REPORT ON THE USE OF
PROBABILISTIC SAFETY ASSESSMENT
FOR NUCLEAR POWER PLANT SAFETY MANAGEMENT

(UTILITIES' REPLY TO A QUESTIONNAIRE)

Prepared by Experts from
Principal Working Group No.5
of the
NEA Committee on the Safety of Nuclear Installations

NOVEMBER, 1989

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY
38, bulevard Suchet, 75016 Paris, France
The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers who have responsibilities for nuclear safety research and nuclear licensing. The Committee was set up in 1973 to develop and co-ordinate the Nuclear Energy Agency's work in nuclear safety matters, replacing the former Committee on Reactor Safety Technology (CREST) with its more limited scope.

The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries. This is done in a number of ways. Full use is made of the traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences. Some of these arrangements are of immediate benefit to Member countries, for example by enriching the data base available to national regulatory authorities and to the scientific community at large. Other questions may be taken up by the Committee itself, with the aim of achieving an international consensus wherever possible. The traditional approach to co-operation is increasingly being reinforced by the creation of co-operative (international) research projects, such as PISC and LOFT, and by a novel form of collaboration known as the international standard problem exercise, for testing the performance of computer codes, test methods, etc. used in safety assessments. These exercises are now being conducted in most sectors of the nuclear safety programme.

The greater part of the CSNI co-operative programme is concerned with safety technology for water reactors. The principal areas covered are operating experience and the human factor, reactor system response during abnormal transients, various aspects of primary circuit integrity, the phenomenology of radioactive releases in reactor accidents, and risk assessment. The Committee also studies the safety of the fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on power plant incidents.

* * * * * *

A "Restricted" OECD document should not be communicated except for official purposes. The Secretariat and Member governments of the OECD are requested to take the necessary action to ensure the security of these documents.

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

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

Nuclear Safety Division
OECD Nuclear Energy Agency
38 boulevard Suchet
F-75016 Paris
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>3</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>7</td>
</tr>
<tr>
<td>2. Purpose and Structure of the Questionnaire</td>
<td>8</td>
</tr>
<tr>
<td>3. List of Questions</td>
<td>9</td>
</tr>
<tr>
<td>4. List of Utilities that have responded to the Questionnaire</td>
<td>12</td>
</tr>
<tr>
<td>5. Results of the Questionnaire</td>
<td>13</td>
</tr>
</tbody>
</table>

**Appendix:** Summarised Responses by Utilities to the Questionnaire

(Page 21 - 78)
SAFETY MANAGEMENT TASKS:

- Supervision of the actual safety or risk level of a plant during its lifetime, based on the initial plant layout (for this purpose, plant-specific PSA can be used, e.g., to compare reliability parameters of safety systems with actual plant parameters).

- Evaluation of any modifications, either planned or compelling, through plant experience (for this purpose, PSA should be reevaluated for assessing system modifications).

Purpose of Questionnaire:

- Description of the state-of-the-art indicating the extent to which the plant safety management makes use of PSA techniques;

- Description of the extent to which PSA assumptions and results are implemented into plant safety regulations, e.g., technical specifications (TS);

- Exchange of experience between Utilities responding to the Questionnaire on the use of PSA as an aid to safety management.

Member countries which have responded to the Questionnaire:

Canada
Finland
Federal Republic of Germany
Japan
Spain
Sweden
United Kingdom
United States of America
Structure of Questionnaire:

In order to obtain broad information on different types of PSA application in plant management systems, the Questionnaire was structured in accordance with various types of safety management tasks:

a. **Plant shut-down during plant operation**, due to component failure in safety systems;

b. **Plant start-up** after scheduled revisions or after an abnormal plant shut-down, for checking if all safety systems are intact;

c. **Safeguarding maintenance activities**: organisation of maintenance, protection safeguarding by maintenance of the system and its surroundings, system commissioning after maintenance, including adequate system test;

d. **Safety-relevant system modification**: such as change of hardware or of procedures;

e. **Operator response to abnormal events**: such as transients and component failures;

f. **Use of data feedback** and reviewing the efficiency of quality assurance (QA);

g. **Surveillance test procedures** of safety systems and components;

h. **Preventive maintenance** for reliability assurance.

Various questions were formulated for each point so as to obtain specific answers in accordance with the above task definitions.
RESULTS OF QUESTIONNAIRE:

Technical Specification and Allowed Outage Times (AOT):

Safety requirements on plant operation, necessary for plant shut-down, are written in TS and mainly focussed on AOT. Examples of AOT of safety systems are given from various plants within the range of 1h to 30 days, should one sub-system not be available. The numbers depend mainly on the degree of redundancy and the importance of the systems. Generally, AOT were assessed by engineering judgement and supported or changed by PSA if it was considered to be excessively conservative. Actual experience on plant shut-down caused by AOT showed that these events are rare (e.g., 10^{-1} - 10^{-2} per plant year).

Data Feedback:

National data banks on component reliability data are in use or planned in various countries. The actual component failure rates are compared against expected failure rates (e.g., based on previous PSA and to be used for living PSA). The data feedback are also used for plant supervision, revealing weak points and improving plant safety and availability.

Surveillance Test Procedures:

Testing frequency is generally based on engineering judgement. PSA is increasingly used for verifying testing frequencies. These assessments result in the increase or decrease of testing frequencies.

Preventive Maintenance (PM):

PM is based on engineering judgement, plant experience (also from other plants), recommendations of component manufacturers and eventually on component reliability data, e.g., by an actual increase of component failure frequency.

PM intervals for safety-important components (pumps and valves) are given within a range of 4 to 10 years.
CONCLUSIONS:

According to the replies from the Utilities, the application of PSA technique to plant safety management varies with the type of their plant.

Those Utilities which are familiar with the PSA technique and have their plant-specific PSA available have already made extensive use of this technique, e.g. to set priorities on back-fitting measures and to optimise plant modifications.

There has also been an increase in the use of data banks to assess reliability data and to review current plant experience, with national plant-specific data banks set up for this purpose. In accordance with this development, the use of living PSA has increased in various Member countries.

Plant-specific reliability data are used to optimise testing procedures and the allowed outage time for the preventive maintenance of safety components. Apart from these, quality assurance for maintenance and test procedures are thought important for maintaining system reliability. It is also thought important to supervise plant parameters and the states of systems and components.

Extended knowledge of plant engineers is considered essential for the increased application of PSA technique to plant management. Such knowledge could possibly be extended, for example, by integrating those engineers into the process of PSA and by using systems collecting reliability data. There are, in fact, ongoing research projects developing computer systems to use PSA technique for plant management.

The present exercise, an exchange of experience by the use of the Questionnaire, could also contribute to the extension of knowledge on the use of PSA.
1. INTRODUCTION:

Up to now, probabilistic safety assessment (PSA) has been used in NPP safety systems for improving system lay-out and for optimising operational systems and surveillance test procedures.

Such a plant-specific PSA describes the safety or risk level of a plant and may also be used by NPP Safety Managements as a supporting means for their safety decisions. The latter application, however, is not yet as well developed and used as the former one.

When using PSA for plant management tasks, we have to bear in mind that probabilistic analyses are based on a fixed set of assumptions of systems build-up and conditions, surveillance test procedures and probabilistic input data.

Because of these assumptions, deviations or modifications of a system or of input parameters are not covered by an already completed PSA.

Against this background, plant safety management tasks - when supported and guided by PSA techniques - can be divided into two categories and defined as follows:

a. Supervision of the actual safety or risk level of a plant over its lifetime, based on the initial plant layout (for this purpose, plant-specific PSA can be used, e.g. to compare reliability parameters of safety systems with actual plant parameters. This job is called reliability assurance. Furthermore, for identification of safety-important parameters and supervising them against any deviations).

b. Evaluation of any modification, either planned or compulsive, through plant experience (for this purpose, PSA should be reevaluated for assessing system modifications).

In practice, plant safety management decisions are based on:

- engineering judgement
- safety design principles and
- (for special tasks) PSA methods.

Because of the diversity and complexity of the management decision making process and the different experiences with PSA from plant to plant and from country to country, the methods available to aid management decisions will of course differ from plant to plant. It is for this reason that the Questionnaire to Utilities has been established, i.e., to describe the state-of-the-art of the present system in respect of safety-relevant decisions and in how far they use PSA in this context.
2. PURPOSE AND STRUCTURE OF THE QUESTIONNAIRE:

The purpose of the Questionnaire covers the following points:

- description of the state-of-the-art indicating the extent to which the plant safety management makes use of PSA techniques;
- description of the extent to which PSA assumptions and results are implemented into plant safety regulations, e.g. technical specifications (TS);
- exchange of experience between utilities responding to the Questionnaire on the use of PSA as an aid to safety management.

So as to obtain broad information on different types of PSA application in plant management systems, the Questionnaire was structured according to different types of safety management tasks:

a. Plant shut-down during plant operation, due to component failure in safety systems;

b. Plant start-up after scheduled revisions or after an abnormal plant shut down, for checking if all safety systems are in an intact state;

c. Safeguarding maintenance activities: organisation of maintenance, protection safeguarding by maintenance of the system and its surroundings, system release after maintenance including sufficient system tests;

d. Safety-relevant system modification: such as change of hardware or of procedures;

e. Operator response to abnormal events: such as transients and component failures;

f. Use of data feedback and reviewing the efficiency of quality assurance (QA);

g. Surveillance test procedures of safety systems and components;

h. Preventive maintenance for reliability assurance.

Various questions were formulated for each point so as to get specific answers in accordance with the above task definitions. The questions are listed in Chapter 3.

The Utilities were requested to state their answers in a short form and, where useful, supplement them by typical examples.

The Utilities which responded to the Questionnaire are listed in Chapter 4.

A summary of the answers received from them is contained in Chapter 5.

