 93-012) or to insufficient checking of a new badly adapted component or the modification of the logic associated with changing a component illustrate also the problems encountered during the phase of definition of the tests.

All these events show the importance of a good analysis of the impact of the maintenance or modification on the system itself (or on the whole process), in order to determine the most adequate and representative test conditions, to identify the parameters to be monitored during the test and the required analysis of test results to be performed afterwards.

Based on the studies made in Finland most requalification problems were related to modifications made at the plant. This shows the importance of clearly defined and also monitored modification processes. During the plant modification process more attention should be paid to the determination of functional tests after modification works. One example is the testing of valves in real flow conditions. Also the importance of physical checks of valves actuation and line-up instead of confidence on indications is highlighted. A more general conclusion is related to the need for independent checks of working papers including instructions for requalification testing after modification and maintenance work at the plant.

The Hungarian events selected for this study show that the failures of the safety system components occurred due to lack of essential design information, ignoring system conditions and interfaces, and lack of comprehensive testing procedures. All problems stem from design deficiencies. At the present time, it is very difficult for the licensee to

obtain relevant design information from the original supplier, because it is practically non-existent.

Preparation of the requalification tests

The phase of preparation of a requalification test program includes the preparation of procedures, the selection of adequate tools and the risk analysis. Problems occurring during requalification tests may origin - from the lack of a proper risk evaluation of the planned work, leading to unforeseen situations - failure to provide adequate, specific and well-prepared procedures and instructions for such work, resulting in unmonitored and improvised actions or omission of certain actions during the carrying out of requalification testing itself. Problems may also stem from inadequate selection or qualification of tools used.

In France, a reactor trip was caused by over-current protection systems of 2 Essential Service Water System pumps and the charging pumps train A, during houseload operation tests. The automatic switchover to train B was successful. After investigation, it was found that all the protection systems of the 6.6 kV actuators supplied by the AC Emergency Supplied Distribution System train A were incorrectly adjusted (between 5 and 33% below the lower threshold) subsequently to maintenance work during outage. The faults were revealed by the high frequency of the electrical power supply during houseload operation (52 Hz). The causes were an unclear worksheet leading the operator to make an incorrect interpretation, thus an error of adjustment.

During the requalification test of a reactor protection channel after the modification of its setpoint, an unexpected actuation of the protection channel occurred resulting in a loss of all reactor coolant pumps followed by a reactor trip. Due to the lack of a specific requalification procedure, some improvisation occurred during the performance of the test. Some errors of judgement were made by the technicians who were in charge of this test when selecting the sequence of actions such as injection of the test signal and powering of the output amplifiers of the protection channel. This made the channel particularly vulnerable to a loss of power to one of its output amplifiers. Such a power loss occurred as a result of a manual switching of power sources of the output amplifier during the requalification test. In addition to the lack of a specific sequential procedure, no risk evaluation of the test had been performed. Furthermore conditions to be respected when re-supplying power to reactor protection channel output amplifiers were unclear for the technicians involved at the time of the incident and had to be clarified by improvement of procedures.

The consequences of such requalification tests may, in terms of safety significance, vary from rather low, such as in cases of spurious actuation of safety signals or reactor trip, to higher significance when they result in destruction of safety equipment.

Organisation and Scheduling / rescheduling of the requalification tests

Responsibility for performance of requalification tests is normally shared by several entities within an organisation (mainly operations, mechanical and/or electrical maintenance and instrumentation and control divisions), depending on the nature and objective of the requalification test. Requalification testing by the maintenance department after maintenance work is mainly focused on the trouble-free performance of the equipment itself. In the case of requalification testing after modifications, testing requirements are covered by the modification dossier and special arrangements may be valid involving contractors under the supervision of the modification project manager. Lack of adequate communication between the departments involved may lead to a failure of requalification. On the other side, having enough information on the scheduling and nature of tests performed by the other departments may help to avoid some events.

In Germany, during a review of the start-up procedure it was discovered that the check for the sump availability was performed in a plant mode, where the sump suction should be operable. During outage the sump is covered to prevent intrusion of foreign material into the sump and the sump suction lines. The covers are removed at the beginning of the start-up. The prescribed check whether the covers had been removed, was scheduled at a later period. At this time the reactor was already in hot stand-by mode. In this mode of operation the sump suction has to be operable to control potential LOCA events. As a result of the procedure review, the check of the sump availability was rescheduled to a mode of operation before the sump suction operability is necessary. This event points out the importance of scheduling the test at the correct plant status.

Preventive maintenance on emergency systems, which protect the plant automatically against external accidents, is allowed during plant power operation by Technical Specifications (TS) but only on one safety train at the time. In Belgium, during the maintenance operations of one of the safety trains, it was fortuitously discovered that a number of motorised valves had been left racked out in closed position in one of the other safety trains after completion of maintenance and requalification activities of that train. The event resulted in the simultaneous inoperability of 2 emergency safety trains for a period of 36 hours which was a violation of TS. The motorised valves were left racked out due to omissions and ad hoc reductions of the formal requalification process by the operating teams involved. In spite of procedure instructions it was decided not to rack in the motorised valves after the completion of functional tests of the control channels which actuate the valves, knowing that a global requalification of the safety train would follow after ending of all maintenance activities. During the global requalification process the shift supervisor omitted to distribute a check list to the field operator for status verification of power breakers. Furthermore a decision was made to reduce requalification tests, as foreseen in the requalification procedure, by omitting functional tests of the affected valves on the basis that no maintenance activities had been performed on the valves themselves. Independent verification of requalification files by the operation division head had not yet been performed at the time of discovery of the TS violation. As a result of this event, the

accepted practice to reduce ad hoc formally required requalification tests was re-evaluated.

In Belgium, during a requalification test of an emergency water supply pump after maintenance on the system, the pump was started without adequate venting of the circuit . This resulted in inadequate cooling of mechanical seals and bearings. As the pump was not immediately stopped by the control room operator and no field operator was near the pump, it ran for some time in these conditions resulting in severe damage of pump internals and temporary unavailability of a safety system. The omission of the venting operation which is an essential step in the global line-up and requalification process was explained by a combination of several factors: the foregoing line-up of the system was performed with unadequate procedures and did not include venting (tagging/untagging sheets used instead of system procedures); the requalification of the pump itself was delayed for four days and a communication problem occurred between operating teams regarding the status of the system when the pump was launched (the system was reported available in an oral way and there was a lack of adequate documentation on the precise status of the system in the control room); the wrong checklist was selected when performing an independent verification of the system status when the pump was started (confusion induced by the existence of 2 types of checklists, one for initial start-up and one for periodical test). In general a lack of supervision was noticed on the correct selection of documents which support critical operations in the requalification process. As a result of this event several corrective actions were taken to reduce the likelihood of occurrence: operating documents supporting line-up and functional tests were improved providing more precise and explicit information regarding venting operations and reduced check-lists were abolished; traceability of performed activities in the requalification process was improved which is essential when more than one shift is involved in the requalification of a system; improved transfer of information on plant status during shift turnovers. In addition, physical presence of field operators near first time start operations of pumps is required when allowed on the basis of worker safety considerations.

Another problem area is the requalification after maintenance works performed during outage and start-up. Time pressure in these cases has an remarkable role in the unsuccessfulness of the requalification process : some tests are forgotten, scheduled too late or with insufficient duration.

Adequate communication between all organisations involved is essential for successful requalification. This communication should be structured and encouraged by administrative means. The operations department, which is responsible for the overall process, should be properly informed of the nature of the work done on the equipment or system to be tested to be able to decide on the required scope of requalification tests. It should also have enough information on the scheduling and nature of requalification tests performed by other departments to assess correctly the impact of such testing on the overall process. A special challenge exists for adequate communication if subcontractors are involved. Other departments should have a clear picture of what is expected from them in the requalification process. Also, correct and comprehensive information exchange

within the operations division, especially at shift turnover, is essential for the continuity of the requalification process.

Adequate documentation of all activities, including the work itself on the equipment previous to the requalification test as well as all steps of the whole requalification process, is essential to ensure traceability.

Management supervision and oversight of the requalification process is important not only in terms of compliance of internal procedures but also regarding the effectiveness of the installed process.

