IAEA-TECDOC-1417

Precursor analyses — The use of deterministic and PSA based methods in the event investigation process at nuclear power plants

IAEA
International Atomic Energy Agency

September 2004

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (i.e. all these areas of safety). The publication categories in the series are **Safety Fundamentals, Safety Requirements** and **Safety Guides**.

Safety standards are coded according to their coverage: nuclear safety (NS), radiation safety (RS), transport safety (TS), waste safety (WS) and general safety (GS).

Information on the IAEA's safety standards programme is available at the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at P.O. Box 100, A-1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by e-mail to Official.Mail@iaea.org.

OTHER SAFETY RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other publications series, in particular the **Safety Reports Series**. Safety Reports provide practical examples and detailed methods that can be used in support of the safety standards. Other IAEA series of safety related publications are the **Provision for the Application of Safety Standards Series**, the **Radiological Assessment Reports Series** and the International Nuclear Safety Group's **INSAG Series**. The IAEA also issues reports on radiological accidents and other special publications.

Safety related publications are also issued in the **Technical Reports Series**, the **IAEA-TECDOC Series**, the **Training Course Series** and the **IAEA Services Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. Security related publications are issued in the **IAEA Nuclear Security Series**.

IAEA-TECDOC-1417

Precursor analyses — The use of deterministic and PSA based methods in the event investigation process at nuclear power plants

IAEA
International Atomic Energy Agency

October 2004

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

PRECURSOR ANALYSES — THE USE OF DETERMINISTIC AND PSA BASED METHODS IN THE EVENT INVESTIGATION PROCESS AT NUCLEAR POWER PLANTS
IAEA, VIENNA, 2004
IAEA-TECDOC-1417
ISBN 92–0–111604–7
ISSN 1011–4289

Printed by the IAEA in Austria
September 2004

FOREWORD

Among the various efforts to improve operational safety of nuclear installations, the systematic collection, evaluation and feedback of operational experience are considered valuable and effective. This may be achieved by establishing a system for the effective feedback of operating experience. Such a system enables all safety related events to be analysed, root causes determined and corrective and preventive actions implemented to avoid "repeat events" or new events rooted in the same causes.

The traditional ways of investigating operational events have been predominantly qualitative. A method established upon probability safety assessment (PSA) called probabilistic precursor event analysis is being increasingly used as it allows for a quantitative estimation of the safety significance of operational events. This method uses the concept of conditional core damage probability as a measure of the safety significance and can be applied to improve the reliability of the selection of events for in-depth analysis as well as for the process of selecting and prioritizing corrective actions.

The purpose of this report is to outline a synergistic process that makes more effective use of operating experience event information by combining the insights and knowledge gained from both approaches, traditional root cause event investigation and PSA based event analysis.

The IAEA has a well established programme for promoting the systematic collection, evaluation and feedback of operating experience among Member States. It is important that the assessment of events is carried out to the extent necessary to provide confidence that the safety consequences have been fully understood, the causes have been correctly established and appropriate corrective actions identified. The precursor analysis, described in this publication is a further step in the IAEA's programme, that enables better determination of the safety significance of events, so that adequate corrective measures could be planned and utilized.

The IAEA officer responsible for this publication was M. Dusic of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

The efficient feedback of operating experience (OE) is a valuable source of information for improving the safety and reliability of nuclear power plants (NPPs). It is therefore essential to collect information on abnormal events from both internal and external sources. Internal operating experience is analysed to obtain a complete understanding of an event and of its safety implications. Corrective or improvement measures may then be developed, prioritized and implemented in the plant if considered appropriate. Information from external events may also be analysed in order to learn lessons from others' experience and prevent similar occurrences at our own plant.

The traditional ways of investigating operational events have been predominantly qualitative. In recent years, a PSA-based method called probabilistic precursor event analysis has been developed, used and applied on a significant scale in many places for a number of plants. The method enables a quantitative estimation of the safety significance of operational events to be incorporated.

The purpose of this report is to outline a synergistic process that makes more effective use of operating experience event information by combining the insights and knowledge gained from both approaches, traditional deterministic event investigation and PSA-based event analysis.

Figure 1 shows a typical classification and number of events at a plant during a year. One of the problems of handling such a large number of events is to preselect the few events which are sufficiently significant to justify detailed evaluation and analysis. It is crucial that no events are screened out that are relevant to plant safety. Bringing in a different perspective, the PSA-based view helps to ensure that safety-related aspects of an event are objectively identified and consequently makes the selection process more reliable.