The detailed answers from the Utilities are compiled for each question and appended to this report. Similar answers have been linked together where possible.
LIST OF QUESTIONS:

3.1 Plant shutdown during plant operation:

a) What plant-specific document contains the safety requirements necessary for plant shutdown?

b) What kinds of requirements are given? Are such requirements based on PSA of plant systems?

c) Give typical examples of allowed outage times (AOT).

d) Are all safety relevant components regulated by AOT or only by representative components? How are these components defined with respect to their sub-systems? Are safety relevant components determined by PSA?

e) What is the base of AOT assessment, e.g. PSA or engineering judgement?

f) Are there additional regulations for other plant conditions, such as during plant shutdown phases due to heat removal from the fuel elements, or containment isolation? Do you use PSA for distinguishing different risk levels of plant operation or plant systems?

g) What is the actual plant experience on plant shutdown caused by AOT? Is there a need for optimising AOT, e.g. by PSA?

h) Are there special requirements for occasions of common mode failures (CMF)? Are these requirements based on or supported by PSA?

3.2 Plant start-up:

a) What kinds of requirements are given? Are the yearly plant start-up after revision coupled with a completely intact safety system (with a system reliability of 1)?

b) Are the same AOT given as in point 3.1?

c) Are the same requirements formulated on plant start-up for after-revision-phase and for after an abnormal event?

d) Are there special requirements for checking the workability of safety features after an abnormal event or transient, e.g., to detect unrevealed system failures?

3.3 Maintenance activities:

a) What are the maintenance safety regulations, e.g. to prevent component unavailability of different redundancies or excessive system leakage?

b) In which way are maintenance procedures formulated, e.g. by standard formats of work order reports? Are the safety regulations and checks for QA integrated?
c) What are the safety regulations on the operational position of valves and on the use of blocking devices during maintenance, e.g. to prevent CMF caused by human error?

d) What are the regulations on how to check (test) the component or system function after maintenance, e.g. to indicate sufficient system reliability?

e) Regarding the above points, what do the documents of maintenance and repair reports look like, e.g. for QA and for evaluating component experience purpose?

3.4 Safety relevant system modifications:

a) What are the main reasons for system modification, e.g. plant experience, experience from PSA/PRA-Studies, accident management?

b) How are maintenance and system or component changes distinguished, e.g. for indicating a new system or component state?

c) What are the criteria for obtaining permission for a system modification and are there any special regulations concerning this topic? Give examples. Do you perform a PSA-re-evaluation of system modification?

d) How far are safety systems operations regulated by plant manuals and how far can these be deviated? Do you check this modification by PSA?

3.5 Operator response to abnormal events:

a) What is the minimum response time for an operator to fulfil a task during an abnormal event, based on:

- formal design criteria
- practical experience

Give examples of the above.

Under what circumstances should an operator task be given credit in safety analysis, e.g. PSA?

b) How do you train for these tasks and what are the tools used, e.g. accident sequence diagrams?

c) Do you use reliability diagrams, such as fault trees, to aid understanding of the accident sequence and different system interactions?

3.6 Use of data feedback:

a) How are test and repair reports used when updating plant experience, e.g. for plant improvements and reliability reviews?

b) How do you judge an increase of component failure rates, e.g. by early faults or by wear-out?
3.7 Surveillance test procedures:

a) How are safety tests organised and documented?

b) Do the test procedures involve all safety relevant components and safety functions? Are safety-relevant components determined by PSA?

c) What is the base for the assessment of the test intervals, e.g. engineering judgement, plant experience, PSA?

d) Is there a special priority on the kind of test procedures, e.g. with emphasis on integral system tests or more on single tests of each component? Do you have special experience as regards the efficiency of each type of the above mentioned tests?

e) Is there any experience in, or criteria on, modifying test procedures and test intervals? Do you use any QA in checking the efficiency of test procedures?

f) Are the timescales of test intervals limited by tolerances? What is the base of such limitations?

g) In some cases it is not possible to perform a sufficiently realistic test procedure. In this event what measures do you consider? Give examples.

3.8 Preventive maintenance for reliability assurance:

a) What are the aspects of preventive maintenance (PM) and how do you determine PM of components, e.g. by engineering judgement, plant experience or statistics, in order to prevent an increase of component failure rates?

b) What is the average number of components and component types under maintenance during refuelling phases?

c) What are the time schedules for internal inspections of safety relevant components such as valves and pumps (e.g. components disassembly and exchange of component parts if necessary)?
d) Are there any component types which require a yearly or more frequent preventive maintenance job, e.g. caused by high wear? Have you any experience on the time scale of component wear-out? Please give examples.

4. LIST OF UTILITIES THAT HAVE RESPONDED TO THE QUESTIONNAIRE:

<table>
<thead>
<tr>
<th>Country</th>
<th>Contact Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td></td>
</tr>
<tr>
<td>TVO, Teollisuuden Voima Oy</td>
<td>A. Piirto</td>
</tr>
<tr>
<td>2 BVR at Olkiluoto</td>
<td></td>
</tr>
<tr>
<td>Imatran Voima Oy</td>
<td>J. Vaurio</td>
</tr>
<tr>
<td>2 PWR at Loviisa</td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>Northeast Utilities</td>
<td>M.V. Bonaca</td>
</tr>
<tr>
<td>BWR Hillstone Unit 1</td>
<td></td>
</tr>
<tr>
<td>PWR Hillstone Unit 3</td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
</tr>
<tr>
<td>Oskarshamn NPP</td>
<td>U. Sjöö</td>
</tr>
<tr>
<td>3 BVR</td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td></td>
</tr>
<tr>
<td>Atomic Energy of Canada Limited</td>
<td>P. Gumley</td>
</tr>
<tr>
<td>Ontario Hydro Utility</td>
<td>J.A. Farr</td>
</tr>
<tr>
<td>CANDU-Units</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
</tr>
<tr>
<td>Nuclear Engineering Research Laboratory, University of Tokyo</td>
<td>S. Kondo</td>
</tr>
<tr>
<td>Tokyo Electric Power Co.</td>
<td></td>
</tr>
<tr>
<td>BVR</td>
<td></td>
</tr>
<tr>
<td>Kansai Electric Power Co.</td>
<td></td>
</tr>
<tr>
<td>PWR</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
</tr>
<tr>
<td>Consejo de Seguridad Nuclear</td>
<td>J.I. Calvo</td>
</tr>
<tr>
<td>UNESA</td>
<td></td>
</tr>
<tr>
<td>PWR and BVR</td>
<td></td>
</tr>
</tbody>
</table>
5. RESULTS OF QUESTIONNAIRE:

The answers received from the Utilities have been compiled for each question and appended to this report. Similar answers have been linked together where possible.

In this Chapter the answers are summarized for each section of the Questionnaire.

- 3.1 Plant shut-down during plant operation:

The questions were focussed on how plant safety operation is regulated and how these regulations are supported by PSA. To maintain the plant in a safe state, the plant parameters should be held within defined boundaries during operation. Excessive deviation from these parameters will result in an increase in plant risk. PSA can be used to assess this risk or to set limits for tolerable deviations.

RESPONSES:

The safety requirements necessary for a plant shutdown are written in the plant's Technical Specifications (TS) and are generally based on regulatory criteria, approved by the regulatory body.

Safety requirements are mainly focussed on allowed outage times (AOT) of safety systems or on limiting conditions for operation (LCO) and surveillance tests (US). If a sub-system is unavailable examples of AOT range from 1h to 30 days, depending mainly on the degree of redundancy and the importance of the system.

In addition to AOT requirements, surveillance tests of other redundant sub-systems are required for improving system reliability during sub-system unavailability (Japan, F.R. of Germany).
In general, all safety-relevant components are regulated by AOT. Assessment of AOT is based on engineering judgement supported by PSA.

F.R.G. : PSA where safety systems are concerned.
U.K. : Mainly PSA.
U.S. : AOT based on conservative engineering judgement should be changed by PSA if felt to be excessively conservative.

Actual experience on plant shutdown caused by AOT show that these events are rare.

Canada : Exact figures are not available, but are in the order of $10^{-1}$ - $10^{-2}$ forced shutdowns/unit/year.

Safety requirements on plant parameters and on the state of specific plant equipment are also specified:

F.R.G. : Boundary values for thermal power, chemical values, air temperatures, etc., demands on closure of specific rooms, tightness of check valves (to project against flooding, external events and interfacing system LOCA).

There are only a few direct requirements of plant operation due to CCF.

Finland : An immediate shutdown is required if the possibility of CCF cannot be excluded.

F.R.G. : If an indication of CCF is observed during maintenance, all redundant components of similar types should be tested immediately. If an increase of the component failure has been observed to be of an extent which may lead to multiple component failures before the next surveillance test, or if the component function does not meet the special conditions of accident demand, all components concerned should be considered as unavailable.

- 3.2 Safety requirements on plant start up:

In reliability analyses, it is normally considered that the plant revision results in renewal of plant equipment. Based on this assumption, all plant systems and components are set in a state of reliability equal to 1 at plant start-up. Additionally, a total check of all safety-important components to the end of the revision phase is essential because multiple plant equipment were out of service or in various operational modes due to preventive and corrective maintenance during the revision phase.

RESPONSES:

Generally given response: A plant start-up generally requires the availability of a full scope of system redundancies.

In some cases the same AOT for start-up and normal operation are used (F.R.G. - in case of short outage time <100 h).
U.S.: Plant start-up requires a controlled transition from cold shutdown (Mode 6) to power operation (Mode 1). In each mode the operability of defined sub-systems should be checked. In these cases the use of AOT is not permitted.

- 3.3 Maintenance activities:

The questions were focussed on regulations on how to prevent plant hazards and on maintenance due to excessive unavailability.

Generally, assumptions on component states are simply made in reliability analyses. If a component failed after a defined repair time, the component should be considered to be completely intact ("as good as new"). Based on this assumption, an appropriate component check after completion of maintenance is an important factor of component reliability.