For example in Sweden the Regulatory Body (SKI) launched an independent investigation after an event at the Swedish NPP. Based on the findings of this investigation and the increasing concerns that SKI had regarded realignment and operability of safety systems after an outage, a general letter was addressed to all Nuclear Power Plants in Sweden. The letter, dated November 28 1996, demanded prompt answers, before the end of January 1997, on five specific demands for action:

- A procedural overhaul of all routines, regarding realignment and verification of operability in safety systems after maintenance.
- An analysis of the need to improve the routines for work control, planing and re-planing during an outage. Special focus should be set on the chronological order of safety system tests.
- An analysis of the routines for handling occasional changes in procedures
- An analysis of possible improvements regarding the operators routines and tools for work control and work follow up
- An analysis of possible improvements, regarding operability indications of components and systems in the control room and improvements in operator round routines.

SKI is encouraging the plants to take further corrective actions and will take initiative to new discussions and reviews. SKI has formed a taskforce within the agency consisting of experts in both engineering and human performance matters. The need to consult external experts and to start research and development projects is also acknowledged.

For Belgium, over the years and with gained experience, a gradual improvement of the requalification practices has been noticed in all plants. Especially improvement of administrative procedures, clearer division of responsibilities for operations and with other departments, and communication has been improved. Clarification of responsibility for operations, improvement of test procedures or other supporting documents are also noticed.

Execution of the tests and post test evaluation

The events selected by contributors were related to errors such as wrong reinstallation of pieces, replacement parts of the wrong type, or valves left at an incorrect position.

In Finland, one of two emergency feed water pumps was damaged at the end of an annual maintenance outage when the pump was operated during a back-up diesel testing on 29 August 1997. The pump stopped few minutes after start due to actuation of a protection function from low pressure on the pump's pressure side. The pump was dismantled and its internals were found to be heavily stuck. The pump damaged because the check valve of its minimum flow circuit was erroneously in the closed position. The valve had remained in the closed position in connection with an earlier work during the outage and its incorrect position was not detected in line-up. When the pump was tested before back-up diesel tests process alarms were blocked due to large amount of alarms and were not recovered before testing the system. Also the system pipeline was not checked as it should be before the testing. The test duration of the pump was not long enough to reveal anomalies in the line-up. Without these errors done during the test preparation and during the execution of the test the pump would not have damaged during the back-up diesel tests. A proper analysis of the pump test results before the back-up diesel tests in which the pump was finally damaged would have revealed wrong valve position and so the pump damage too.

In France, non-opening of a valve in the injection system during a surveillance test revealed a lubrication defect in the servomotor which resulted in deterioration of the wheel/worm screw system. The origin of the defect lies in the fact that servicing sheets mentioned a level of lubricant to be injected into the wheel/worm screw system housing, instead of the quantity of lubricant required by the vendor. Taking into account the common cause aspect of the anomaly which involved a large number of safety-related valves equipped with these servomotors, internal inspections of the valves were carried out. The task was made much easier in analysing records available or performed after inspections using the valve functioning diagnosis aid device (SAMIR). These inspections led to the increase of lubricant, as well as several servomotor preventive replacement. The vendor was requested to perform further assessment regarding valve behaviour and wheel/worm screw system degradation resulting from both a lack of lubricant and number of actuations.

Another group of work errors covers wrong adjustments in electronic cabinets. Finally judgement errors can be made during complex work such as (re)calibration of instrumentation, which are sometimes insufficiently described in detail because the technicians qualified to perform such work are considered to be experts.

During a pressure transient in an German BWR, all safety and relief valves opened and closed properly but the evaluation of the event showed several irregularities, especially the limitation of the valve stroke of three of these valves. The subsequent analysis revealed the deformation of central pivots caused by ignition of radiolysis gases. For the three valves, reductions of the stroke of 12 mm, 8 mm and 6,5 mm were

determined due the deformation of the central pivot. During subsequent tests one valve, which was actuated via a pilot valve that had not been actuated during the transient, showed also the irregular stroke described above. Such behaviour was also observed on another valve during the valve tests in the previous year. But the subsequent inspection of this valve had indicated no abnormalities. The irregularities in the maintenance records did not trigger a detailed investigation at that time. About half a year before this event, a similar event occurred in another NPP with one safety and relief valve stuck open during test. The event analysis revealed that the failure mechanism was the ignition of radiolysis gases while opening of the pilot valves.

In a Belgian NPP, the excessive hysteresis value of a high intermediate neutron flux setpoint resulted in a reactor trip, when reactor power was decreased below a reactor protection interlock at 10% power. During calibration of all setpoints connected to this channel just before the previous start-up, an error occurred in the selection of the potentiometer in order to adjust the as found hysteresis value of the P6 interlock setpoint. The potentiometer of the reactor trip setpoint, which had been calibrated just before, was erroneously selected due to an error in the calibration procedure and was adjusted up to the end of its range without noticeable effect on the hysteresis of the P6 interlock. The situation was left as such and the noticed problems during the calibration were recorded in the test protocol. The consequences of the committed error were in this case rather benign (reactor trip during power reduction or plant shutdown) but could have been more significant if the error had occurred on other reactor protection setpoints. There was an obvious lack of questioning attitude during the calibration job itself. In addition there was a lack of verification and follow-up of the test protocols. No formal independent requalification tests are foreseen after setpoint adjustments as such interventions are integrated in the requalification procedure of the reactor protection cabinets. An analysis of the need to require such formal requalification after interventions on the setpoints is still pending. A commitment was made to improve the independent verification process on the basis of test protocols.

Errors performed during this phase are very tricky because they may induce latent failures in safety equipment, when not discovered. Common mode defects typically result from this activity. More over, the problems during the realisation of the test itself or afterwards (such as lack of questioning attitudes from the test personnel, last-minute decisions to change or omitting steps in the requalification process and lack of verification, analysis and follow-up of test results) cannot be checked because there is no " requalification of a requalification ".

It shows the importance of a good analysis in order to determine the most adequate and representative test conditions, to identify the parameters to be monitored during the test and the required analysis of test results to be performed afterwards. Special attention has also to be attached to the means and tools used to perform the (re)qualification test because the same error may also have crept into their design. Finally, training of plant personnel, some commitments to re-evaluate established practices and improvements of the traceability of requalification activities are also very helpful. It seems

to me that this paragraph is not specific to this section as it covers also other phases of the requalification process.

In Finland, based on operating experience, the operating personnel have been given further training in procedures relating to the checking and restoration of valve normal state. Also the importance of detailed online documentation when making changes in the plant systems was highlighted.

In France, since 1990, the test results of restarting after an outage have to be presented to the regulator, in the 10 days following the plant being switched to 90% capacity. These meetings to present start-up tests brought to light the persistence of difficulties. According to the IPSN, the root of these difficulties is the organisation of the plants and the test documents. Progress can reasonably be expected as a result of the good practices observed at some plants.

Examples of recommendations

The following requirements made by Electricité de France, the french licensee, may be of some use. They were known as the “Directive 76” :

1. Requalification is an integral part of the maintenance activities.

Each maintenance document must include requalification activities.

2. Requalification must be prepared in advance at the start of the maintenance activities, be this one scheduled or unplanned.

In particular, requalification consists of establishing:

⇒ assessment whether requalification is required,

⇒ the nature of the requalification tests (type of test, operating procedure, criteria to be checked, test conditions etc.),

⇒ additional or compensatory measures to be taken in the absence of suitable tests, depending on the nature of the maintenance activities and the result of the risks evaluation.

The risks are evaluated at the preliminary analysis stage as regards of :

⇒ the maintenance activities,

⇒ the requalification itself,

⇒ the plant operation modifications associated with the maintenance activities.

3. Maintenance documents should make it possible to trace the planning and execution of the maintenance activities and the requalification results.

The Quality Plan, or any other equivalent document, should state the maintenance-operation interface, clearly showing, in view of the analysis mentioned above, the intrinsic and functional requalification tests.

4. Requalification tests require a range of skills (maintenance, operations etc). Responsibilities must be clearly assigned during the activity planning phase.

As a general rule:

⇒ the nature and organisation of intrinsic requalification is the responsibility of the maintenance coordinator, with the support of individuals with the necessary skills,

⇒ the nature and organisation of functional requalification is the responsibility of the operations coordinator, who obtains the necessary information and relies on the skills of the maintenance coordinator or coordinators.