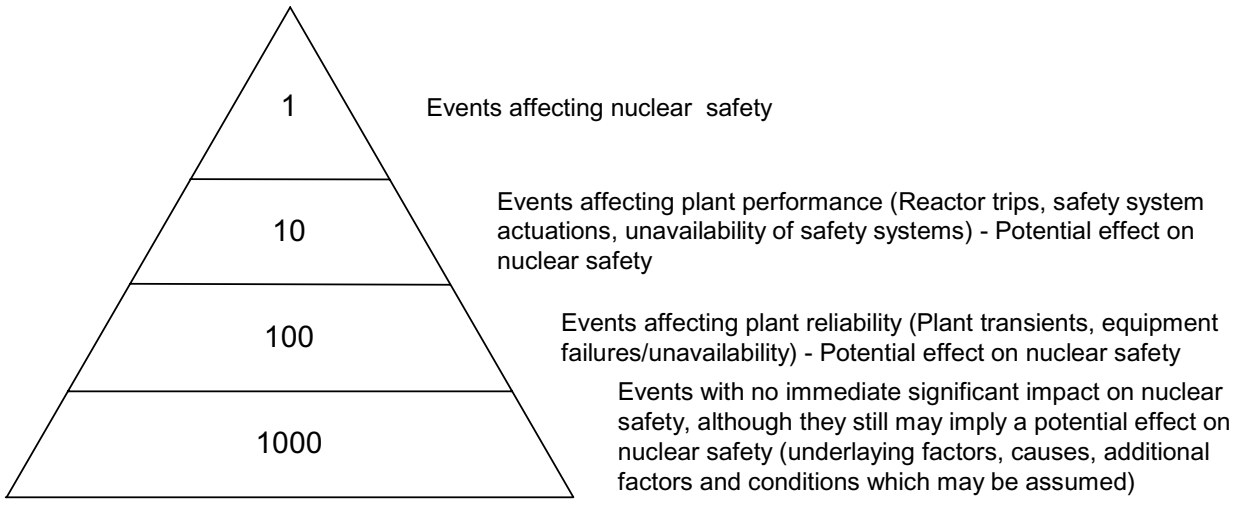


FIG. 1. Typical distribution of event types.

The PSA-based view on operational events and PSA-based event analysis can support the process of operational event analysis at the following stages of the operational event investigation:

1. Initial screening stage: It introduces an element of quantitative analysis into the selection process. Quantitative analysis of the safety significance of nuclear plant events can be a very useful measure when it comes to selecting internal and external operating experience information for its relevance.
2. In-depth analysis: PSA based event evaluation provides a quantitative measure for judging the significance of operational events, contributors to operational events, sub-events, conditions and other influences such as human performance.
3. The development and selection of recommended corrective/preventive actions for implementation and prioritization can be enhanced by taking account of information and insights derived from PSA-based analysis.

In terms of the PSA-based event evaluation, the concept of *conditional core damage probability* (CCDP) provides a useful measure of safety significance for operational events which can be applied to improve the efficiency of selection of events for in-depth analysis, to support in-depth analysis and to support the process for developing, selecting and prioritizing actions. Conditional core damage probability can be derived from PSA studies for a wide variety of operational events. The concept of conditional core damage probability is outlined in the chapter on PSA-based event analysis, but basically it is a measure how far, in the PSA model, is the event which is being evaluated from the core damage scenario.

It should be pointed out that traditional operational event analysis has a wider scope than a typical plant PSA which focuses on nuclear safety. Thus, for example, traditional operational event analysis may also deal with incidents relating to industrial safety which are usually not considered in a PSA. An incident of this type is, for example, a tool dropped by maintenance staff, which hurts other staff but has no measurable implications on nuclear safety. Events of this kind are therefore outside of the scope of a typical PSA based event evaluation.