RESPONSES:

Maintenance safety regulations are covered in TS and QA Manuals, e.g., restrictions on components or system removals from service for planned maintenance (Canada), and bringing the components into service within AOT.

U.S.: (Similar to other responses) detailed written procedures exist for all maintenance activities and contain standard formats addressing items such as:

- preparations and required tools
- system isolations and tagging equipment out-of-service
- disassembly and inspection
- maintenance actions
- reassembly and subsequent inspections
- post-maintenance tests
- restoration and clearing of tags following completion of maintenance activities.

F.R.G.: The operating manual gives a list of systems and equipments that must be available before start-up of the plant. Furthermore, check lists are given for the necessary position of manually-operated valves. In certain cases, these valves are fitted with a key which can only be removed from the valve if it is in the correct position. This is applicable to valves with which pilot valves for safety valves or relief valves can be blocked. Also valves with wich residual heat removal can be blocked are fitted with such keys. All these keys must be in the control room before start-up.

- 3.4 Safety-relevant system modifications:

The questions were focussed on safety assessment of system modifications and to what extent PSA is used for reevaluation of system modifications.
RESPONSES:

Finland: Safety-relevant system modifications are approved by the Authorities.

F.R.G.: All modifications should be classified as related to their significance for safety. The related formal procedures differ with respect to the degree of safety for which a permit is being applied.

U.S.: Plant changes are regulated by U.S. standards if the following can be excluded:

- an increase in the probability of an accident
- an increase in the consequences of an accident
- the creation of a new type of accident not previously considered in existing plant accident analyses.

U.S.(NU): Maintenance of the PSA models is essential to ensure that they continue to provide an accurate description of the plant. Plant changes (hardware and procedures) and operational data (maintenance, running time and equipment failure data) are being collected to update the PSA models. The NU procedural framework is used to collect plant design-change documentation.

- 3.5 Operator response to abnormal events:

The questions were focussed on to what extent an operator can perform a safety task with the adequate reliability and on how to improve operator tasks in this respect.

RESPONSES:

Design criteria: operator response time in abnormal events is generally based on 30 minutes.

Canada: 15 minutes of response time for control room actions; 30 minutes of response time for field actions.

In practice, responses range between a few seconds and a few minutes. Simulator training has been introduced for plant operators.

Finland (PWR): Initial training of operators, lasting from 6 to 8 weeks, and an annual retraining of 10 days.

U.K. (UKAEA): Reliability diagram support usage: fault trees are not routinely employed by the operators. These are used, where appropriate, by the safety and assessment teams in formulating the operating rules and procedures.
3.6 The use of data feedback

The questions were focussed on evaluating operational experience of safety components and on reliability data collecting.

RESPONSES

Sveden/Finland (BWR): Plant data have been collected for a national data bank, used for component reliability data and for PSA. Plans for achieving a living PRA model are under discussion, or it is already in use.

Canada: Test records are used to compile component failure rate statistics, which are subsequently used in routine and non-routine reliability analyses. Actual component failure rates are compared annually against expected failure rates. Statistically significant deviations are investigated to determine the root cause (similar to other responses).

U.S. (NU): Plant-specific PSA is developed. An essential feature of these models is their reliance on plant-specific reliability information to the maximum extent possible.

Spain/Japan: National data banks are being built up.

Unavailability of safety-related components and sub-systems has been documented and used for reliability analyses and on reliability targets (Canada, F.R.G., Japan, Spain, U.K. (UKAEA) and U.S. (NU)).

F.R.G.: A review of plant experience, e.g., based on actual reliability data, should be carried out after 10 years of plant operation.

3.7 Surveillance test procedures:

The questions were focussed on the importance of surveillance tests for supervising plant safety and reliability and on how these tasks are evaluated by PSA.

Since most safety equipments of NPP are in the stand-by state, surveillance tests and optimal test frequencies are important to safety. On the basis of a constant-failure-rate model, the component test interval has a strong influence on the component availability.

The simplified model of constant failure rate should be used only within reasonable boundaries of test frequencies (TF). This is necessary to avoid an increase in the failure rate due to wear by a high TF or by aging unrevealed by a too-low TF.
RESPONSES:

Surveillance test procedures are written in plant documentation and, to a practical extent, cover all safety-related functions (Canada: similar to other responses). The surveillance test management is supported by computerised systems (F.R.G., Spain, U.K.).

Test intervals are based on engineering judgement. PSA is being increasingly used for verifying test intervals (Sweden, similar to other responses).

Plant experience is used to improve test intervals and test procedures. Test intervals specified in the TS can only be modified by formal changes to TS (U.S., similar to F.R.G.). The ratio of a test interval to a tolerance interval is regulated between about 25 and 30 per cent (F.R.G., Finland, Spain).

Canada: (Similar to other responses): surveillance tests should be performed under conditions simulating an actual demand as far as possible. Because of this, integral tests are given greater attention than the testing of individual components.

For performing sufficiently-realistic test procedures, the operational conditions of any component are verified by a combination of visual checks, functional tests (testing as many failure modes as possible), inspection etc. Where it is not possible to test a particular failure mode, greater attention is given to QA in design, commissioning and operation, in order to ensure adequate confidence.

3.8 Preventive maintenance (PM) for reliability assurance:

Because of the Utilities' large investment in PM, the questions were focussed on how the PM programme is determined and what are the experiences with PM for improving or establishing sufficient component reliabilities.

Up to now there is no experience available to indicate how component failure rates and system unavailability are correlated to the extent of PM. This is important, e.g., in using generic failure data.

RESPONSES

Preventive maintenance has been carried out mainly by engineering judgement, supported by plant experience (component reliability data, U.K./UKAEA), and experience from other plants, as well as recommendations from component manufacturers.

During annual plant shutdown phases, up to 1000 components, such as valves, pumps and electrical equipment are subject to PM.
Canada: If component failure rates were increasing such that reliability targets were being exceeded, additional preventive maintenance measures would be considered.

Time schedules of component internal inspections vary from annual up to ten-yearly schedules.

Japan: Valve overhaul is made once every 1 - 10 years and pump overhaul about every 4 years.

F.R.G.: Internal inspections of safety-important valves are made every 4 years.

Few components require annual or more frequent PM, e.g., rotating DC/AC converters, steam generator tubes, ventilation-fan belt drives. In general, if excessive wear should require such frequent maintenance, changes would have to be made (of design, materials or procedures).
## Appendix

Summarised Responses by Utilities to the Questionnaire

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Plant shutdown during plant operation</td>
<td>21</td>
</tr>
<tr>
<td>3.2</td>
<td>Plant start-up</td>
<td>33</td>
</tr>
<tr>
<td>3.3</td>
<td>Maintenance Activities</td>
<td>37</td>
</tr>
<tr>
<td>3.4</td>
<td>Safety-Relevant System Modifications</td>
<td>45</td>
</tr>
<tr>
<td>3.5</td>
<td>Operation Response to Abnormal Events</td>
<td>50</td>
</tr>
<tr>
<td>3.6</td>
<td>Use of Data Feedback</td>
<td>55</td>
</tr>
<tr>
<td>3.7</td>
<td>Surveillance Test Procedure</td>
<td>66</td>
</tr>
<tr>
<td>3.8</td>
<td>Preventive Maintenance</td>
<td>74</td>
</tr>
</tbody>
</table>
3.1 Plant shutdown during plant operation

a) What plant-specific document contains the requirements necessary for plant shutdown?

Answer:

Generally given response:
Technical Specifications (TS) based on Regulatory Criteria and permitted by regulatory body.
UK: Operating Rules, Operating Limits.

US:

Most plants additionally have written procedures which go beyond areas covered in the Technical Specifications and require plant shutdown items such as chemistry deviations, and as precautionary measures for events such as High Winds, Hurricanes, and other natural occurrences.

F.R.G. (BWR):

The Technical Specifications ("Anlagentechnische Voraussetzungen") of the operating manual Part 2, chapter 1.1-1.4) contain the specific requirements, that have to be obeyed if systems or components of the safety system are not available.
* conditions for start up procedure (Part 2, chapter 1.2)
* conditions for plant operation (Part 2, chapter 1.3)
* conditions for plant shut-down (Part 2, chapter 1.4)
  + Reactor pressure vessel closed, Water temperature 150 °C
  + Reactor pressure vessel closed, Water temperature 150 °C,
  + Reactor pressure vessel open with fuel elements in the reactor pressure vessel
  + Reactor pressure vessel open with fuel elements in the fuel element cooling pool.

The Technical Specifications are reviewed by an independent expert and approved by the licensing authority.

...
3.1 Plant shut-down during plant operation

b) What kind of requirements are given?

Answer:

Generally given response:

Allowed outage times (AOT) of safety related system functions, e.g. shut-down system ECCS, Containment integrity, Diesel generators.

Canada:

Requirements are that if the system is unavailable, reactor shall be shut down in x hours if repairs are estimated to exceed y hours.

For other safety-related systems, actions on system unavailability vary, depending on system importance. For some, the Station Manager can approve continued operation based on prevailing unit conditions. Others require shutdown similar to Special Safety Systems.

US:

TS contains requirements on Limiting Conditions for Operation (LCO) as well as on Surveillance Tests (see 3.7 a for additional remarks).

Spain:


F.R.G. (PWR)

The Technical Specifications cover all safety aspects, that have to be taken into consideration during plant operation and shut-down. Thus, the specifications do not only cover allowed outage times (AOT) for safety-related systems and equipment, but also items like

- boundary values for operating values, such as thermal power, offset factors, chemical values, air temperatures, etc.

- requirements related to the opening of watertight rooms inside the annulus. The opening of these rooms is restricted, because in case of a leak of the cooling water systems inside these rooms, water would flow into the annulus, where the ECCSs are installed.

...
- requirements related to the tightness of check valves in the pipes that are connected to the primary circuit and that penetrate the containment (such as ECCS-pipes and recharging pipe). These requirements are necessary, because no automatic isolation is initiated in case of a rupture of these pipes outside of the containment building.