5. Overall coordination of requalification operations is necessary.

The resources and skills necessary must be identified in order to be able to:

⇒ guarantee the comprehensiveness of the requalification in terms of the maintenance or modification work,

⇒ verify that initiation of "maintenance - intrinsic requalification - functional requalification" operations is coherent (management of interfaces between departments),

⇒ gain an overview of the tests and determine whether equipment and functional sub-systems are operable (during the unit outages, a report is made to the Unit Outage Safety Commission).

6. It is necessary to await the results of requalification and the resolution of any deviations before declaring equipment or systems available.

In France, these good practices likely led to good results :

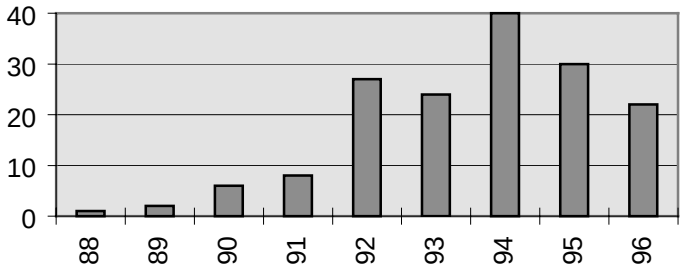

Figure 3 - Numbers of significant safety-related incidents associated with requalification.

The change in the number of significant safety-related incidents associated with requalification over the period 1988 to 1996 (figure 3 above) must be analysed to identify trends. Overall, it reflects that this particular problem has been taken into account. Problems relating to requalification were discovered in the period 1988-1990. In the period 1991-1993, measures taken by EDF[4] became more widespread and bolstered requalification. The increase in incidents can be partly explained by the growing number of power plants. The decrease from 1995 corresponds to the year in which the EDF's proposed measures were supposed to start taking effect.

Conclusion

The requalification of equipment ensures the operability of this equipment, i.e. components and systems, after being taken out of service during an outage. The requalification is designed as a barrier in the defence-in-depth concept that permits the declaration of operability and thus to fulfil the minimum requirements for starting up.

The requalification is equally vulnerable to human and technical problems. The human induced problems are on one hand human failures during the requalification and on the other hand organisational deficiencies. The organisational deficiencies include problems in the scheduling of requalification tests, procedural deficiencies, and deficiencies in the documentation and communication. The technical problems are generally based on limitations of the requalification tests. These limitations exist mainly for systems and components, which cannot be tested under the conditions present during design basis accidents. Therefore, thorough design and extensive tests of this equipment has to be performed in advance of the installation.

The requalification is not the only measure to demonstrate the availability of systems and components. During operation in-service inspections have the task to show the operability of safety related systems, in particular for stand-by systems. But, the scope of requalification tests and in-service inspections show some overlap. Thus, failures introduced during maintenance activities, which have not been detected during requalification, have a comparable high chance to be overlooked during in-service inspections, too. These types of latent failures, which are only triggered by real demand

[4] Guide d'intervention sur les matériels, Electricité de France.

conditions, are of specific interest. They can only be avoided by quality assurance measures for maintenance activities and by testing under conditions as realistic as possible.

Compared to in-service inspections the requalification is specific due to the complexity and time pressure of multiple tasks at the end of an outage. This situation is characterised by thorough configuration control of safety related equipment. The shift team has the difficult task to ensure the appropriate configuration of equipment under high communication pressure within the shift and with other personnel. Special attention has also been given to the communication between shifts especially at shift turnover.

In this report the main areas of requalification and its typical problems are discussed. Internationally selected events are described to underline these typical problems. The selection of events is not intended to be complete. Conclusions regarding safety significance or statistical purposes cannot be drawn from this selection.

The operating experience regarding requalification shows that there exists equipment especially vulnerable to latent failures introduced during the requalification procedure. Generally, stand-by safety systems, valves, electrical equipment (e.g. breakers, relays, and switches), as well as the instrumentation where the measured value normally does not change during operation, can be identified as vulnerable.

The lessons learned from the events indicate that typically the actions taken are specific to the event. Personnel training and procedure modification are often being (or have often been) mentioned as areas of actions taken. Generic actions taken have rarely been initiated due to the selected events.

The supervision authorities shall ensure that the plant operators learn from the experiences gained by the requalification. These experiences are basis for the continuous optimisation of the administrative control and of the requalification procedures.

A further source for optimisation measures is the good practice of other utilities and authorities. Some good practices are mentioned in chapter 3 of this report.

Appendix 1 - Contributions

Representatives from Belgium, Finland, Germany, Hungary, the United States of America, United Kingdom and France agreed to participate in the study, and the representative of France volunteered to coordinate it. Sweden joined the Working Group later. Countries contributed to the study by submitting either reports documenting the most representative examples in their respective countries, along with general comments underlying the specific findings and insights resulting from their respective evaluations, or selections of events in their respective countries relevant to the study.

Contributing Countries	Type of contribution
BELGIUM	- Analysis of Selected Events - Note on the basic concept of requalification
FINLAND	- Report on human factors related to maintenance and modification - Analysis of Selected Events
GERMANY	- Analysis of Selected Events - Proposals for the introduction and conclusion
HUNGARY	- Analysis of Selected Events
SWEDEN	- Events relevant to the study, Draft of analysis - Report on undetected latent failures of safety-related systems *(mainly relevant to the dedicated Generic study)*
USA	- Around 40 Information Notices (1993-1997)
FRANCE (Lead)	- Synthesis of Evaluations on Requalification

Appendix 2 - Event descriptions

Belgium

Trip of emergency diesel generator during periodic test with high outside temperatures

During a series of in service tests at nominal and 110% of nominal power level of an emergency diesel generator, high oil and cooling water temperature alarms occurred

after a few minutes of operation, resulting in respectively manual and automatic trips of the DG. The tests occurred during a period of warm days with outside temperatures going up to 28°C, which is rather unusual for the plant location. The root cause was determined to be an inadequate design of the capacity of the DG cooling system, which according to design should be qualified for operation with outside temperatures up to 30°C. The design deficiency was a common mode problem because redundant trains were affected as well. The lack of cooling capacity was explained by the fact that the DGs had been modified a few months before with the objective to increase its continuous duty rating (nominal power level). The design deficiency had not been detected during the post-modification requalification tests which had been performed with success but at lower ambient temperatures. In the establishment of acceptance criteria for the post-modification tests insufficient attention had been given to the influence of ambient temperatures on the operability of the DGs. During the review of the post-modification test results operating parameters such as increase of oil and cooling temperatures had been insufficiently analysed as well.

Reactor trip due to a spurious emergency protection signal

During the requalification test of a reactor protection channel after the modification of its setpoint, an unexpected actuation of the protection channel occurred resulting in a loss of all reactor coolant pumps followed by a reactor trip. Due to the lack of a specific requalification procedure, some improvisation occurred during the performance of the test. Some errors of judgement were made by the technicians who were in charge of this test when selecting the sequence of actions such as injection of the test signal and powering of the output amplifiers of the protection channel. This made the channel particularly vulnerable to a loss of power to one of its output amplifiers. Such a power loss occurred as a result of a manual switching of power sources of the output amplifier during the requalification test. In addition to the lack of a specific sequential procedure, no risk evaluation had been performed of the test. Furthermore conditions to be respected when re-supplying power to reactor protection channel output amplifiers were unclear for the technicians involved at the time of the incident and had to be clarified by improvement of procedures as a result of it.

Reactor trip due to full closure of feedwater isolation valve during partial stroke test

During the first performance after the plant outage of a periodic partial stroke test of the feedwater isolation valves at full power, a fast full closure of one of the valves occurred instead of the foreseen slow partial closure, resulting in a reactor trip. The hydraulic circuit of each feedwater isolation valve is equipped with 3 separate solenoid valves: 2 for fast closure which are separately actuated by 2 different reactor protection signals, protecting the plant against internal and external accidents, and 1 solenoid valve for slow closure only used during testing. The failure was explained by the inversion of the cable connections to 2 of these solenoid valves. The consequences of this failure were not only an increased risk of reactor trip during testing, but also the inoperability of a fast

isolation function of the feedwater line (needed in case of a feedwater line break as a consequence of an external event). The cable connection error had not been detected during the post-outage requalification test of the valve performed shortly before start-up of the plant. The scope of this test and the periodic test procedures used for this test were inadequate to detect the cabling error: only full closure tests were performed to qualify the protection channels and valve closure time was only verified by actuating one of the fast closure solenoid valves. The origin of the cable connection error could not be traced back because no intervention had been planned on this valve during the previous outage.