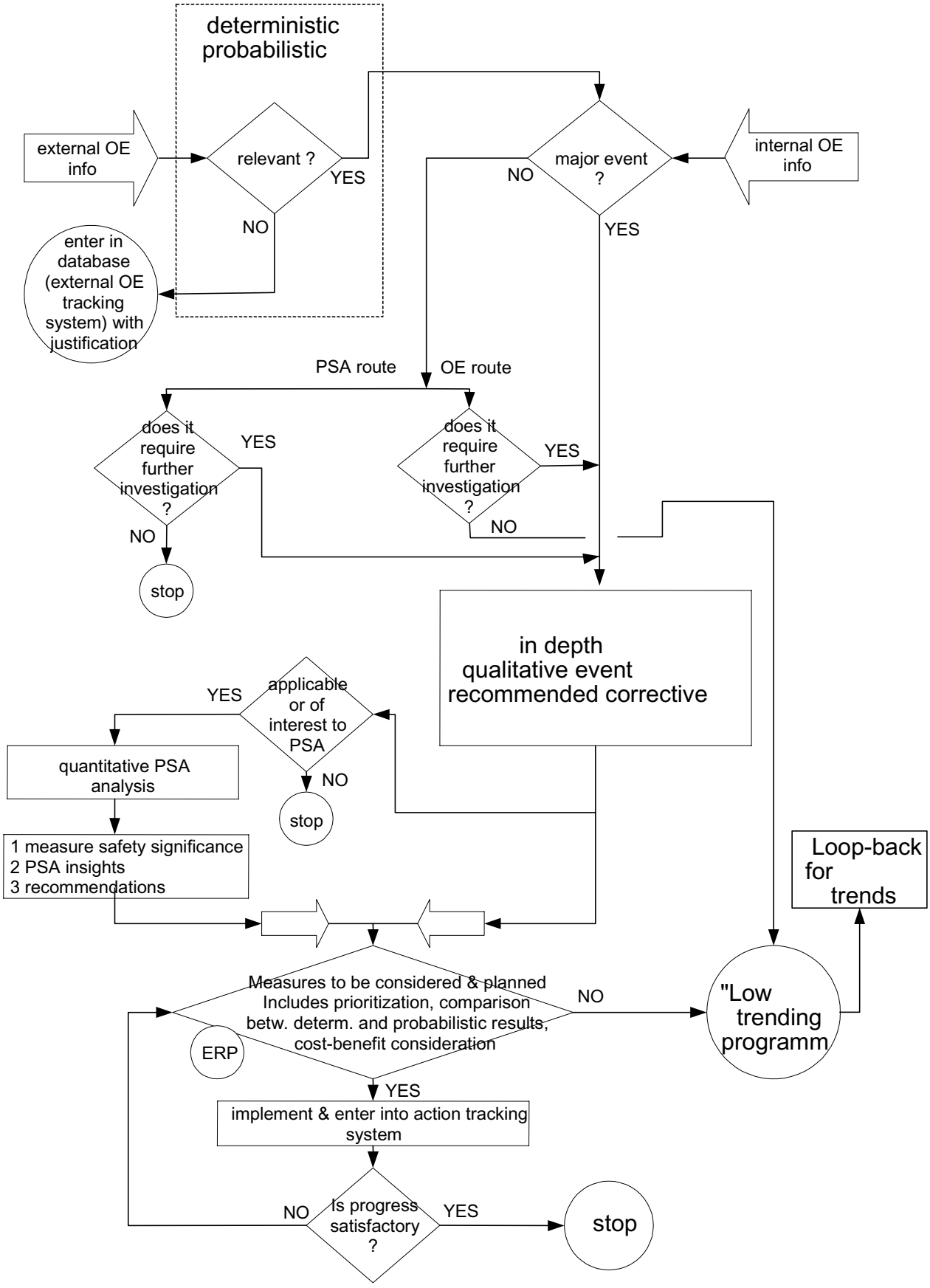


FIG. 2. Process flow chart for operational event analysis.

2. EVENT INVESTIGATION PROCESS

Figure 2 depicts a flow chart for the overall process which includes both, the PSA based view and analysis, and the traditional deterministic practice used at many nuclear power plants (NPPs) for processing operating experience (OE) information arising from on- and off-site. It shows the basic elements of the process:

- screening and selection
- in-depth analysis
- implementation of actions.

The individual steps are described in detail in Section 2.1.

2.1. SCREENING BY OE PERSONNEL

There are two principal sources of operating experience (OE) information which have to be considered at any particular nuclear power plant: off-site or external OE; and on-site or internal OE.

Assessment of events is carried out to the extent necessary to provide confidence that the safety consequences have been fully understood, the causes have been correctly established and appropriate corrective actions identified. The assessment is normally carried out by a dedicated group of experts called operating experience personnel, who are specially trained in event investigation techniques. Such group of experts can be located at the plant or at the utility headquarters. Regulatory Body should also have a specially trained operating experience personnel, capable of performing independent analysis of unusual events that happened at the plant.

Off-site or external OE can be disseminated by international organizations such as: IAEA/NEA via the incident reporting system (IRS) database of events; the World Association of Nuclear Operators (WANO) also collects and distributes event reports to its members, as does the US-based Institute of nuclear power operations (INPO) for its national and international participants — predominantly operating experience from the NPPs in the USA. It is also the case that some nuclear plant event information is shared nationally or between plants at different sites owned and operated by the same company. For the purposes of this report all these sources are classified as external OE.

All this information needs to be sorted in order to decide which external OE information is relevant to a particular site and what further action, if any, might be appropriate. At NPPs it is usually the responsibility of the Operating Experience Group to facilitate these judgments: this may involve assessment by other on-site colleagues for specialist issues. It is important already at this stage, that the PSA perspective is given due consideration in order to prevent potentially significant event reports being screened out at this stage.

For any incoming external OE information which is judged as requiring no follow-up at site, an outline of the event, (the title is often sufficient), and an identifier should be recorded in a database together with the reasons why the information is deemed ‘not relevant’.

The majority of relevant OE information however, arises **on-site** and can be classified as internal OE. This includes event reports of all types — variously called abnormal event

reports, major and minor events or high level and low level events; also included are deteriorating performance and near-miss reports at the sites operating near-miss reporting schemes. These abnormal event reports will have been immediately categorized, by an appropriate on-site engineer. Examples of categories might be; nuclear plant event, conventional plant event, radiological event, industrial safety event, non-radiological environmental event etc. For each of these categories, there are likely to be sub-divisions (often as many as 30), covering a wide range of eventualities. These are usually numbered sequentially according to the severity of the event. Linked to these categories and sub-categories are reporting requirements and NPPs will also have guidance documents to specify whether it is necessary to undertake an on-site event investigation and furthermore what level of investigation should be carried out; i.e. a thorough formal Inquiry, using the whole range of Root Cause Analysis techniques, conducted by a trained and experienced root cause analysis team and taking several days, or simply an 'Apparent Cause' investigation which may be conducted by a single experienced person and completed in a few hours. These categorized abnormal event reports are usually first presented at some daily on-site meeting.

So, the selection of on-site events for further investigation based on categorization is relatively straightforward and objective, but there will be a large number of other internal event reports that do not meet the criteria for automatic investigation due to their consequences/severity. The problem is to select suitable events from this collection such that valuable on-site resources are used efficiently and at the same time ensure that events with safety significance are not overlooked. Historically, the judgment as to which of the minor events to investigate has been made on a qualitative though somewhat arbitrary basis — shown in the flow chart above as *OE route.* Examples of minor events deemed suitable for proactive investigation might include: non-consequential similar but frequent incidents or ones that involve the recurrence of a particular work group, a particular plant system or component, a particular work activity or a plant status. It may be decided to conduct an investigation on an event based on its potential (rather than actual) consequences; or generally, where it is thought that an investigation of a single event or a group of similar events may yield useful learning points, then a detailed investigation might be initiated.