- the number of people working inside the containment is restricted due to the capacity of the air locks.

- the opening time for aircraft impact barriers is restricted on the basis of probabilistic analyses.
3.1 Plant shut-down during plant operation

c) Give typical examples of allowed outage times (AOT)

Answer:

UK (SGHW):

Examples of periods of unavailability of items of safety-related plant:

- one hydraulic pump out of service ≥ 7 days.
- any HP/LPECW automatic changeover valve not available for ≥ 10 hrs.
- north or south flume system not available, for ≥ 48 hr.
  In the event of any of these AOT approaching exceedance, a controlled shut-down of the reactor must be implemented.

Finland:

AOT of 3 weeks, single failure is still manageable
3 days, single failure no longer manageable
24 h, 1 containment isolation valve failure
8 h, 1 failure at 1 out of 3 reactor protection channels; to be set fail-safe after 8 h
1 h, 1 out of 2 pressurizer safety valves stuck closed.

Japan:

1. When one Diesel Generator is inoperable, the reactor can be in operation for 10 days on condition of operability of another Diesel Generator, performing the surveillance at once and every day.

2. When one core spray pump is inoperable, the reactor can be in operation for 10 days on condition of operability of another core spray pump and Diesel Generator, performing the surveillance at once and every day.

Canada:

Allowed repair times vary between none for unavailability of a Shutdown System, to 8, 12 or 24 hours for unavailability of other safety-related systems. Note that these times are for the systems as a whole, and are for forced maintenance. Requirements prohibit making a system unavailable for planned maintenance.
US:

Millstone Unit 3

<table>
<thead>
<tr>
<th>PWR</th>
<th>AOT(1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ECCS Accumulator (4 total)</td>
<td>1 hr.</td>
</tr>
<tr>
<td>RPS Grip Channel (2)</td>
<td>48 hrs.</td>
</tr>
<tr>
<td>1 ECCS Subsystem, including:</td>
<td>72 hrs.</td>
</tr>
<tr>
<td>1 Charging Pump</td>
<td></td>
</tr>
<tr>
<td>1 High Head Safety Injection Pump</td>
<td></td>
</tr>
<tr>
<td>1 RHR heat exchanger</td>
<td></td>
</tr>
<tr>
<td>1 RHR pump</td>
<td></td>
</tr>
<tr>
<td>1 Containment Recirculation Heat Exchanger</td>
<td></td>
</tr>
<tr>
<td>1 Containment Recirculation Pump</td>
<td></td>
</tr>
</tbody>
</table>

AFW pumps (2 electric/1 steam driven) 72 hrs.

NOTES:

(1) Standard nomenclature in U.S. Technical Specifications does not use AOTs. For purposes of comparison we are providing Action Statement time frames for restoration without having to initiate plant shutdown.

(2) Based upon one less than the minimum required operable channels.

F.R.G. (PWR):

As a general rule, all safety related systems (like ECCS) consist of 4 subsystems, with a capacity of 50% for each subsystem (4 x 50%).

In case one such subsystem is unavailable, the AOT is 14 days. In case two are unavailable, the AOT is 24 hours. In case three are unavailable, the plant has to be shut down immediately.

AOT is longer if additional equipment with the same capacity is available. Also for the emergency diesel engines the AOT is longer because there is a capacity of 4 x 50% for "normal" loss of power and another 4 x 50% capacity for loss of power due to accidents like aircraft impact, earthquake, sabotage and big explosions.

...
F.R.G. (BWR):

Examples of AOT
* Immediate start of plant shut-down
* 8/10/72/100 hours, single failure is no longer manageable
* 7/14/30 days, single failure is still manageable
* 1/6 months, single failure is still manageable

F.R.G. (THTR):

Control devices of decay heat removal system 100 h
Steamgenerator - DHRS 500 h
Air recirculation system of reactor building 700 h
Emergency diesel generator (1) 650 h
Shut-down system (reflector rods) 1450 h
Shut-down system (core rods) 7400 h
Control gas supply of core rods 430 h
Reactor protection system/devices 100 h

Spain:

- With the number of operable channels less than required by the minimum operable channels per trip system for RPV water level, be in at least hot shutdown within 2 hours.

- With one centrifugal charging pump inoperable, return to the operable status in 72 hours or be in hot stand-by in the next 6 hours or in cold shutdown in the next 30 hours.
3.1 Plant shut-down during plant operation

d) Are all safety-relevant components regulated by AOT or only by representative components? How are these components defined with respect to their sub-systems?

Answer:

US (similar to other responses):

All safety relevant components are regulated by Technical Specifications LCOs and Action Statements.

Technical Specifications are written in terms of subsystems (or trains of equipment). Operability of a subsystem requires operability of all components in a subsystem and all train-related support systems.

Canada:

No mandatory maximum outage times are specified at the component level. However, where maintenance outage time is significant, it is monitored to check for consistency with assumptions in reliability analysis.

Japan:

AOT regulations are applied to major safety-related components such as ECCS pumps and Diesel Generators. Most of other components are regulated only by representative components. For supporting sub-system, no specific limitation is defined, but general requirements are naturally included in the associated regulation.

UK (SGHW):

Only representative components of safety systems are regulated by AOT. These are items such as pumps, valves, filters, etc. where redundancy exists.

F.R.G.

All safety related systems, components and equipment are regulated. The systems and components are considered to be available, if in an emergency, they would meet their operational design requirements. Generally, this includes a sufficient cooling water supply, emergency power supply, lubrication, etc.
3.1 Plant shut-down during plant operation

e) What is the basis of AOT assessment, e.g., PSA or engineering judgement?

Answer:

F.R.G. (similar to other responses):

Both, engineering judgement and PSA, were used to determine AOT. In general, AOT was determined on the basis of common practice and conservative engineering judgement. With these AOT-figures, the reliability of safety systems was determined and compared with the requirements.

US:

The vast majority of the bases are conservative engineering judgement. Recently, PSA is being used to change certain AOTs which are felt to be excessively conservative.
3.1 Plant shut-down during plant operation

f) Are there additional regulations for other plant conditions, such as during plant shutdown phases due to heat removal from the fuel elements, or containment isolation?

Answer:

Japan (similar to other responses):

For plant shutdown phases, requirements to secure cooling capability of fuels and sub-critical condition of the core are defined.

US:

Technical Specifications Action Statements cover all such areas that are safety-related, including:

- Reactor Shutdown
- Decay Heat Removal
- Emergency Core Cooling
- Containment Isolation
- Containment Cooling
- Control Room Habitability
- Fire Protection
- Physical Security
- Radiological Monitoring and Protection.

F.R.G. (BWR)

During refuelling outages, 3 out of 4 redundancies of the residual heat removal system have to be available (stand-by), while the number of redundancies in service depends on the decay heat output.

If because of maintenance work, there are only 2 out of 4 redundancies available, this work has to be planned in such a way that one of the two redundancies unavailable can be brought into service within an appropriate time. This time is limited by the tolerable water temperature in the reactor vessel and in the fuel element cooling storage pool.
F.R.G. (PWR):

Technical Specifications are divided into:

- general requirements
- requirements for start-up
- requirements for operation
- requirements for shut-down

The requirements for shut-down are given for different shut-down conditions, such as:

- fuel in the reactor vessel, primary circuit closed and water level in pressurizer
- water level lowered to the loop and cover of the PRV open
- refuelling pool flooded
- all fuel discharged into storage pool

Containment isolation requirements are also dependent on conditions like:

- primary coolant under pressure or not
- primary coolant cold and without pressure
- refuelling respective discharging under way
- all fuel discharged into storage pool
3.1 Plant shut-down during plant operation

   g) What is the actual plant experience on plant shutdown by AOT?

   Answer:

   Finland:

   BWR: Two shut-downs caused by AOT over 13 years of plant life time.

   Sweden:

   Very few cases of plant shut down due to AOT during 17 years of operation and three units.

   Japan:

   There has been no such experience.

   Canada:

   Forced shutdown due to safety system unavailability are rare (most failures causing system unavailability can be repaired and the system returned at least to a minimally acceptable condition within the allowed repair times). Exact figures are not available, but are in the order of $10^{-3}$ to $10^{-2}$ forced shutdowns/unit/year.

   UK (SGHW):

   Extremely rare. It has happened on failure of the hydraulic system supply - this necessitates an X trip within a short period ($\sim 30$ min).

   F.R.G. (BWR) / similar experience to other German plants

   In the three years of operation the plant has not been shut down because of requirements of AOT.
3.1 Plant shut-down during plant operation

h) Are there special requirements for occasions of common mode failures (CMF)?

Answer:

US: (similar to other responses)

No. Technical Specifications directly address situations where more than one subsystem becomes inoperable whether due to random or common cause failures.

Canada:

For CANDU, two special safety shutdown systems are provided and each system is required to meet an unavailability target on a shutdown demand of $10^{-3}$. Independence and separation of these two shutdown systems are a design requirement to keep common mode failures to a minimum. However, if either or both shutdown systems are affected by such failures the reactor has to be placed in a guaranteed shutdown state. There are similar policies and principles to be followed in the event of other process system running failures or safety related system unavailabilities where common mode failures are shown to be present.

Finland:

Immediate start of shutdown is required, if the possibility of CCF cannot be excluded.

F.R.G. (BWR):

A shut-down is normally required, if 2 out of 4 redundancies are not available, though in some cases a short AOT is given. All events in the emergency shut-down system have to be reported. The reports are used to evaluate an increase of the failure rate in this system.

There is a special requirement concerning common mode failure for the highly redundant system of the safety and relief valves.

*If one safety/relief valve has failed all other valves have to be checked by a surveillance test.

*If there is a failure of two valves the plant has to be shut down because of the possibility of common mode failure.

Common mode failures have to be reported to the Licensing Authority as a "significant event".

F.R.G. (PWR):

All equipment failures have to be investigated with respect to common mode failures.