Reactor trip and turbine trip during full load rejection capacity test

A full load rejection capacity test failed due to the inadvertent actuation of the reactor flux variation protection channel as a result of moderate reactor coolant pump speed variations during the test. The failure was explained by an incorrect setting of gain factors for coolant pump speed in the electronic compensation module of the reactor protection channel. Previously performed full load rejection capacity tests had never shown this problem because they were systematically performed at the end of a cycle when reactor coolant pump speed compensation is hidden by the effect of the high negative reactor coolant temperature reactivity coefficient. The consequence of the incorrect adjustment of the protection channel was a loss of full load rejection capacity during a part of the cycle. The incorrect settings of the gain factors were not discovered during the periodic functional tests of the channel with an automatic testing console, because the latter had identical deficiencies in its design: these design deficiencies were not discovered due to a lack of global validation of the design.

Incorrect installation of water pump bearings on 2 safety diesel generators

During the periodic functional 1 hour test of a DG a low temperature cooling water circuit leakage was detected, which was due to a damaged mechanical seal of the water circulation pump. Inspection of the pump showed that the pump rotor itself was also heavily damaged and that all was due to the incorrect installation of one of the pump bearings. Further inspections on the water circulation pump of the high temperature cooling water circuit of the same DG and on the pumps of the redundant DGs revealed that additional pumps were affected by the same installation error although no physical damage to seal or pump rotor had yet occurred. The installation error was traced back to an overhaul operation of the DGs 8 to 9 months ago and neither the requalification test after this overhaul intervention nor the monthly periodic tests performed within that period had allowed to detect the bearing installation problem. The consequence of this event was a loss of long term operability of 2 redundant safety diesel generators. The event showed that the requalification tests performed after DG overhaul were not adapted to detect such bearing installation errors: for requalification purposes use was made of normal periodic functional test procedures which typically require full load tests during 1 hour which is far too short to detect these kind of deficiencies. As a result of this and similar events a generic discussion has been started with the utilities in the frame of the Technical

Specifications improvement program with regard to the required duration of periodic endurance tests and of requalification tests after maintenance interventions.

Simultaneous inoperability of 2 emergency safety system trains

Preventive maintenance on emergency systems, which protect the plant automatically against external accidents, is allowed during plant power operation by Technical Specifications (TS) but only on one safety train at the time. During the maintenance operations of one of the safety trains, it was fortuitously discovered that a number of motorised valves had been left racked out in closed position in one of the other safety trains after completion of maintenance and requalification activities of that train. The event resulted in the simultaneous inoperability of 2 emergency safety trains for a period of 36 hours which was a violation of TS. The motorised valves were left racked out due to omissions and ad hoc reductions of the formal requalification process by the operating teams involved. In spite of procedure instructions it was decided not to rack in the motorised valves after the completion of functional tests of the control channels which actuate the valves, knowing that a global requalification of the safety train would follow after ending of all maintenance activities. During the global requalification process the shift supervisor omitted to distribute a check list to the field operator for status verification of power breakers. Furthermore a decision was made to reduce requalification tests, as foreseen in the requalification procedure, by omitting functional tests of the affected valves on the basis that no maintenance activities had been performed on the valves themselves. Independent verification of requalification files by the operation division head had not yet been performed at the time of discovery of the TS violation. As a result of this event the accepted practice to reduce ad hoc formally required requalification tests was re-evaluated.

Failures of condense water tank level instrumentation

During the installation of a new level measuring instrument on a condense water tank, a cabling error was made (CR indication connected to wrong transmitter due to the inversion of 2 connection leads), resulting in an unnoticed wrong level indication in the control room. The discrepancy between real and indicated tank levels was discovered by operators after many months of operation and was explained by the fact that no formal requalification test of the CR indication had been foreseen. The cabling error was corrected and an ad hoc decision was taken by the technicians, without formal request, to recalibrate the alarm thresholds connected to this level instrument. This operation being badly prepared, a confusion occurred in reference levels and a mistake was made when taking into account the residual water volume in the tank below the lower instrument connection point. As a result of the second mistake the Technical Specification alarms on the tank level were wrongly adjusted. No independent verification of the recalibration job took place and the operation department was unaware of this latter intervention. Also the second mistake was only discovered by operators after a few months of operation. Both errors resulted in an overestimation of the available water volume (the second as large as

87 m³). Following this event, the utility identified a need to improve communication between instrumentation and operation departments concerning the nature of interventions on instrumentation. This should allow a better definition of needs for independent functional requalification by the operation department of interventions on instrumentation.

Inadvertent reactor trip during power reduction

The excessive hysteresis value of a high intermediate neutron flux setpoint resulted in a reactor trip, when reactor power was decreased below a reactor protection interlock at 10% power. During calibration of all setpoints connected to this channel just before the previous start-up, an error occurred in the selection of the potentiometer in order to adjust the as found hysteresis value of the P6 interlock setpoint. The potentiometer of the reactor trip setpoint, which had been calibrated just before, was erroneously selected due to an error in the calibration procedure and was adjusted up to the end of its range without noticeable effect on the hysteresis of the P6 interlock. The situation was left as such and the noticed problems during the calibration were recorded in the test protocol. The consequences of the committed error were in this case rather benign (reactor trip during power reduction or plant shutdown) but could have been more significant if the error had occurred on other reactor protection setpoints. There was an obvious lack of questioning attitude during the calibration job itself. In addition there was a lack of verification and follow-up of the test protocols. No formal independent requalification tests are foreseen after setpoint adjustments as such interventions are integrated in the requalification procedure of the reactor protection cabinets. An analysis of the need to require such formal requalification after interventions on the setpoints is still pending. A commitment was made to improve the independent verification process on the basis of test protocols.

Failure of 2 redundant pilot operated safety valves due to use of wrong type of seal

On each of the 3 trains of the shutdown cooling system a tandem of almost identical pilot operated safety valves, but with different set-pressures, is installed to protect both reactor coolant and shutdown cooling systems from over-pressurisation in intermediate and cold shutdown conditions. During the outage a maintenance activity occurred on the safety valves in 2 trains, in which replacement seals of the wrong type were installed in the actuators of the valves with the lower setting, which act as isolation valve in the tandem disposition. These valves are normally in open position when the shutdown coolant system is at nominal pressure. However the error resulted during post-outage pressurisation of the circuit in a progressive water ingress and additional downward force on the valve disc resulting in a progressive closure of the valve, which rendered both redundant safety trains inoperable for low temperature overpressure protection. The requalification of the safety valves had been of a generic nature and had been limited to a verification that the isolation valves opened correctly when the system was pressurised (verification of the setting pressure of the valve). It did not consider the particular nature of the maintenance intervention, which had been performed for the first time and by a

specialised service contractor. As this particular failure mode was not expected, the position of the valves was not monitored any further. The problem was only discovered by chance a few days later by an operator on the basis of anomalous valve position indications on the electrical cabinet display. As corrective action a periodic surveillance of safety valve positions during the shutdown mode has been introduced and a study was launched to improve the current requalification procedure for these valves (possibilities sought to pressurise valves by test device instead of by system pressure).

Destruction of emergency water supply pump during its requalification test

During the performance of a requalification test of an emergency water supply pump after a maintenance intervention on the system, the pump was started without adequate venting of the circuit . This resulted in inadequate cooling of mechanical seals and bearings. As the pump was not immediately stopped by the control room operator and no field operator was near the pump, it ran for some time in these conditions resulting in severe damage of pump internals and temporary unavailability of a safety system. The omission of the venting operation which is an essential step in the global line-up and requalification process was explained by a combination of factors: the foregoing line-up of the system was not performed with adequate procedures and did not include venting (tagging/detagging sheets used instead of system procedures); the requalification of the pump itself was delayed for four days and a communication problem occurred between operating teams regarding the status of the system when the pump was launched (the system was reported available in an oral way and there was a lack of adequate documentation on the precise status of the system in the control room); the wrong checklist was selected when performing an independent verification of the system status when the pump was started (confusion induced by the existence of 2 types of checklists, one for first start and one for periodical test). In general a lack of supervision was noticed on the correct selection of documents which support critical operations in the requalification process. As a result of this event several corrective actions were taken to reduce the likelihood of reoccurrence: operating documents supporting line-up and functional tests were improved providing more precise and explicit information regarding venting operations and reduced check-lists were abolished; traceability of performed activities in the requalification process was improved which is essential when more than one shift is involved in the requalification of a system; improved transfer of information on plant status during shift turnovers. In addition physical presence of field operators near first time start operations of pumps is required when allowed on the basis of worker safety considerations.