Event information emanating from on-site which does not result in further detailed investigation is entered into the Trending Programme database of low-level events. This can be periodically examined to identify trends and patterns in the data. When adverse trends are identified they should be treated as events and considered at Event Review Panel (ERP) meetings or similar as described in later sections.

NPP personnel who have the responsibility for initial screening of OE information for relevance and safety significance are frequently concerned that pertinent information may be filtered out; and commonly, where there is any doubt, events are screened 'in' which can often lead to inefficient use of plant resources. Barriers that will help to avoid this include sending incoming external event reports to on-site colleagues for their specialist assessment; in other words seeking a second opinion. However, one hitherto untapped source of guidance may be provided by Probabilistic Safety Assessment (PSA) specialists, particularly where a PSA model of the plant exists.

2.2. INITIAL SCREENING OF OPERATIONAL EVENTS BASED ON PSA

The OE route is the one normally carried out as described in the previous paragraph 2.1. The main purpose of including a PSA route here is to bring in the PSA perspective at this early

stage in the process, to ensure that no potentially significant operational events are lost for further consideration. In addition, the view on the operational events is significantly broadened already at this stage by bringing in qualitative and quantitative knowledge from the PSA. The following paragraphs describe how, and with what methods and tools, that work can be carried out on the PSA route.

As there are many operational events which have to be scrutinized at this stage only a very limited effort can be spent on individual operational events. Thus, efficient methods to deal with the individual operational events are required and available. In a number of NPPs, a regular and systematic process has been established to collect and evaluate operational data for PSA, such as component failures. These data are, for example, used for trending analyses and to maintain a so called "living PSA", which means that a plant specific PSA is updated and actualized in short regular time intervals. As a more advanced application of PSA in some NPPs, so called PSA based safety or risk monitors have been installed, which provide a kind of on-line PSA to follow and investigate the day-to-day risk of a plant. Such risk monitor requires input of operational event data almost on-line. In other plants, the relation of the plant and the PSA is more static. As a consequence of the differing situation regarding the PSA and plant operational information, the actual organization of the PSA route can be only described in a general way here. Actual implementation at a specific plant would largely make use of already existing connections and links, using PSA tools in place. Otherwise, some simple and efficient ways can be established by which the work for the PSA route can be carried out without much additional effort and workload. This is described below.

The first step in the PSA route needs to consider whether or not a particular operational event is within the PSA perspective. The PSA usually provides ordered lists of items modelled in the PSA, such as equipment, systems and human interactions. These listed items are named PSA related items (equipment, systems, human interactions etc.). Today these lists are normally in electronic format and structured in a way to enable a quick check whether or not an event affects PSA related items. There are systems in the plant which are usually not of interest for a PSA, and thus outside of its scope, for example equipment in the waste treatment plant. Although failures in the waste treatment plant may cause a limited release of radioactive materials, they may still be significant enough to warrant in depth analysis on the OE route. On the other hand, there are systems which are not viewed as strictly safety related on the OE route, but which may be significant under PSA perspective. An example of such system found at one NPP was the instrument air system. The safety equipment supported by instrument air at this plant is either organized in a fail safe manner, thus a failure of instrument air does not make these systems unavailable, or local air bottles are provided to operate devices although only for a limited time. However, instrument air is also required to operate the main condensate and feedwater systems, which are required to be used as high and low pressure injection systems after an incident. Moreover, a loss of instrument air directly results in the important initiating event "total loss of feedwater and condensate system". Thus, the PSA instrument air turned out to be a very important (risk relevant) supply system. Apart from the check of and comparison with the lists of PSA related items, this first step can be simply based on the judgment of the PSA team using the PSA expertise.

Most of the PSAs today provide in addition to the lists of PSA related items, numeric values for the importance. Details regarding the definition and uses of the different importance measures can be found in the IAEA Safety Series No. 50-P-4, pp. 90 [Ref. 1]. One of the importance measures is the Fussell-Vesely importance, which is the fractional contribution of the failure of a particular item to the overall core damage frequency. This allows a very quick

estimate to be made of the risk significance for events, which can be roughly depicted by failures of PSA related items such as deficiencies in equipment, systems or human errors.

Simplified or condensed representations can be derived from the PSA to carry out a quick and approximate estimate for the risk induced by an operational event. In France (EdF) for example a table in matrix form has been generated based on the PSA to make a quick rough estimate for the risk significance of an event. The table has a horizontal axis listing safety functions (called lines of defence) and a vertical axis with initiating events. Based on the PSA, fragilities (or impact) have been calculated for the matrix allowing to estimate the risk impact of events involving an initiator or a degradation of lines of defence, or both in combination [see Ref. 2].

If an operational event is found to be within the PSA perspective and considered to be sufficiently significant based on a rough risk estimate, the event is recommended to undergo in depth analysis.

2.3. IN-DEPTH DETERMINISTIC EVENT INVESTIGATION

The goal of event investigation is to improve overall plant safety and reliability of operations by learning from experience.