In case, a common mode failure cannot be excluded for any of the equipment mentioned in the Technical Specifications, the regulatory authority has to be informed and the mean time between failures has to be estimated (for example by more frequent surveillance testing). If the mean time between failures is less, than the time between the surveillance tests, these components have to be considered as unavailable. The unavailability has to be compared with AOT.
3.2 Plant start-up

a) What kinds of requirements are given?

Answer:

Japan (similar to other responses):
To check all related systems and components necessary for plant operation and safety function for their integrity.

US:
Plant start-up requires a controlled transition from cold shutdown (Mode 6) to power operation (Mode 1). Each of these modes has different subsystem operability requirements specified in Technical Specifications and in plant specific procedures. Transition from one mode to a higher mode can only occur if the operability requirements of the higher mode is met. In particular, it is not permitted to enter Mode 1 from Mode 2 with a subsystem inoperable by making use of an AOT.

UK (UKAEA):
The Operating Limits specify minimum availability and maximum permitted operating conditions. The start-up document acts as a check list for the operator in raising from shutdown to full power.

F.R.G.:
For every safety-relevant system the number of redundancies is specified, which have to be available in order to start up. Generally said, a start-up requires the availability of the full scope system redundancies.

F.R.G. (THTR):
Various start up procedures are regulated in TS, e.g., depending on the state of specific reactor component temperature.
3.2 Plant start-up

b) Are the same AOT given as in point 3.1?

Answer:

Finland (similar to other responses):
Same AOT for start-up and normal operation are used.

Canada:
Start-up would not be permitted with a Special Safety System unavailable.

F.R.G.
In general AOTs are not stated. Instead of this, modified restrictions are used, e.g., restrictions on power output. If AOTs are allowed, the same AOT for start-up and normal operation are used.
3.2 Plant start-up

c) Are the same requirements formulated on plant start-up for after-revision-phase and for after an abnormal event?

Answer:

Japan (similar to other responses):

Almost same, but for "after-revision" certain preservice inspections and tests of the related items are required before start-up.

UK (FBR):

Post-event return to power is required to satisfy the same operational rules and limits as for a routine return to power, and would be carried out of the relevant POIs. Depending on the nature, and possible severity, of the event it may be that the return to power would be carried out after special assessments and safety reviews. These may be subject to discussions at the Safety Working Party (SWP), as would bound to be so if the plant had moved outside operating limits or rule boundaries.

UK (SGHW):

No. Following a revision-phase, a series of 19 start-up documents must be followed to check that the plant is in a safe and correct state. Following abnormal events a less exhaustive procedure would be followed though the Plant Manager would specify any special safety-related tests he judged necessary.

F.R.G.:

The AOT-requirements are dependent on the duration of the outage:

- In case of a short outage (interruption of power generation after an abnormal event ≤ 100 h) the same AOT as in point 3.1 applies.

- After an outage of less than 14-days, all equipment with an AOT ≤ 100 h must be available.

- After an outage of > 14 days (refuelling), all safety-related equipment must be available before start-up.

...
3.2 Plant start-up

d) Are there special requirements for checking the workability of safety features after an abnormal event or transient?

Answer:

UK / UKAEA (similar to other responses):

As indicated in (c), each abnormal shutdown would be considered on its merits and special testing carried out as judged necessary.

Finland:

Safety features are tested after abnormal events and transients only for failed components.

F.R.G. (BWR):

Every start-up-procedure has to be conducted in accordance with start-up-checklists. In these checklists (operating manual part 2, chapter 3,1/3,2) the availability/workability of the safety system has to be confirmed. Besides this, after every normal or abnormal shut-down, the valve-off-time of the main isolation valves has to be checked.
3.3 Maintenance Activities

a) What are the maintenance safety regulations?

Answer:

Generally given responses:
Technical Specification and QA manuals.

Canada:

Maintenance regulations are specified in general terms in Operating Policies and Principles. The regulations cover:

1) Restrictions on removing components or systems from service for planned maintenance.

2) Requirement that, during maintenance, the component/channel be placed in a safe state (if possible) during maintenance.

3) Requirement for testing after all maintenance.

4) Level of authorization required for maintenance activities.

5) Requirements that there must always be a back-up method of heat removal available.

US:

There are no explicit safety regulations requiring maintenance. Unscheduled maintenance acts which necessitate declaring a subsystem inoperable are bounded by Technical Specification Action Statements.

F.R.G.

According to the rules given, a federal rule (BMI-Richtlinie zur Vorbereitung und Durchführung von Instandhaltungs- und Änderungsarbeiten in Kernkraftwerken) prior to any maintenance activity, this has to be checked against:

- requirements of technical specifications
- decommissioning procedure for the corresponding components
- work safety requirements
- health physics requirements
- measures for fire protection
- procedures for start-up of components and systems

Before a maintenance activity can start, these requirements have to be specified on a written work permit by specialists of the appropriate level.

...
3.3 Maintenance Activities

b) In which way are maintenance procedures formulated, e.g. by standard formats of work order reports?

Answer:

Canada (similar to other responses):

Routine maintenance is performed using standard written procedures. Non-routine maintenance is performed using "work plans": written procedures for specific circumstances, reviewed and authorized at an appropriate level.

US:

Detailed written procedures exist for all maintenance activities and contain a standard format addressing items such as:

- preparations and required tools
- system isolations and tagging equipment out-of-service
- disassembly and inspection
- maintenance actions
- reassembly and subsequent inspections
- post-maintenance tests
- restoration and clearing of tags following completion of maintenance activities.

Finland:

Maintenance procedures are based on those of the deliverer of the equipment (translated into finnish for most important equipment).

The maintenance work-planners write isolation lists based on earlier computerized experience. Earlier plans are saved in the computerized "work-plan-bank".

Japan:

Standard maintenance procedures are prepared by the electric power company. The company which is requested to do the maintenance work will prepare the maintenance procedures for the specific outage based on the standard maintenance procedures, and will submit it to the electric power company for comments.
F.R.G.

Standard formats are used to define the order of steps for decommissioning and commissioning of components. The steps are given in form of a check list.

In case of more sophisticated maintenance activities (such as maintenance during refuelling), "work plans" are issued, where the maintenance item is listed in the form of a schedule of sequence and time. For each single maintenance item, standard forms are used to define the decommissioning and commissioning order.
3.3 Maintenance Activities

c) What are the safety regulations on the operational position of valves and on the use of blocking devices during maintenance?

Answer:

Sweden (similar to other responses):
All tagging, isolation of components, etc., is taken care of and administered by the shift personnel in charge.

Spain:
- There are specific valves that are required in a certain position for safety purposes and they are controlled by administrative procedures. If due to maintenance reasons it's necessary to change their position that would result in a T.S. action.
- There aren't any general safety regulations about blocking devices.

Japan

There is no specific safety regulation on the valve position. However, actual valve positions during operation are specified in the "operating procedures for each system". Valve positions during maintenance are specified by the permit work, permitted by the shift supervisor, and are controlled by tags, which are attached to the valves.

F.R.G.

The check list on the work permit does not only contain valve positions, but also blocking devices, keys, etc. In case electrical power supply for certain components has to be disconnected, the corresponding switchgear is marked by tagging.

During the course of commissioning, all the tags, keys, blocking devices, etc. are recollected according to the check list.
The operating manual gives a list of systems and equipment that must be available before start-up of the plant. Furthermore, check lists for the necessary position of manually operated valves are given. In certain cases these valves are each equipped with a key that can only be taken off the valve if it is in the proper position. This is the case for valves with which pilot valves for safety valves or relief-valves can be blocked. Also, valves with which residual heat removal can be blocked, are equipped with such keys. All these keys must be on the control room before start-up.
3.3 Maintenance Activities

d) What are the regulations on how to check (test) the components or system function after maintenance?

Answer:

Canada (similar to other responses):

Regulations specify that components must be tested following maintenance, prior to being placed in service. No detailed requirements specified, although each maintenance procedure does include details of tests which must be performed.

F.R.G.:

The operation manual contains strict regulations for checks of the reactor protection system and safety system after maintenance. In this case a cross check has to be ordered by the plant management in the form sheet of the work authorization procedure.

Besides this, the work order system contains requirements for functional tests of the component or the system.
3.3 Maintenance Activities

e) Regarding the above points, what do the documents of maintenance and repair reports look like?

Answer:

Spain:

There are pre-fixed format documents that contain details such as:

- Plant status.

- Equipment description.

- Need to notify Control Room.

- Work Radiation Permit requirements.

- Work performed report.

Canada:

Generally, each report is a single sheet, giving a brief description of the work done, including a record that a test was performed and authorization for release for service.

Japan:

Maintenance reports on the MITI inspections contain plant name, inspection name, inspection number, inspection results, and specific comments, and attached to the sheet. The data sheet describes each inspection result, some of whose formats are check sheets and which include some important measured data in numerical data.

US:

Computer generated maintenance work order, generated and used by Northeast Utilities Production Maintenance Management System (PMMS).

Detailed descriptions of maintenance procedure are used, e.g., for disassembly/reassembly Main Steam Isolation Valve.
UK (UKAEA):

The PTW/CTW are single-page formatted sheets specifying:
- the item(s) of plant in question
- the work to be done
- all necessary isolations
- precautions against specific hazards
- health and safety
- a record of plant handover

Maintenance/repair reports are also single-page formatted.

F.R.G.

Filling in the forms requires specification of:
- description of the work
- description of necessary work safety measures
- restrictions with respect to technical specifications
- work order for decommissioning and commissioning
- certification that decommissioning has been carried out
- certification that maintenance has been carried out
- certification that functional testing has been carried out.
3.4 Safety-relevant system modifications

a) What are the main reasons for system modification?

Answer:

Spain: (similar to other responses)
Licensing requirements,
Safety improvements,
Operating improvements,
Supplier recommendations.