Finland

Damage of the emergency feedwater pump due to pumping against closed valve during the start-up

One of two emergency feed water pumps was damaged at the end of an annual maintenance outage when the pump was operated during a back-up diesel testing on 29

August 1997. The pump stopped few minutes after start due to actuation of a protection function from low pressure on the pump's pressure side. The pump was dismantled and its internals were found to be heavily stuck. The pump damaged because the check valve of its minimum flow circuit was erroneously in the closed position. The valve had remained in the closed position in connection with an earlier work during the outage and its incorrect position was not detected in line-up. When the pump was tested before back-up diesel tests process alarms were blocked due to large amount of alarms and were not recovered before testing the system. Also the system pipeline was not checked as it should be before the testing. The test duration of the pump was not long enough to reveal anomalies in the line-up. Without these errors done during the test preparation and during the execution of the test the pump would not have damaged during the back-up diesel tests. A proper analysis of the pump test results before the back-up diesel tests in which the pump was finally damaged would have revealed wrong valve position and so the pump damage too.

Incorrectly adjusted auxiliary service water system valves at both plant units

Based on inspections carried out after periodic tests it was found out that the actuators of seven valves of the auxiliary service water system had incorrect adjustments for about two months. Owing to their incorrect set points, two valves would not have closed tightly, if that had been necessary.

The incorrect adjustments of the valve actuators were detected on the basis of periodic tests carried out on 25 November 1997. During inspection it emerged that at both plant units some auxiliary sea water circuit valves with their actuators had been detached for the duration of piping work carried out during the annual maintenance outage. The actuators had not been detached from the valves but it may have been necessary to manually close the valves during the work and this may have shifted the set points. Due to this, altogether five valves at both units, which had been detached with their actuators in the annual maintenance outage, were checked. Of the checked valves, two were found to leak.

The leaking valves were of little safety significance. Owing to the unleaktightness of the one leaking valve, a small part of the water required to cool the reactor in the event of an accident would have been spent in the cooling of components less important to plant safety.

The function of the valves was not tested and checking of the adjustments of the actuators was not required before the start-up because the possibility to wrong adjustments was not recognised during the work planning. To prevent recurrence, the utility will include in the procedures the checking of the set points of valve actuators in case a valve has been detached from a pipeline and its actuator has not been detached.

Wrong relief pressure settings in the pressuriser pilot valves

During the outage (autumn 1997) pressuriser pilot valves (6 altogether) were calibrated with new testing device. In the periodical inspection of the pilot valve testing device in 20.3.1998 it was detected that it was calibrated for overpressure instead of absolute pressure leading to the fact that all pilot valves were set to open at 1 bar higher pressure.

Normal practise at the plant is that all pressure indications are absolute pressure. The device was ordered to be calibrated for absolute pressure but manufacturer delivered it calibrated for overpressure. During the delivery inspections and commission of the testing device pressures were misinterpreted because of an human error.

When ordering electrical transmitters and displays physical adjustment and display values should be defined unambiguous with corresponding electrical values and these should also be presented in installation documents.

Valve additional limits not set in the installation during the outage

In order to prevent boron dilution, a specific boron dilution protection automatics were installed at the plant in 1992. This included additional limit breakers for certain valves. Additional limits are needed in order to manually disconnect protection automatics if needed.

During the outage 1997 this type of valve and its actuator was in maintenance. During the installation of the valve the additional limit breakers were not connected. The reason for this was that the valve with additional limit breakers and the actuator are situated in different rooms and connected to each other with a long cardan shaft. When planning the post maintenance test the testing of the boron dilution protection automatics manual disconnection was not discovered.

The utility charted all valves and actuators that have additional limits and added additional limits in to the database for each valve and actuator so that they will be appear in working orders and related papers.

Incorrect safety system valve position

On 31 October 1997 one incorrect safety system valve position was observed at containment filtered venting system. It was detected when the state of valves important to safety was checked to ensure their correct position. The incorrect valve position was caused by human error when filling the containment with nitrogen after line-up checks during the start-up. It went unnoticed due to insufficient inspection routines related to the line-up of systems in which work has been done after start up.The shut-off valve that was in an incorrect position is in a by-pass line beside the check valve of the system main pipeline. The valve’s open position would not have had any effect on system operability.

According to analyses, back flow of air from the environment to the containment would have been possible through the open valve if containment pressure had suddenly decreased below normal atmospheric pressure. At this phase no hydrogen gas would have been left in the containment; thus, if the valve had been open, the containment function would not have been endangered in a potential accident.

The valve had been left open after work done in the 1997 annual maintenance. The valve had to be opened in connection with the work and it was not closed afterwards. Inaccurate observation of the operating instructions obviously contributed to the matter. The valve also was not part of the inspections made during plant unit start-up after annual maintenance to ensure valve normal state. Containment filtered venting system cannot not be tested so the importance of physical checks is high. As recommended by the working group set up to analyse the matter after the event, certain safety-significant valves were added to check lists that include inspections ensuring valve normal position. The utility has also established post start-up checks for the valves which position had been moved for some reason after the line-up checks.

Incorrect position of two diesel room dampers

On 19 August 1998 the dampers of suction air ducts of two back-up diesels were observed to be incorrectly open. The operation of the diesels could have been endangered in an unlikely situation caused by several simultaneous disturbances like fires.

The diesels are located in separate rooms. Atmospheric air is normally used for diesel operating air. The diesel suction air duct has a damper that can be opened to take operating air even from the diesel room should the use of atmospheric air be prevented. The damper automatically opens if the filter in the suction air duct for atmospheric air gets clogged up, for example due to fouling. The damper can also be controlled by a push button in the diesel room. Due to the damper's location, its position cannot be observed from the point of control.

During a diesel's periodic test the dampers were detected to be open. The positions of the dampers had been previously checked in the 1998 annual maintenance outages.

Correct damper position is vital in a situation where a diesel should start and the diesel room carbon dioxide system is simultaneously tripped, either inadvertently or to put out a fire. In such a case, carbon dioxide sucked from the diesel room into the diesel operating air would choke diesel operation. It is very unlikely, however, that such situations would simultaneously endanger the operation of more than one diesel. The function of the dampers had not been tested during the outage.

To ensure correct damper position, The utility has plans to fit dampers with signal lights to indicate their open or closed position. The lights would be clearly visible to the damper position control points in respective diesel rooms.

Inadvertently closed manually operated valves in the boron supply system

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 the unit by means of the two piston pumps on July 25, 1986, 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.

Erroneous removal of protections for two primary circuit make-up water pumps,

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, 1987, during a random check-up of instrument connections, that the high capacity make-up water pumps had almost all their protection signals switched off. 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 pressurisation of the primary circuit by the pumps might jeopardise 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.

Inoperability of the reactor pressure control valves

The reactor overpressure protection and pressure control system comprised ten relief valves and two quick-opening and control valves.

A turbine trip occurred on October 6, 1987, 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 pressure control system valves and the transfer of reactor pressure control to the control valves of the pressure control 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 plants 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.

Faulty states of the primary shut-oft valves of the impulse lines of certain pressure measurements of the plant protection system

It was noted on June 14, 1988, 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 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.

Unsatisfactory functioning of the check valve of the discharge line of an emergency core cooling system

During the annual maintenance a discharge test of a pressurised water tank of the emergency core cooling system was performed on August 21, 1991. 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 pressurised 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 other tanks. 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.

Inoperability of the fire extinguishing system of the containment inner intermediate ring

A periodic inspection of the fire extinguishing system of the reactor containment inner intermediate ring was performed on 27 October, 1992. Water flow from the system and fire hydrants was observed to be non-existent. 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, 1991, 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.

Shut-down service water system reliability was impaired

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 shutdown 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 backflushing 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 both plant units. 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.

France

Generic design fault in the installation of low-level sensors in containment spray system

During draining of the spray additive tank associated with the containment spray system (EAS) in unit 4 of the Cattenom nuclear power plant, to allow maintenance work to be carried out on a mixing pump, the low-level alarm in the spray additive tank failed to trip. This alarm initiates isolation of the spray additive tank from the rest of the EAS system. In the event of an accident requiring actuation of the containment spray system, there would be a potential risk to safety in that failure of the low-level alarm to trip could lead to damage to the EAS pumps as a result of air being entrained from the spray additive tank once the latter had been emptied.