Examination of the traditional Event Investigation process will identify stages where decision-making can be greatly enhanced by the introduction of supplementary information from PSA-based analysis. Consider the basic Event Investigation process in five stages:

1. Establish the facts — **what** happened?
2. Analyse data to determine **how** it happened, and the causes or **why** the event occurred.
3. Develop recommended corrective/preventive actions.
4. Report the lessons learned, internally and externally.
5. Conduct an Effectiveness Review.

This is a well-established but purely qualitative approach. Stages 1 and 2 can be undertaken using selected techniques from a number of root cause analysis methodologies; (as a result of a co-ordinated research project, the IAEA has produced guidance on the selection of "Incident Analysis Methodologies" from a toolbox of techniques available to identify causal factors in IAEA-TECDOC-1278 (Ref. 3). With this approach, the chosen methodology does not simply ask **what** happened, but also **how** and **why** it happened. The chosen methodology should be effective in identifying subtle, underlying root causes of undesirable conditions and in determining effective corrective actions. Root causes can be defined as the underlying events or conditions that, if corrected, will prevent or minimize the likelihood of recurrence of a problem.

Before attempting to determine the cause(s) of an event, the facts must be established, i.e. **"what happened"** must be clearly understood. "What happened" is the condition as a consequence of undesirable plant, procedural or a person's performance — at the time of the event. **"How it happened"** is determined by understanding how the undesirable performance failed to achieve the desired result. Those factors or conditions that adversely affect expected performance are the causes of an event — **"why it happened"**.

One of the first priorities when beginning any investigation is, normally, to determine as much as possible about the activity that was being performed. This is done typically by a review of work documents, logs, alarm printouts, personnel reports, procedures and other documents etc. in an effort to determine **what** the task was about and **how** it was performed. This process may be carried out either by paper and pencil task analysis or a walk-through task analysis — and frequently by both.

Paper and pencil task analysis is a method where a task is broken down on paper into sub tasks identifying the sequence of actions, instructions, conditions, tools and materials associated with performance of a particular task.

What happened must be determined before **How** can be established. Only then can **Why** be deduced.

An event and causal factor chart (ECFC) is one way to graphically display an entire event. The chart is often a key tool in root cause analysis. The chart displays the sequence of events plotted on a time line, with appropriate start and end points. It can be plotted on a large-scale wall chart to enable the whole sequence to be seen, and notes to be added. As the event line is developed, additional situational features such as related conditions, secondary events and presumptions are added. Barriers, changes, causes and effects can be graphically shown.

It is important that such a chart is developed iteratively. A preliminary chart can be developed, based on the initial available information, and indicating any presumptive data. Gaps in the investigator's understanding of the event become apparent, making the preliminary chart a valuable aid to preparing questions to be asked when interviewing personnel involved in the event. Following each interview, the chart should be updated with the new information obtained. In this way, probable causal factors become evident as the chart is developed. Often, less obvious causal factors become evident through this technique, making it a powerful analysis method.

Event and causal factor charting is an advantageous and effective technique because:

- By using specified symbols and line forms, the chart depicts the exact sequence of events, enables information to be organized logically and prompts the identification of: undesirable conditions, secondary events, presumptions, causal factors, changes, primary events and control barriers that are non-existent or unreliable.

- It captures the entire situation in one integrated frame making it straightforward for the reader to recognize the key points of the event.

- It helps to ensure objectivity — it is based on verifiable facts, and as the chart is developed, causal factors become evident. It also provides a cause-oriented explanation of the situation.

The chart can also be used to display the cause and effect relationships that exist within the conditions surrounding an inappropriate action. Each condition identified is then itself treated as an effect to determine its cause, and these new conditions are further incorporated into the chart. This cause and effect analysis is repeated until further analysis will not benefit the correction of the initial problem.

Corrective actions based on causal factors rather than symptoms are likely to be effective and long lasting. These reactive actions based on casual factors together with pro-active preventive actions based on weak barriers and other findings will ensure that the number of repeat problems is very much reduced, resulting in fewer subsequent events that may degrade plant safety and reliability.

The product of any event investigation will be (at least), a number of root causes, contributory causes and an assessment of barriers/defences. From this information, recommended corrective/preventive actions can be developed to obviate recurrence of the event under investigation or to prevent a 'new' event. Note that these recommended corrective actions are pure or ideal solutions to remove causes and install or repair ineffective/missing barriers, and are not moderated by constraints such as finance or plant availability. Additional information arising from event investigations may identify error precursors and/or latent weaknesses that did not contribute to the event being investigated but which nevertheless, may cause a future event. This bonus information too, needs to be addressed and demonstrates how event investigation techniques can be used proactively — hence **preventive** actions as well as corrective actions.

On completion of an investigation by a trained individual or a team of investigators and delivery of the report, it is the responsibility of other NPP/operating organization groups to decide which of the recommendations, including any from PSA analysis, shall be implemented and to set and track actions with timescales. The forum will also generally decide on which events contain significant learning points for others and which should therefore, be reported internally and/or externally.

At many NPPs the responsibility for making these decisions is vested in an Event Review Panel (ERP) or similar, which meets at some pre-determined frequency to review selected OE information from on- and off-site. The ERP will be chaired by a senior NPP manager and comprises representatives from various plant departments. At least one member of the OE group should be present and it would be prudent to have representation from PSA specialists, especially when there is an input from the *PSA route*.