Finland:
The main reasons are if the modifications are considered sufficiently important from the point of view of:
- own operating experience,
- experience gained with the on-site training simulator,
- operating experience from other PWR plants,
- Three Mile Island (TMI) accident,
- new information on materials and components,
- changes in licensing requirements, and
- results of experiments carried out by Utility.

Japan:
There are not so many examples of system modifications. One of those was the addition of PCS. In this case, the electric power company carefully watched the situation of development of the new thought of safety system design in the U.S. and determined to add those system voluntarily.

UK (UKAEA):
Improvement of reliability and serviceability also (rarely) elimination of any identified fail-danger mode.
3.4 Safety-relevant system modifications

b) How are maintenance and system or component changes distinguished?

Answer:

Canada:
Replacement of failed components with identical components is considered as maintenance. Nonidentical component replacement is considered as modification.

Finland:
The distinction between maintenance and system component changes depends on whether a change of design feature of the system or of the components is given or not.

US:
Physical modifications to systems or components require that processing of a Plant Design Change Request (PDCR) to determine whether it is safety or non-safety related.

Japan:
Construction for plants requires to get Application for Permit for Construction Plan by MITI. System/component changes are categorized by whether or not Application or Amendment for Permit for Construction Plan is necessary. Modification Report System to be circulated within the plant.

F.R.G.:
Replacement or repair of failed components is considered as maintenance. Nonidentical component replacement or any other alteration of systems or component is considered to be a modification.

General practice is to distinguish between
- Alteration (Änderung)
- Repair (Reparatur)
- Replacement (Austausch)
- Maintenance and inspection (Wartung)
3.4 Safety-relevant system modifications

c) What are the criteria for the necessity of getting a permission for a system modification and are there any special regulations concerning this topic? Give examples please.

Answer:

Finland (similar to other responses):

Safety relevant system modifications are approved by the Authorities. All proposals and modifications are checked by the safety office.

Canada:

Regulations governing approvals necessary for modifications are:

(1) Prior regulatory approval is required for all changes which could significantly and adversely affect the assessment of public risk as stated in current licensing submissions.

(2) Prior Station Manager approval is required for all changes to Special Safety Systems which do not place the system in a safe state, and for all permanent changes.

(3) Prior Shift Supervisor approval is required for temporary changes to any system.

US:

In the United States, Table 10 of the Code of Federal Regulations, Section 50.59, addresses plant changes for which permission is not required. These regulations allow plant design change and special tests, provided the change does not:

- increase the probability of an accident
- increase the consequences of an accident
- create a new type of accident not previously considered in existing plant accident analyses.

PSA maintenance activities

The maintenance of the PSA models is essential to ensure that they continue to provide an accurate description of the plant. Plant changes (hardware and procedures) and operational data (maintenance, run time, and equipment failure data) are being collected to update the PSA models. The NU procedural framework is used to collect plant design change documentation.
UK (UKAEA):

Subject to 'safety approval modifications' (SAM) procedure. All plant modifications are vetted within this system; items of safety significance are subject to independent (off-site, outside the reactor line management teams) assessment.

The criteria are embodied in the Modifications Procedure. Any safety-related system modifications must be approved by the SGHWR Safety-Commitee before implementation.

Examples:— upgrading of the LPECW supply system
- improvements in LSD system alarm indications
- installation of full-range stack monitors (for monitoring large releases under accident conditions).

F.R.G.:

All modifications have to be classified relative to their significance for safety. The related formal procedure differs according to the degree of approval demanded.

* Modifications of direct safety significance demand a licensing procedure.

* Modifications of minor safety significance have to be approved by the licensing authority.

* Modifications without safety significance but involve changes in the documents of the original licensing procedures (e. g., system diagrams) have to be confirmed by the Authority that the modification is classified rightly.

* Modifications without safety significance and no changes in documents of the original procedure have solely to pass the internal review and release procedure.

The formal procedure is described in the operating manual and quality assurance manual.
3.4 Safety-relevant system modifications

d) How far are safety systems operations regulated by plant manuals and how far can these be deviated from?

Answer:

Sweden (similar to other responses):

Operations of safety systems are very closely regulated in procedures and technical specifications.

Spain:

- There are written procedures.
- There are administrative procedures that allow the deviation of the written instructions in some circumstances and provided some authorizations are given. These deviations will be later procedural changes.

Canada:

Operators must follow written procedures. The Station Manager may authorize deviations given adequate technical justification, but must still remain within the bounds of the OP&Ps.

The Shift Supervisor may also authorize deviations, but has more limited authority than the Station Manager.

UK (UKAEA):

Safety systems operations are fully regulated according to the SGHWR Operating Manual. Deviations are limited by strict controls (e.g., keys under the direct control of the Shift Manager).
3.5 Operator response to abnormal events

a) What is the minimum response time for an operator to fulfil a task during an abnormal event, based on:
   - formal design criteria
   - practical experience

Please give examples of the above.

Answer:

Finland (similar to Sweden):

Design is based on the 1/2-hour rule. During that time the automatic equipment should take care of the necessary safety functions.

In practice the first operator actions take place within a couple of minutes after the scram.

Spain:

Based on formal design criteria.

In the LOCA case, there will be no credit given after the accident during certain time for the operator actions.

US:

Formal design criteria, typically, only allow crediting operator actions 30 minutes after a design-basis event.

Practical experience indicates that well trained operators are capable of diagnosing events, and initiating actions in time periods as short as three seconds.

As an example: In August, 1985 at the Millstone Unit 1 BWR, after 317 continuous days of power operation, a spurious main steam line isolation and reactor trip occurred. Actuation of the logic was annunciated on an alarm panel. Operators diagnosed the event and in 3.0 seconds (the time required for the MSIVs to close) manually initiated cooling, using the emergency Isolation Condenser before any significant pressure rise could occur. So quickly were these actions taken that none of the relief valves lifted.

...
Canada:

Formal design criteria are:

- 15 minute response time for control room actions.
- 30 minute response time for field actions.

In practice, response ranges between a few seconds to a few minutes. As an example, in the pressure tube rupture incident at Pickering NGS-A in 1983, operator actions to shut the reactor down and start a second pressurizing pump took 10 minutes after the first alarms indicating a large leak.

Japan:

(1) formal design criteria
(2) Practical experience
(3) example

10 minutes (it is the description of Safety Evaluation Guideline).
It would be less than 10 minutes, but has not been measured practically.
- starting of containment spray system
- Valve Isolation as Off-gas system failure accident.

UK (UKAEA):

Formal design criteria: the operator should not need to intervene during the first 30 minutes after a LOCA. Practical experience: to protect plant against damage, response times may need to be in the order of a few minutes (e.g., loss of ancillary cooling water).

F.R.G. (PWR):

The design of the plant is based on the 1/2-h rule. Nevertheless, it is felt, that in case of an accident, it takes about one hour, before operator actions are necessary. Therefore, operators are taught to check the automatic actions and to make sure that certain safety requirements (like subcriticality, residual heat removal etc.) are met during an accident, instead of making any short-term corrective actions. Such actions should only be made if this improves the plant safety under all circumstances (like manual trip), or if the plant availability can be improved in case of simple incidents like failure of automatic control, etc.
3.5 Operator response to abnormal events

b) How do you train for these tasks and what are the tools used, e.g., accident sequence diagrams?

Answer:

Spain (similar to other responses):

With training on Emergency Operating Procedure and plant-specific simulator.

US:

One out of every six weeks, plant operators attend formal training lectures conducted by the Training Department, and practice on a full plant simulator. Some of the scenarios are developed based on the insights of plant-specific PSAs.

Finland:

In Loviisa there is a full-scale simulator that models the plant behaviour in normal modes of operation and in various transients and even during a small loss of coolant accident (LOCA).

The initial training of the operators lasts six to eight weeks and the annual retraining 10 days. The simulator is used also for

- validation of operator aids and instrumentation improvements
- formulation and verification of plant operating instructions
- development of better simulation models
- study of alarm reduction in plant transients
- verification of plant modifications
- defining success criteria for PRA
- other kinds of research.

Operator actions due to a SG-tube leakage are required within approximately 10 - 15 min.

UK (UKAEA):

Training by discussions on the job, illustration on the Simulator, practice in emergency exercises. The operator must also understand written instructions concerning his required response to identified plant faults. In the event of a reactor
trip, he must complete a check list which acts as a kind of fault sequence diagram to aid an early assessment of the nature of the fault.

F.R.G.:

Manual actions are practised during simulator courses. Every shift supervisor or reactor operator has to take a 1-week-simulator course once a year.

Actions are practised in accordance with operating procedures. For each characteristic accident, these procedures give the sequence of automatic and manual actions and the plant state that should be achieved through these actions.

In case a malfunction of safety equipment occurs during the course of an accident, corrective manual actions, in order to maintain plant safety conditions, are given in special emergency procedures (Schutzziele).
3.5 Operator response to abnormal events

c) Do you use reliability diagrams, such as fault trees, to aid understanding of the accident sequence and different system interactions?

Answer:

Japan:

We use FT extensively.

Symptom-based emergency procedure guidance (reference document) is used to complement the present scenario-based manual.

Canada:

Fault trees or event trees are not generally used directly in operator training. More usually, they will be interpreted by technical section staff who will then include the results in training material.

UK (UKAEA):

Reliability diagram support usage

Fault trees are not routinely employed by the operators, these are used, where appropriate, by the safety and assessment teams in formulating the operating rules and procedures.

F.R.G. (PWR):

Fault trees do not play an important role during the training of accident sequences. Nevertheless, the importance of emergency feedwater supply and emergency power-supply equipment was demonstrated to the operators by fault trees.

The shift has to change to actions, that are directed towards safety requirements (Schutzziele), when certain safety systems fail to operate during an accident.

...
3.6 Use of data feedback

a) How are test and repair reports used when updating plant experience, e.g. for plant improvements and reliability reviews?

Answer:

Canada:

Test records are used to compile component failure rate statistics, which are then used in routine and non-routine reliability analyses.