This malfunction was attributable to the design of the bottom instrument tap connection for the level detector column, which creates a trap for a residual amount of sodium hydroxide. The presence of this residual volume of sodium hydroxide prevents the low-level sensor from generating the signal indicating that the tank is empty which is used to initiate isolation of the tank.

This design fault proved to be generic and thus common to all 1300 MWe reactor units. It had remained undetected during both start-up and periodic tests due to the fact that such tests consist simply in simulating a low level in the tank by isolating the tank from level-sensing instrumentation lines. As a result, the fault was only discovered once the tank had actually been drained.

All spray additive tanks in 1300 MWe units have therefore been modified by raising the low-level setpoint to a level that will ensure generation of a trip signal. This modification does not involve any change in the volume of sodium hydroxide injected into the EAS system.

The main lesson learned from this fault is the need to establish whether tests are properly representative. In cases where standard operating conditions cannot be reproduced during a test, a careful assessment must be made of the differences between standard and test conditions, and measures drawn up to compensate for such differences.

Tricastin 2, March 1993 : Lubricant anomaly of safety-related valve servomotors

Non-opening of a valve from the injection system during a surveillance test revealed a lubrication defect in the servomotor which resulted in deterioration of the wheel/worm screw system. The origin of the defect lay in the fact that servicing sheets mentioned a level of lubricant to be injected into the wheel/worm screw system housing, instead of the quantity of lubricant required by the vendor. Taking into account the common cause aspect of the anomaly which involved a large number of safety-related valves equipped with these servomotors, internal inspections of the valves were carried out. The task was made much easier in analysing records available or performed after inspections

using the valve functioning diagnosis aid device (SAMIR). These inspections led to lubricant addition, as well as several servomotor preventive replacement. The vendor was requested to perform further assessment regarding valve behaviour and wheel/worm screw system degradation resulting from both a lack of lubricant and number of actuations.

Tricastin 1, august 1990 : Installation anomalies in the containment decompression

A test carried out during pressure testing of the containment at Tricastin unit 1 revealed that the orifice plates in the reactor building decompression system for units 1 and 2 had not been properly installed. This system had been installed in all PWR units in France and is designed to reduce pressure in the reactor building in the event of an accident. This anomaly meant that the line connecting the sand-bed filter to the reactor building had been closed off.

Inspections carried out at all nuclear plants in France revealed similar anomalies at five other units. Remedial action was taken immediately. In the event of an accident, the anomalies detected would either have precluded use of the filter or would have resulted in the filter being used under abnormal conditions. The causes of the anomaly were a failure to comply with quality assurance rules, particularly during end of installation inspections, and the fact that no functional tests had been performed on the system.

Nogent 1, January 1999 : Overcurrent protection of essential service water pumps and charging pump

A trip was caused by overcurrent protection systems of 2 Essential Service Water System pumps and the charging pumps train A, during houseload operation tests. The automatic switchover to train B was successful.

After investigation, it was found that all the protection systems of the 6.6 kV actuators supplied by the AC Emergency Supplied Distribution System train A were incorrectly adjusted (between 5 and 33% below the lower threshold) subsequently to maintenance work during outage. The faults were revealed by the high frequency of the electrical power supply during houseload operation (52 Hz).

The causes were : an error of adjustment and checking operations, an incorrect application of the worksheet, a lack of traceability, a inadequate second-line checking and a inadequate requalification.

The risk of common mode failure leading to loss of safety injection, thus core melting down is very high (approximatively 5 E-3).

The lessons learned from this event is one must consider many lines of defence : quality of work (preparation, planning, questionning attitude) and carrying out alternately the maintenance work on redundant systems.

Germany

Example for rescheduling

During a review of the start-up procedure it was discovered that the check for the sump availability was performed in a plant mode, where the sump suction should be operable. During outage the sump is covered to prevent intrusion of foreign material into the sump and the sump suction lines. The covers are removed at the beginning of the start-up. The prescribed check whether the covers had been removed was scheduled at a later period. At this time the reactor was already in hot stand-by mode. In this mode of operation the sump suction has to be operable to control LOCA events. As a result of the procedure review the check of the sump availability was rescheduled to a mode of operation before the sump suction operability is necessary.

Example for an incident where tests cannot be performed in the same manner like real demand

Due to a failure in the measured value logging of the AC-voltage control a safety related rectifier was shut off. The supply of the respective DC-busbar was uninterruptedly performed by a battery. In accordance with the design, the rotating transformer was coupled off automatically from the DC-busbar to save battery capacity. The supply was switched over to the 380-V emergency power busbar of the neighbouring redundancy. At this time the earth fault alarm of the DC 220-V-busbar was triggered caused by a faulty earth fault alarm relay. There was no switching action made due to the alarm. The cause of the relay fault was a misadjustment in the compensation of the relay. The adjustment operation was performed during the last refuelling outage after replacement of the relay. The correct adjustment cannot be checked after the replacement or by in-service inspections.

Example for deficiencies in the evaluation of maintenance recordings

During a pressure transient in a BWR, all safety and relief valves opened and closed properly but the evaluation of the event showed several irregularities, especially the limitation of the valve stroke of three of these valves. The subsequent analysis revealed the deformation of central pivots caused by ignition of radiolysis gases.

For the three valves, reductions of the stroke of 12 mm, 8 mm and 6,5 mm were determined due the deformation of the central pivot. During subsequent tests one valve, which was actuated via a pilot valve that had not been actuated during the transient, showed also the irregular stroke described above. Such behaviour was also observed on another valve during the valve tests in the previous year. But the subsequent inspection of this valve had indicated no abnormalities. The irregularities in the maintenance records did not trigger a detailed investigation at that time. About half a year before this event, a similar event occurred in another NPP with one safety and relief valve stuck open during test. The

event analysis revealed that the failure mechanism was the ignition of radiolysis gases while opening of the pilot valves.

Hungary

Simultaneous unavailability of 2 auxiliary emergency feedwater pumps

As one of the highest priority safety upgrading measures, the relocation of the 2 auxiliary emergency feedwater pumps and the related pipelines from the turbine hall to the reactor building was carried out on Unit 1 during the 1997 refuelling outage (similar modifications made to Unit 2 in 1996). The system was tested and declared operable. However, during the next few days during unit start-up when a different test was being carried out, the auxiliary feedwater pumps tripped several times. However, every time the troubleshooting and the corrective action taken seemed to give satisfactory results. The post-maintenance start-ups right after the repairs were successful. The pump trip occurred again a few days later when the next test was performed.

On June 13, during the load sequencer test, the related auxiliary emergency feedwater pump tripped right after startup. The other stand-by pump was tested immediately, but it tripped too. In accordance with the technical specifications that require bringing the unit to cold shutdown conditions in case of unavailability of both auxiliary feedwater systems, the operators started to cool the unit down.

Troubleshooting was immediately started. The pumps providing cooling water for the emergency feedwater pump bearings, the flow switch devices and the auxiliary emergency feedwater was thoroughly inspected and started up several times. This time the failure could be replicated. The pump protection is enabled when the pressure in the system is higher than 55 bar. It took 1-2 seconds to have this pressure build-up following pump start-up. A similar amount of time was required to reach the necessary cooling water flow. In some cases the pump protection had been enabled before the cooling water flow reached the required value, therefore tripping the pump shortly after start-up.

As a consequence of the event, degradation of the heat removal safety function occurred because both auxiliary emergency feedwater pumps became unavailable. The significance of the event increased by the fact that the unavailability was caused by common mode failure and both trains of the auxiliary emergency feedwater system were unable to perform automatic start-up on demand.

Unavailability of STARO-ETA UPS units

In the area of electrical power supply, action has been taken to increase the reliability of household electrical power supply systems. Due to the ageing of materials used in the internal electronic devices in the originally installed uninterruptible power supply (UPS) units (irreversible motor generators) their replacement by the new STARO-ETA system was started in 1993. There are four UPS systems in each unit, 3 for the safety

trains and one for the non-safety related loads requiring a UPS. First the non-safety related units were replaced with STARO-ETA UPS equipment. After having positive operating experience of the newly equipment, the replacement of the safety-related UPS units was also started. Up to now at PAKS NPP, 12 out of the 16 UPS units have been replaced.