2.4. PSA-BASED IN-DEPTH EVENT INVESTIGATION

As shown in the overall flow diagram, (see Fig. 2), the precursor event analysis case is forwarded to the PSA group from the operating experience group after or during their in depth analysis of the operating event. All the information available or elaborated regarding the operational event and its implication should be provided to the group carrying out the PSA-based evaluation.

There are two main steps for detailed precursor analysis as shown in the main flow diagram:

1. Relating the operational event to the plant specific or at least a plant type specific PSA model and finding out whether or not the event can be adequately analysed by PSA based models. Depending on the type of operational event, there are events which do not fall into the PSA perspective or cannot be treated in a useful way by this approach. If this is the case, it should be noted, with a short justification, an information notice sent to the operating experience group and the process stopped. Otherwise detailed analysis is carried out in the second step.

2. Precursor analysis, mapping of the precursor on the PSA model, qualitative and quantitative evaluation, interpretation of results and derivation of insights.

The use of PSA based event analysis can serve two purposes:

- it can provide a numerical value for the risk significance of an operational event, and
- it increases the understanding of the plant vulnerabilities given the event occurrence. Basically, in precursor analysis a re-analysis of the PSA is performed under the condition that the operational event has occurred.

As outlined in more detail below the analysis comprises the following steps:

1. Precursor event review and analysis
   - understanding the event
   - identify causes, important factors and develop the context of the event in terms of the PSA perspective.

2. Mapping of the precursor on the PSA, logic presentation
   - relate the event and its implications to the PSA model
   - are PSA models adequate?
   - revise, extend if necessary.

3. Quantification
   - estimate failure probabilities
   - if required, perform human reliability analysis (HRA)
   - adapt PSA reliability models.

4. Initial evaluation
   - recalculate conditional core damage probability for all appropriate sequences.

5. Recovery actions
   - determine potential recovery actions,
   - model recoveries.

6. Evaluation
   - calculate new importances,
   - perform uncertainty and sensitivity analyses.

7. Extension
   - what would happen if the event occurs under different conditions and context?

8. Interpretation, conclusions, insights, corrective measures

Basically there are the following two types of precursor events:

(i) The precursor event represents a transient which interrupts normal operation of the plant, thus there is a real effect on plant operation. In this case the event can be easily related to an initiating event of the PSA (if modelled) and the accident scenarios affected by the event are those developing from this initiating event.

(ii) The precursor event involves the unavailability or a degradation of equipment or systems without an immediate impact on plant operation. If the precursor event is related to one (or several) safety functions, a systematic survey of the principal scenarios on which the precursor event impacts needs to be done. First, all the initiators which require the affected safety function(s) need to be identified. In the event scenarios or sequences developing from these initiating events (Event Trees) only the scenarios which entail the precursor event are retained. Preferably the computerized PSA database is used for this purpose to ensure that the search and identification process is exhaustive.

Precursor events which entail both, an initiating event and equipment or system unavailability, are also possible and both types of impacts need to be included in the subsequent analysis in a combined manner.

The primary result is the conditional probability for core damage, given that the precursor event has happened. A detailed description of the procedure for PSA based precursor analysis is given in the following paragraphs.

2.4.1. Purpose of PSA based event analysis

The fundamental purpose of PSA based analysis of operational events or of precursor analysis is to find answers to the following two basic questions:

a) How could a precursor event have degenerated into an accident with more serious consequences?
b) Is it possible to determine and measure what separates a precursor event from a potential accident with more serious consequences?

Thus, the analysis contains a qualitative and a quantitative element:

Qualitative element of the precursor analysis. Finding the qualitative lessons to be learnt from the actual events considered as precursors for potentially more serious accidents. This gives an increased understanding of the vulnerabilities of the plant given the event occurrence.

Quantitative element of the precursor analysis. Measuring the severity of the event. In this quantitative part of the analysis, the conditional probability that an operational event would progress to accidents with unacceptable consequences is calculated. Based on this information, events can be ranked according to their risk significance. Moreover it can be used to prioritize which weaknesses should be handled first, and to assess the level of safety of the plant.

Basically, in precursor analysis a re-analysis of the PSA is performed under the condition that the operational event has occurred.

Special attention is given to operating experience feedback information: by extrapolating precursor events to accident scenarios with serious consequences, valuable insights can be gained about serious incidents on the basis of minor events, without suffering their real consequences. The method thus makes it possible to learn from minor precursor events in the same way as we would learn from real accident experience.

2.4.2. Background and approach

Precursor events are operational events that may constitute important elements of accident sequences potentially leading to unacceptable consequences. The most commonly used definitions of unacceptable consequences are core damage, beyond design conditions or unacceptable releases of radioactive material to the environment.

The PSA model used for precursor analysis should be sufficiently complete in scope to include the plant response to the operational event. It should be plant specific or at least plant type specific, to reflect the operational and design features of the plant with acceptable accuracy. It should include all relevant initiating events and all relevant operating conditions of the plant. For precursor analysis the PSA model sometimes has to be refined to a sufficient level of detail to reflect the precursor event analysis. This could involve modelling of missing accident sequences, missing component failure modes, or restoring accident sequences that were originally truncated or screened out. This could include changes in the fault tree model of the PSA or re-modelling or modelling of additional operator actions within the fault trees.