Sweden:

For example, in the maintenance department, analyses are made to identify areas where improvements can be made. Data are also collected for a national database used for component reliability data for the PSA.

Finland:

The reliability data collection system is under development. One of its tasks in future is the updating of the parameters for a living PSA, and to facilitate trend studies and feedback from experience, so as to optimize maintenance planning, spare parts inventory, technical specifications and AOT. The data collection system is based on a detailed failure event classification in order to evaluate the two important component characteristics for risk assessment

. Failure rates for components that cause initiating events i.e., their failures activate one or more safety functions;

. Unavailabilities (fractional dead times) of components needed after initiating events to accomplish a safety function.

Japan:

We use "Reliability Evaluation System" of the Company for plant improvements. (i.e., computer system to accumulate and evaluate the operation and maintenance experiences.)
US:

The use of plant-specific reliability data is critical in assuring the fidelity of the PSA models. The plant-specific data alone provides significant insights into many plant systems. By using this data, not only is attention given to problem equipment, but also credit is taken for above average equipment performance attributable to activities such as a strong preventive maintenance program. This assures that applications of the PSA model to the design process and for operations input are made with knowledge of existing plant reliability and that such activities are directed to areas needing the most attention.

Significant resources were expended to obtain the plant-specific reliability information, using diverse sources of data such as plant operating and maintenance logs for both MP#1 and CY. This process had generated raw numbers of actual components or system failure, numbers of demands or in-service hours, and total run hours for each individual pump since initial plant operation. Maintenance unavailabilities of systems and components were systematically analyzed to provide means and variances for many key plant systems and components.

It is noticeable that such effort had provided a number of insights into system reliability without even having performed fault tree analyses. For MP#1, for example, this plant specific data base indicates that MOV failure to open (5 failures in 369 demands) is much higher for MOVs inside drywell than for those outside the drywell, that MOV failure to open is significantly higher than ECCS pump failure to start; and that electrical breaker failure to close is insignificant (9 failures in 45,571 demands). This information is very different from the engineering judgment based data provided by WASH-1400, which attributes the same failure rate to all of the above components. These insights are becoming so valuable, that periodic updates of this data base are planned to reveal any trends in the reliability data.

UK (UKAEA):

Maintenance and operational staff become aware of poor reliability components due to the amount of maintenance, all recorded, required to keep them available. Additional, reliability data is collected independently.
F.R.G.

The plant engineers responsible for plant systems and also the quality assurance department received each maintenance report and test report for reviewing system and component experience.

This information is used for planning preventive maintenance. If the mean time between repairs become too short, component improvements will be treated.
3.6 Use of data feedback

b) How do you judge an increase of component failure rates. e. g. by early faults or wear-out?

Answer:

Canada:

Actual component failure rates are compared annually against expected failure rates. Statistically significant deviations are investigated to determine the root cause.

Japan (similar to other responses):

There are no precise criteria in procedure to judge an increase of component failure rates. But, in maintenance, we issue a paper called MRF (Maintenance Request Form), that can be used to judge increases in failure rates.

F.R.G.:

The stipulated reliability data used in the licensing procedure are criteria for evaluating plant operating experience. These criteria have been used also for specific cases, such as reduction of the frequency of tests of the high-pressure injection system due to the low system failure rate from plant experience.
3.6 Use of data feedback

c) What are the criteria to indicate a common mode failure, e.g., in advance?

Answer:

Japan (similar to other responses):

There are no criteria to indicate a common mode failure. When failure occurs, we analyse the failure causes and judge whether the failure is common mode failure or not.

US:

The key criteria used in classifying failure experience as common cause failures is the root cause analyses found in Plant Incident Reports (PIRs) and the proximity in time between multiple events.

Canada:

Potential common mode failures are identified by reliability analyses and avoided to the extent it is practical by design or procedural changes.
3.6 Use of data feedback

d) Do you use plant-specific reliability analyses or PSA/PRA to review plant experience?

Answer:

Finland:

PRA (level 1) going on. Plans for achieving a living PRA-model are under discussion.

US:

As a result of a task force plan developed four years ago at Northeast Utilities, plant-specific probabilistic safety analysis models are being developed for all Northeast Utilities operating nuclear plants. An essential feature of these models is their reliance on plant-specific reliability information to the maximum extent possible. This assures that future design efforts and decisions on backfitting or procedural changes are made with full knowledge of existing plant reliability. The use of plant-specific reliability data assures that the impacts of problem components are given appropriate attention and that proper credit is given for those components, which because of plant-specific maintenance practices, have exhibited better than industry-average performance. This helps to assure that future activities are targeted to the areas needing the most attention.

In 1984, a corporate goal was established for using the living PSA models in all plant support activities (Design, Changes, Technical Specifications Changes, Procedural Changes, Training). This required the establishment of procedural links assuring the timely update of the models and their utilization in the plant change process. This procedural upgrading is now nearing completion.

Canada:

Detailed PRA-type analysis has not been done for any plant currently operating. However, reliability analyses for selected safety-related systems are routinely used at all stations to evaluate the performance of these systems compared to design reliability targets. A detailed PRA is in progress for a plant under construction. It is anticipated that ongoing reliability assessments of this plant will be done in a manner similar to that used on existing plants.
UK/UKAEA (similar to other responses):

To date, only to a limited extent. The present intention is to apply modern techniques in a systematic manner as part of the safety review programme.

F.R.G.:

Similar to German response of Point 3.6 b. A general review of plant operational experience shall be carried out after 10 years of operation.
3.6 Use of data feedback.

e) Do you use data banks of abnormal plant events or maintenance activities for statistical purposes or for reliability data? Give a short description of same.

Answer:

Spain:

A National Data Bank is at the project stage.

Japan:

Central Research Institute of Electric Power Industry (CRIEPI) are collecting failure data and are establishing a data base on system/component reliability. We are planning to use the data for PSA studies in the future.

Canada:

Statistics of abnormal events are maintained and compared annually against relevant licensing or operating targets (e.g., process system failure rates, safety system unavailabilities). All unsafe component failures on Special Safety Systems are recorded in component data banks and used in annual updates of plant-specific reliability analyses. Maintenance outage times are monitored to ensure consistency with assumptions made in the reliability analyses.

F.R.G.:

Such data are collected and analysed in order to improve plant safety and reliability by altering components or operating modes. These data have not yet been used for statistical purposes.

F.R.G. (THTR):

An EDP-Databank system is in use to get a feedback of plant experience. The data will be used for optimization system modification and improvements, to reveal weak points and aging processes. The system is used also for administrative purposes as management of surveillance test, maintenance planning.
Finland / Sweden:

Purpose and scope of ATV

The ATV data bank was initiated in 1974 by the nuclear power utilities in Sweden /4-2/. Later, the Finnish TVO power company joined the collection system for operating safety data. The main purpose of the system is to provide the power industry with different kinds of operating safety data and failure statistics.

The systems can be used to generate different kinds of summarizing tables: selected, sorted, or merged according to various parameters such as type, manufacturer, material, size, etc. However, much of the information is in coded format which makes its interpretation difficult. Component-specific reliability characteristics, e.g., failure rates and mean repair times, can be calculated. Such an analysis, updated every year, might give valuable information about possible trends in component behaviour.

The maintenance staff at the utilities are responsible for the monthly reporting of failures which have occurred in safety and process-related components.

...
3.6 Use of data feedback

f) Do you document the unavailability times of safety-relevant components and determine their cumulative unavailabilities?

Answer:

Japan (similar to other responses):

We document the unavailability times of safety relevant components such as ECCS. But we have not determined their cumulative unavailabilities by analyzing the data.

Canada:

Unavailability times for safety-related components are documented and used in reliability analyses (not necessarily directly as cumulative unavailabilities per component — more often actual failure rates used with expected repair times). Cumulative unavailability at the system level is used directly in comparisons with targets.

US:

Collection and analyses of maintenance unavailabilities

Maintenance is another source of unavailability which was also systematically analyzed. Raw data was obtained for the duration that individual trains were out of service for maintenance. Such outages occur either due to unscheduled maintenance to restore a component or system which fails during periodic surveillance tests or due to preventative maintenance. Certain preventative maintenance is performed for reasons other than component failures. As an example, during a surveillance test, an ECCS pump may correctly start and run for the duration of the test, but plant personnel may observe minor leakage. In some cases, this will result in declaring a train inoperable, valving out the leaking component, and overhauling the pump or seal to eliminate the leak. Data on such events is systematically logged on hardcopy Maintenance Job Orders. The log book for these job orders was systematically reviewed to determine the total time of each maintenance event. The mean total yearly maintenance unavailability for each train of equipment and its associated variance were then computed using data from the last 14 years. To perform uncertainty analyses, it was assumed that the maintenance unavailabilities were Beta-distributed.
F.R.G.: The unavailability of the components of the safety system are subject of the monthly plant report. On the basis of this information annual cumulative unavailabilities are calculated.
3.7 Surveillance test procedure

a) How are safety tests organised and documented?

Answer:

Sweden (similar to other responses):

Procedures based on Technical Specifications also prescribe documentation in a special test log-book.

Spain:

There are computerized systems that indicate to the persons responsible for testing (a) the test to be performed and (b) allowable time interval. When the surveillance test has been finished, the results are checked and kept on the documentation files.

Canada:

Regulations specify that tests must be performed to substantiate reliability claims made in licensing submissions. Station Technical Section staff prepare test procedures and schedule the tests. Operating staff perform tests using standard-written test forms. The test forms are filled in by the operator during the test - checking off each action as performed, recording relevant data and noting any failures or problems. Completed test forms are then sent to the Technical Section staff to ensure that the test was performed as scheduled, and to record any failures.

UK (FBR):

Safety test organisation

These are covered by start-up procedure documents, supported by computer-identified scheduling. They are subject to formal review in the plant Annual Safety Review report. The overall efficiency is in part checked during emergency exercises.