Several operational events have occurred recently at PAKS NPP caused by the failure of newly installed STARO-ETA UPS units. Mains voltage and frequency transients led to tripping of the UPS units and disturbances in the power supply system. The problems caused deviations from normal operation conditions and the required actions specified in the technical specifications being taken.

The STARO-ETA system was developed especially for UPS. The words STARO and ETA are German abbreviations used for this particular type of equipment. In both STARO and ETA operating modes the generator supplies its consumers with constant voltage.

The event led to operational conditions which did not meet the criteria defined in the technical specifications. The actions required were taken immediately every time, thus technical specifications violation did not happened. As a result of the events, several unplanned tests requiring diesel generator start-up have had to be run.

Jamming of journals in the essential service water system

The AP-250 KMNW type journals were installed in the essential service water system on Units 2 and 3. On 9 October 1996, during an interlock test on Unit 3, jamming of a newly installed journal was discovered. Afterwards, when the journal was inspected, it was concluded that the jamming had been caused be hardening of the material used for packing and lubrication. However, further testing in the laboratory could not replicate the phenomenon of hardening. Following this event, all the installed journals were tested and another one on Unit 2 was also found to be inoperable. After dismantling, it was revealed that deformation of the casing caused by incorrect installation led to jamming.

The jamming of the journals in the essential service water system resulted in degradation of the heat removal function, because the necessary cooling water for the emergency core cooling system heat exchangers could not be provided.

Sweden

Erroneous safety system status control after outage

Between 1995 and 1998 nine different events with partly the same root causes have been identified. All of the events involve safety components erroneously left inoperable after an outage. The nine events are from seven different Nuclear Power Plant Units in Sweden. Five are BWR units and two are PWR units.

Involved Plants in order of appearance:

Plant	Type	Power (MWe)	Start of Operation
Forsmark 2	BWR	1006	1981
Barsebaeck 2	BWR	615	1977
Forsmark 1	BWR	1006	1980
Oskarshamn 2 (2 events)	BWR	630	1975
Ringhals 2	PWR	917	1975
Ringhals 4	PWR	960	1983
Oskarshamn 1(2 events)	BWR	465	1972

Approximately once a year the plants go in to a refueling outage with extensive additional maintenance work. Various tests and verifications then precede the startup in order to ensure the plants operability for the coming power operation. These tests are guided by overall work orders and system and functional specific procedures. It is a complex work that due to different maintenance tasks has to be performed in somewhat different order one year to another. When a system is verified operable it is sometimes necessary to make it inoperable again in order to verify the operability of other systems without undesired initiation of safety functions. Additional maintenance tasks due to revealed faults or weaknesses can call for re-planning and re-scheduling of tests.

In between the refueling outages there can be other planned or unplanned outage due to problems with components where there is a risk for or an actual violation of the Technical Specifications. When an event calls for a short outage there is always an updated list with additional maintenance work that is useful to get done during the outage. Even a short outage often means that several different maintenance tasks will be performed.

The events described below are of different safety significance but they all illustrate problems regarding operability control of standby systems or components :

- Valves in the Containment Pressure Relief systems erroneously closed (July 1995 at Forsmark 2)
- Erroneously left open valve caused degraded containment pressure suppression function (June 1996 at Barsebaeck 2)
- Valves in the Containment Pressure Relief systems erroneously closed (July 1996 at Forsmark 1)
- Erroneously left open Disconnecting Switch caused inoperability in the Low Pressure Core Spray System (November 1996 at Oskarshamn 2)
- Steady State Protection System erroneously left inoperable (August 1997 at Ringhals 2)

- Valves in the Containment Spray System erroneously closed (September 1997 at Ringhals 4)
- Valves in the Containment Pressure Relief systems erroneously closed (October 1997 at Oskarshamn 1)
- Valve in the Residual Heat Removal System erroneously left inoperable (August 1998 at Oskarshamn 2)
- Valves in the Standby Liquid Control system erroneously left inoperable (October 1998 at Oskarshamn 1)

There are general weaknesses in administrative processes. The routine as how to act in case a procedure is shown to be inadequate in a specific unforeseen situation has often been too weak. Insufficiently controlled maintenance has sometimes been performed in systems that have already been declared operable. This along with the logistic problems of operability tests has caused some of the events. The routines for re-planning during an outage have sometimes been significantly weaker than the original planning routine.

There have been weaknesses in management. Management has sometimes not been aware of the full impact of poor procedural routines. Management has not always realized the safety significance of supervision and follow up on deviation in human performance. When things are going well it might be difficult to maintain and boost understanding of the importance of maintaining barriers and the defense in depth strategy. But, by not doing so management will ensure that things will not go well in the future. It is important that people are encouraged to maintain the safety first focus at all times.

There have been weaknesses in human performance. In several cases there have been a reliance on earlier closed out procedures or anticipated procedural steps without adequately checking that procedures have been closed out correctly or that future procedural steps actually cover the anticipated actions. A common root cause has been time pressure. Enough time is always a strict condition for success. Lack of time on the other hand is a guarantee for mistakes and failure.

There are weaknesses in the control room layout. The control room layout and the instrumentation do sometimes not give the operators enough information on the operability of systems and components. Control rooms are typically designed for operation and not for outage or the transition between outage and full operation. This contributes to peoples difficulties in creating a mental overview of the plant's operability.

Isolation condenser blocked after reactor scram - Oskarshamn 1

The auxiliary condenser system consists of a condenser placed beneath the main steam lines near the reactor pressure vessel (outside containment). From the main steam lines, two steam lines are connected to the condenser. On the outlet side, two pipes with one control valve and one isolation valve in each line, lead the water back to the reactor pressure vessel, via the recirculation loops. Normally the isolation valves from the

auxiliary condenser open on scram signal and the two control valves from the auxiliary condenser adopt reactor pressure control. The auxiliary condenser adds capacity and diversity to the reactor pressure relief system. On January 21, a reactor scram with steam dump block occurred. On this occasion, two high temperature signals from the auxiliary condenser was obtained after six seconds and shortly afterwards the isolation valves from the condenser unexpectedly closed. Reactor pressure control automatically switched over to the pressure relief system and steam was blown down to the condensation pool. When the high flow alarm was cleared in the control room, the isolation valves opened again and reactor pressure was re-routed to the auxiliary condenser. The available systems for residual heat removal from the reactor was reduced as both the turbine condenser and the auxiliary condenser were unavailable.

The temperature switches were redesigned so that they would actuate when deenergised. The cause of closure of the isolation valves from the isolation condenser was that the two temperature switches, that actuated after the scram, were set to actuate when energised (working current) instead of deenergised. Thereby the logic to the valves were supplied with false signals.

The old temperature switches were replaced with new ones. The new ones were incorrectly designed resulting in that the switches actuated when they were energised instead of when deenergised. The mistake in design was not discovered during the verification tests as these tests only included partial testing of the signals, not the complete signal chain. Because of the mistake in design and the insufficient verification of the new design, the event was classified as Level 1 on the INES.

Feedwater logic design - Oskarshamn 1

When, in 1995, an emergency operating scenario sequence was run on KSU's Orkarshamn 1 simulator, a logic error was detected for the outboard feedwater isolation valve. The valve received a closure signal only during the first 10 seconds after containment isolation following a steam feedwater line break. This was on condition that the reactor power, at the same time, was less than 35% and that the valve was in the automatic operation mode. The malfunction was introduced in 1989 when the feedwater controller was replaced. Afterwards, no test was carried out with the valve in the automatic operating mode. The logic was modified.

USA

IN 93-13 Undetected modification of flow characteristics in the high pressure safety injection system

On September 23, 1992, with Unit 2 shut down, Energy Operations, Inc. (the licensee) evaluated flow imbalances that were found during testing of the high pressure safety injection (HPSI) system. The licensee determined that the flow rates through five of the system valves were less than required. Because of the low flow rates, the licensee

concluded that the sum of the flow rates of the three injection paths with the lowest flow rates was less than that assumed in the plant design basis calculations which support the plant safety analysis.

The licensee investigated the event and determined that replacement stem disc assemblies, supplied as "like for like" and installed as early as 1982, were not identical to the original assemblies. Subsequent to the event, the licensee had the vendor rework spare valve discs to meet the design requirements and installed these in the five affected valves. The licensee then conducted flow balance testing to ensure that all system flow requirements were met.