In precursor analysis a re-analysis of the PSA is performed under the condition that the operational event has occurred. On this basis new conditional probabilities of accident sequences are calculated.

2.4.3. Analysis and quantification of conditional probabilities

As mentioned above, a re-analysis of the PSA needs to be performed under the condition that the operational event considered has occurred. In performing this task, all the basic events of the PSA model should be checked whether or not their reliability parameters are impacted by the operational event, and, if necessary these parameters have to be re-assessed. Basic events representing failed components should be modelled as failed for example with house events[1], i.e. these failed components should not be represented as a failure event with an associated failure probability in the modified PSA model.

For operational events involving component malfunctions or unavailabilities, but no initiating event, all initiating events have to be postulated for which the degraded/failed components are demanded during accident sequences. The actual or estimated duration d of component unavailabilities (e.g. half test interval) have to be taken into account. By multiplying this duration d with the frequency f_i of the initiating event i the conditional probability of the occurrence of the initiating event is calculated:[2]

$$P_i = d \cdot f_i \qquad (2.4\text{-}1)$$

and the conditional probability of the accident sequences is:

---

[1] House events in fault trees are switches used to switch on or off parts of the logic PSA structure.

[2] For high frequency or long duration events the more appropriate exponential representation $(1-\exp(d*f_j))$ should be used.

$$P\{\text{accident} \mid \text{precursor j}\} = \sum_i P_i \cdot \Pi_i \{\text{accident} \mid \text{precursor j}\} \quad (2.4\text{-}2)$$

with:

Π_i = conditional probability of all accident sequences which have to be taken into account given the occurrence of the precursor event j and the initiating event i.

2.4.4. Results and interpretation

The main results of precursor investigations are the conditional probabilities according to Formula (2.4-2). As a numerical threshold for judging the significance of operational events based on a conservative estimate of the conditional core damage probability a value of 10^{-6} is widely accepted and used. Multiplying the conditional probability of the precursor event j with the frequency, i.e. one event within the observation time in reactor years, and summing up all precursor events within the observation time yields:

$$\lambda = \frac{\sum_j P\{\text{accident} \mid \text{precursor j}\}}{\text{observation time}} \quad (2.4\text{-}3)$$

λ is an estimator for the unacceptable consequences, typically either core damage frequency or beyond design basis frequency. The estimator is called core damage index, beyond design basis index, or simply safety or risk index.

2.4.5. Procedure

Figure 3 shows the task flow for PSA-based precursor analysis. The individual tasks are explained in the paragraphs below.