F.R.G.:

According to the NPP-safety rules (KTA-Regel) a list of all safety relevant systems and components to be tested for surveillance has to be established for each plant. This list identifies the items to be tested, the test frequency and the necessary operational conditions for the test.
For each test, a written test procedure exists which has to be followed during the test.

A record form, on which the conduct of the test is reported, is attached to the test procedure.

To conduct the periodic surveillance test a computerized test schedule system is used for planning, performing, following up and reporting. This schedule keeps track of the test intervals. The results are documented in form sheets and have to be evaluated by the responsible system engineer. All surveillance test documents are kept in the main document repository (Archiv). Besides this, the results of all functional surveillance tests are recorded in the log-book of the shift supervisor. For some functional tests, e.g., for the main pressure relief valves specific results come from computer print-outs due to the use of computerized testing devices.
3.7 Surveillance test procedure

b) Do the test procedures involve all safety-relevant components and safety functions?

Answer:

Canada (similar to other responses):
Test procedures are written to cover, to the extent practical, all safety-related functions.

US:
Yes, different procedures test different portions of systems (e.g., sensory instruments, actuation logic, motor-operated valves, pumps, check valves, etc.).

UK (FBR):
All dynamic components with a safety function are tested, with rare exceptions (e.g., the emergency sodium transfer system).
3.7 Surveillance test procedure

c) What is the basis for the assessment of the test intervals, e.g., engineering judgement, plant experience, PSA?

Answer:

Sweden (similar to other responses):

Basically engineering judgement. PSA is more and more used to verify the test intervals.

Finland:

Originally, the engineering judgement by Asea-Atom was used. Plant experience has been used to assess the frequency of tests (three complete checks). Changes in test intervals of the auxiliary feed water system are based on probabilistic system analyses.

Canada:

Depend to some extent on the plant and the safety-related importance of the system. Test intervals for all Special Safety Systems at all plants are determined on the basis of reliability analyses. Test intervals can be changed on the basis of experience, with accompanying reliability analysis which demonstrates that reliability targets for the system will be met with the new test intervals.
3.7 Surveillance test procedure

d) Is there a special priority on the kind of test procedures, e.g., with emphasis on integral system tests or more on single tests of each component?

Do you have special experience as regards the efficiency of each type of the above mentioned tests?

Answer:

US (similar to other responses):

Practical considerations limit integral system tests to refuel outages. Single component tests can generally be performed while the plant is on line.

Canada:

The policy is to test under conditions simulating an actual demand as much as possible. In practice, tests generally are written as a number of overlapping functional tests of subsystems. Redundant channels/components are tested separately.

F.R.G.:

Most of the functional surveillance tests, especially for the safety systems are integral system tests. But functional test of single components, e.g. the relief valves, are performed as well.
3.7 Surveillance test procedure

e) Is there any experience in, or criteria on, modifying test procedures and test intervals?

Answer:

US (similar to other responses):
Test intervals specified in plant Technical Specifications can only be modified by formal changes to the Technical Specifications. PSA is frequently used in analyzing whether or not test intervals should be changed.

Canada:

Most safety-related systems have reliability targets established in design. Test intervals can be modified using plant-specific experience, provided reliability targets are still met. This is a relatively frequent and ongoing process. Procedures are also modified based on experience.

UK (UKAEA):

Yes, e.g., LSD testing - test interval depends on statistical interpretation of operational reliability.
3.7 Surveillance test procedure

f) Are the timescales of test intervals limited by tolerances?

Answer:

Sweden (similar to other responses):
Not in general. The method has been used in some cases.

Finland:
The tolerance in test interval is + 30 % for tests having an interval less than a time between refuelling outages (approximately one year).

Canada:
There are no formal time limits set for test interval tolerances. However, procedures ensure that any test which cannot be performed when scheduled is identified and tracked, and is performed as soon as possible.

Spain:
Yes. Each Surveillance Requirement shall be performed within the specified time interval with:

a) A maximum-allowable extension not to exceed 25 % of the surveillance interval, but

b) the combined time interval for any 3 consecutive surveillance intervals shall not exceed 3,25 times the specified surveillance interval.

F.R.G.:
The test intervals are limited by tolerances.

Test interval: 1 week + 1 day
1 month + 1 week
3 month + 2 weeks
1 year + 2 month

The tolerances given, are based upon recommendations of the Reactor Safeguards Commission (RSK).
3.7 Surveillance test procedure

  g) In some cases it is not possible to perform a sufficiently realistic test procedure. In this event, what measures do you consider? Please give examples.

Answer:

Canada (similar to other responses):

For verifying the condition of any component, a combination of visual checks, functional tests (which test for as many failure modes as possible), inspections, etc., is used. Where it is not possible to test for a particular failure mode, we rely on Quality Assurance in design, commissioning and operations to ensure adequate confidence. An example would be that ECCS full-flow tests cannot be done once a unit is in service. Such a test would be placed on overlapping partial tests and QA.

Spain:

Alternative methods: different fluids, partial tests.

(PWR) Containment Spray: colored smoke, compressed air.

(BWR) Stand-by Liquid Control System: water test tank.

Japan:

We have many cases of sufficiently realistic test procedures. Some examples are as follows,

. ECCS surveillance test (the test using only test loop)
. ADS surveillance test (only electrical circuit test)

UK (UKAEA):

As full as possible a test is performed, with suitable isolations to prevent interaction with normal reactor operation. Example - testing of pond dump trip valves (hydraulics isolated) and only the solenoids operated.

...
3.8 Preventive maintenance for reliability assurance

a) What are the aspects of preventive maintenance (PM) and how do you determine PM of components, e.g., by engineering judgement plant experience or statistics, in order to prevent an increase of component failure rates?

Answer:

Spain (similar to other responses):

Initially, as recommended by the manufacturer and by engineering judgement. Then, by plant experience (equipment history) and experience from others.

Japan:

So far we have determined PM of components by engineering judgement and through national & international operating experience. Also, we have been invited to study the applicable method to determine the components by statistics and the nature of degradation.

UK (UKAEA):

PM is carried out to optimise the reliability of nominated plant (affecting reactor protection, plant safety or station efficiency) by ensuring that systematic attention is given at a suitable frequency. PM is determined by engineering judgement as modified by plant experience.

F.R.G.:

Recommendations of the manufacturer and the practice of other plants are followed. During operation, special attention is given to slow changes in oil temperature, bearing temperature, vibration, noise, chemical data of oil etc. Any abnormal changes may result in an early inspection or maintenance. In the long-term, maintenance intervals will be fixed on the basis of this experience.
3.8 Preventive maintenance for reliability assurance

b) What is the average number of components and component types under maintenance during refuelling phases?

Answer:

Japan:

BWR

Components, for which maintenance is made during refuelling outages are determined, on the basis of the maintenance interval for each of the maintenance types, such as those accompanying disassembly or as simple inspections among all components in the plants. For example at 1,100 MWe BWR plants, there are one RPV, 140 Heat Exchangers, 360 pumps, 30,000 valves, 1,300 motors and 10,000 instruments.

PWR

200 - 300 valves, 10 - 20 pumps, all reactor protection systems and safeguard systems.

Canada:

Data not available. (Note: CANDU units do not have fuelling outages as such.)

UK (SGHWR):

Typically 700 - 800 (annual shutdown).

UK (FBR):

Refuelling operation at PFR are not, per se, the major outage events. Planned outage intervals are more dictated by the needs of routine regulatory 'in-service inspection', planned maintenance, and the experimental programmes. During a typical biennial ISI dictated shutdown of some four to eight weeks, some 1,000 sub systems might receive significant maintenance attention.
3.8 Preventive maintenance for reliability assurance

c) What are the time schedules for internal inspections of safety-relevant components such as valves and pumps (e.g., components disassembly and exchange of component parts, if necessary)?

Answer:

Canada:

Apart from actions necessary to satisfy regulatory requirements (e.g., overhaul of relief valves to comply with ASME code), internal inspections/overhauls of components such as valves and pumps are generally not preplanned. Standby generators undergo major overhauls once per year, but for other components we are moving more towards "predictive" maintenance (i.e., monitoring vibration levels, etc., to determine when overhauls are desirable) or simply breakdown maintenance. Note that if failure rates were increasing such that reliability targets were being exceeded, additional preventive maintenance measure would be considered.

Japan:

Valve overhaul is made once every 1 - 10 years and pump overhaul is made approximately once per 4 years. At the time of overhaul, pump mechanical seal, valve gland, and other miscellaneous O-rings will be replaced by new ones.

Sweden:

1-5 years based on operation time and experience.

UK (UKAEA):

PM varies from annually to ten-yearly, depending on nature of plant.

F.R.G.:

The inspection of safety-related components is part of the surveillance test programme. Certain components which are representative for system conditions and system function have been selected and are inspected regularly. The inspection time
varies between 1 and 5 years and depends mainly on the contribution of the system to the safety function. For example in a BWR one control rod drive (out of 205) is inspected every year. A selected amount of valves of the high-pressure safety injection system have to be inspected within 4 years.

PWR: 1 out of 4 redundant safety system are under PM each year.
3.8 Preventive maintenance for reliability assurance

d) Are there any component types which require a yearly or more frequent preventive maintenance job, e.g., caused by high wear?

Answer:

Sweden:
Yes, E.g. rotating DC/AC-converters have to undergo surveillance a couple of times during one year of operation.

UK (UKAEA):
Yes, e.g., ventilation fan belt drives.

Japan:

BWR
Any components which cannot be replaced without affecting the plant operation can operate successfully for at least 1 cycle (12 months).
Consumed parts which are replaced every refuelling outage are the mechanical seals for pumps which are used during normal operation.

PWR
Typically, such as steam generator tubes are inspected for their degree of degradation yearly.

Canada:

Generally no. If excessive wear was necessitating such frequent maintenance, changes would be made (to design, materials or procedure) to avoid the excessive wear.

Spain:

Important systems and components are subjected to preventive maintenance once per cycle, during refuelling.