The technical specifications for ANO Unit 2, require flow balance testing after system modifications which could affect flow characteristics, but do not require periodic flow balance testing. The licensee did not recognise that the replacement stem disc assemblies were different from the original stem disc assemblies and, therefore, did not test the system after changing the components.

The licensee discovered the flow imbalances and degraded flow rates during a full flow test performed in response to Generic Letter 89-04, "Guidance on Developing Acceptable In service Testing Programs." During this test, the total indicated flow was found to be lower than the actual flow. After investigation, the difference was found to have been caused by a flow orifice that had been installed backwards. While investigating the problem, the licensee determined the actual system flow by isolating the hot leg injection paths and summing the indicated flows of the four cold leg injection paths. From these measurements, the licensee found that the flows varied greatly. The large variation in indicated flows of the cold leg injection paths led the licensee to find the improper discs.

Although the individual loop flows varied greatly, the total flow of the system met the acceptance criteria. Performing full flow testing alone would not have caused the licensee to find the degraded flow in parts of the system. Therefore, the flow imbalances might have remained undetected if the flow orifice had been installed correctly and investigation of the flow orifice problem not been required.

The licensee reviewed the technical specifications for similar surveillance test requirements. The licensee then evaluated the similar tests to determine whether they were adequate to fully test the system and were required to be performed at appropriate times. Upon completing this review and another review to find systems with similar valves, the licensee performed flow balance testing on the low pressure safety injection system with satisfactory results. The licensee revised the HPSI flow testing procedure to provide for confirmation of satisfactory flow balance and capacity during each refuelling outage.

IN 93-63 Improper use of soluble weld purge dam material

On May 1, 1993 at 1215 CDT, Unit 1 was nearing the end of a refuelling outage in the Cold Shutdown mode with all control rods fully inserted. Reactor pressure was at approximately 100 psig, and reactor coolant temperature was at approximately 145

degrees Fahrenheit and increasing in preparation for the ASME XI Class 1 System Leakage Test. At that time a full Reactor Protection System actuation signal was received on a low water level signal. The low water level signal also produced a trip signal to several Group 2 Primary Containment Isolation System (PCIS) valves, per design. Licensed Operations personnel verified that actual reactor water level was not low by comparing instrumentation. Two unsuccessful attempts were made to correct the condition by filling the affected instruments' variable sensing line and performing various instrument valve manipulations. When these efforts proved unsuccessful, Instrument and Control technicians filled and vented the reference line of the affected instrumentation. While using a manual hydrostatic test pump to fill the reference line, some resistance to flow was encountered, indicating the line was partially plugged. Further pressurization, however, cleared the obstruction. The investigation showed that the most likely cause of the blockage was soluble weld purge dam material that had not been used properly during a modification of the piping associated with the "B" channel condensing chamber. The modification required cutting out and then rewelding sections of the reference-leg piping. To complete this work, a temporary plug had been installed in the associated reactor vessel penetration, but did not provide a completely watertight seal. To perform a dry weld on the reference leg, the soluble weld purge dam material was used to plug the reference leg near the weld location. The welders rolled the material into a plug several inches long and forced it into the 2.5 centimetre [1-inch] diameter reference-leg piping.

The soluble weld purge dam material is Dissolvo WLD-35, but is frequently called rice paper. It is intended to contain or dam weld purge gas inside piping at a weld location. Once the weld is completed, the piping is filled with water and the paper is supposed to dissolve completely. Plant managers at Hatch consider the use of the material to absorb small quantities of water an acceptable welding practice. A licensee event review team concluded that the rice paper had not dissolved completely because air was trapped on the downstream side of the roll, which prevented the paper from becoming saturated. Testing with models of similar piping arrangements and material showed that significant periods of time could elapse before the material dissolved completely. Dissolution of the paper is dependent on sufficient exposure to water, and large accumulations of tightly packed rice paper could prevent the paper from dissolving completely. Testing suggests that the length of a plug of the material should be limited to less than 2.5 centimetres [1 inch]. When contacted, the vendor for the material confirmed that the length of the material should not be more than one pipe diameter to ensure that it dissolves completely. The licensee initiated corrective actions, including requirements for post-maintenance functional testing to ensure that the material has dissolved completely whenever it is used to plug piping. Training will be conducted to provide guidance on the appropriate quantity of material to use in such applications.

The event described above serves to highlight the potential consequences of improper use of soluble weld purge dam material. Failure to provide adequate instructions to workers and inadequate post-maintenance functional testing can result in blockage of piping and inoperability of systems.

IN 93-76 Inoperable emergency diesel generator caused by painting

On January 20, 1993, Unit 1 was in Mode 1 at 95% power. Standby Diesel Generator 13 failed to start during a monthly surveillance, 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. The primary cause of this event was lack of application of proper work process controls. The applicable painting procedure was inadequate, in that mandatory, in-process controls and maintenance tests were not required when painting safety-related components. An inappropriate decision to delete the PMT was made and the added precautions were inadequate. Additionally, the pre-job briefing was inadequate. A contributing cause was inadequate implementation of lessons learned from industry operating experience. Although previous industry events of a similar nature had been reviewed as part of the station Operating Experience Review Program, the personnel involved in the painting were not fully cognisant of this experience and controls were insufficient to ensure cited corrective actions were implemented. Other contributing causes were inadequate verbal communications which led to a lack of clearly defined responsibility for ensuring paint was not applied inappropriately.

The events described above demonstrate that even apparently benign actions such as cleaning and painting may have consequences that are detrimental to safety, and that personnel are not always adequately aware of the potential effects of such actions on the safety functions of safety-related equipment.

LER 93-012 Emergency diesel generator sequencer circuit deficiencies

On November 4, 1993, a test to verify the automatic loading capability, on a Safety Injection Signal (SIS), for the 2-1 Emergency Diesel Generator (EDG) failed. The Unit was in Cold Shutdown at the time of the testing. The test verifies that all loads will deenergise on the respective safety-related emergency busses and that the EDG sequencer circuitry will automatically load safety-related loads at specified time intervals, following starting of the EDG. On November 6, 1993, the 2-2 EDG also failed its respective test for automatic loading capability. This event constituted a common mode failure which could have safety implications during an event involving a loss of offsite power and safety injection actuation. Operator action may have been required to manually sequence Emergency Diesel Generator loads.

The cause for the emergency diesel generator (EDG) failures was identified as inadequate design understanding prior to implementation, and insufficient post modification testing following the installation of the digital (microprocessor based) solid state timers. The design changes were made to the EDG Load Sequencers during the Second Refuelling Outage and also following digital solid state timer circuit modifications performed during the Third Refuelling Outage. The testing conducted did not adequately validate the design change from electromechanical to microprocessor based solid state timers. An inductive voltage surge was produced by the deenergization of auxiliary relays within the load sequencer circuitry which caused the solid state timer to misoperate. The timer relays

are Automatic Timing & Controls Company, Model 365-A, Long Range Timers. These timers were recommended by the manufacturer as direct replacements for the original electomechanical timers, where improved timing accuracy is desired.

IN 97-52 Inadvertent loss of capability for emergency core cooling system motors

An investigation of temperature differences between the Unit 1 safety injection pump (SIP) B motor coolers discovered that the motor cooling for this pump had been significantly degraded due to improper gasket installation and incorrect assembly of the motor coolers. On November 1 1996, design engineering personnel completed an evaluation and were able to determine that SIP B would not be able to perform its intended safety function. Therefore, the unit had operated in a condition prohibited by the Technical Specifications because both SIPs are required to be in service when the unit is in Modes 1, 2, or 3.

On November 6, 1996, a review was completed that found occasions when SIP A was out of service and SIP B was relied on to perform the safety injection function. Therefore, an unanalysed condition had existed, when SIP A was out of service, that significantly compromised plant safety. The NRC Operations Centre was notified.

The analysis of event have showed there was no significant adverse effect on plant safety or on the health and safety of the public as a result of this event.

The causes of this event were improper gasket installation and inadequate procedural guidance resulting in incorrect assembly of the motor coolers. A review of work orders determined that the as-found motor cooler assemblies' configurations had been in place at least since 1991, and possibly since original construction. In addition, no specific functional testing of heat exchangers had been performed which could have identified the installation errors.