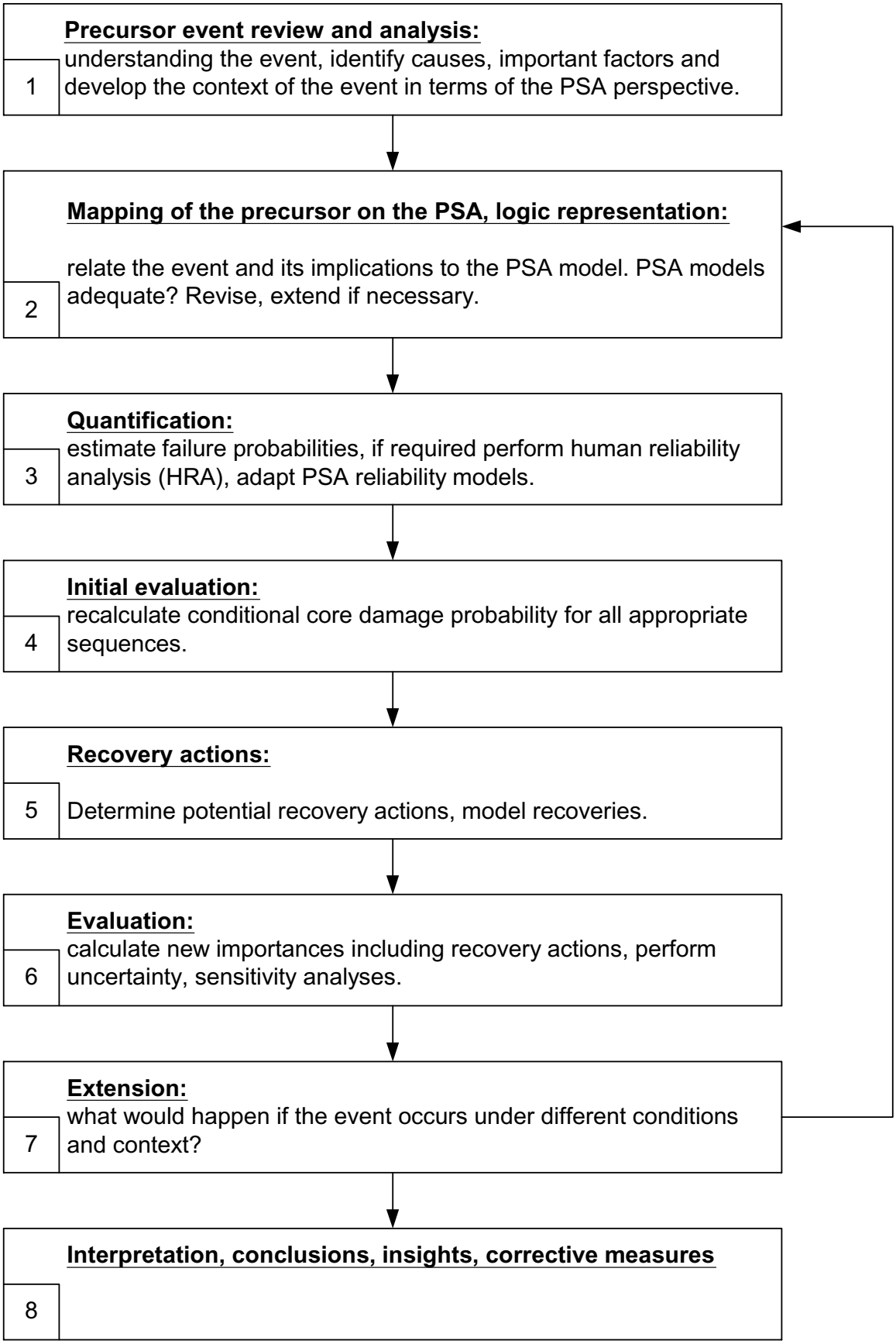


FIG. 3. Procedural tasks in precursor analysis.

Task 1, Precursor event review and analysis: Understanding the event, identify causes, important factors and develop the context of the event in terms of the PSA perspective.

The objective of this task is to develop a thorough understanding of the precursor event and of its context. Gathering of additional information regarding the event and related plant design and operational features is usually needed for this task, but also for some of the following tasks. The information to be compiled and reviewed includes the following items and aspects:

- Initial status of the plant;
- Chronology of events;
- Equipment and system deviations, failures and unavailabilities;
- Operating staff behaviour, actions, deviations and errors, especially actions not covered by procedures and training;
- Status of related procedures, whether they were adequate, inappropriate or even missing;
- Favorable events, systems which worked successfully, fast detection, successful recoveries;
- Conditions or events of interest which occurred or were identified for some time period (like 1-2 weeks) before and after the incident to be sure that hidden complications are not left unaccounted for in the analysis.

This information is reviewed and analysed to identify causes and important factors, and in order to develop an appreciation of the context of the precursor event. A systematic description is established containing the above information and the results of the initial analysis.

Task 2, Mapping of the precursor on the PSA, logic representation: Relate the event and its implications to the PSA model. PSA models adequate? Revise, extend if necessary.

In order to relate the precursor event to the PSA, the analyst determines which accident sequences are involved or could be involved, what fault tree models, basic events or operator actions are affected, and what recovery actions could be applied or are made impossible. In the mapping process the relation between the observed precursor events with the events described in the PSA models is established. Basically there are the two following types of precursor events:

(i) The precursor event represents a transient which interrupts normal operation of the plant, thus there is a real effect on plant operation. In this case the event can be easily related to an initiating event of the PSA (if modelled) and the accident scenarios affected by the event are those developing from this initiating event. A subtype of this kind of events are disturbances which alone do not cause an initiating event, but would do so if combined with other events. Handling of such events can be carried out with an additional probabilistic model (e.g. a small event tree).

(ii) The precursor event involves the unavailability or a degradation of equipment or systems without an immediate impact on plant operation. If the precursor event is related to one (or several) safety functions, a systematic survey of the principal scenarios on which the precursor event impacts needs to be done. First, all the initiators which require the affected safety function(s) need to be identified. In the event scenarios or sequences developing from these initiating events only the scenarios which entail the precursor event are retained. Preferably the computerized PSA database is used for this purpose to ensure that the search and identification process is exhaustive.

Precursor events which entail both, an initiating event and equipment or system unavailability are also possible and both types of impacts need to be included in the subsequent analysis in a combined manner.

Representation entails the modelling of the operational event for the accident scenarios identified in terms of one or several event trees. This kind of representation has two advantages:

- It provides a clear and structured representation of accident scenarios,
- It provides the basis for the subsequent quantification task.

Depending on the type of the given operational event, it is sometimes necessary to adapt or extend the models of the reference PSA due to the following reasons:

- Most PSAs only retain events and accident sequences that contribute in a non-negligible manner to the core damage frequency or other defined unacceptable consequences. Sometimes it is necessary to restore accident sequences that were eliminated or truncated out in the reference PSA.

- The level of detail of the PSA events and models is insufficient for directly depicting the operational event in the PSA. In this case, additional considerations are necessary to establish the connection between the operational event and the PSA events and models.

- The PSA is incomplete or inadequate. This would also mean that the reference PSA should be revised if necessary.

The derived event trees for precursor analysis should be as simple as possible. For this purpose, the scenarios which are impossible or negligible considering the associated and available lines of defence or safety functions, are deleted. In general, the quantification elements connected to the event trees of the reference PSA already allow simplification by only retaining the dominant scenarios, even before performing the tasks of quantification, which follows. Further simplification could be possible by integrating similar or analogous scenarios.

Task 3, Quantification: Estimate failure probabilities, if required perform human reliability analysis (HRA), adapt PSA reliability models.

This task consists of mapping quantitative precursor data onto the model developed in the previous Task 2. The objective is to carry out the quantification reflecting the conditions given for the precursor event. This quantification may be conservative, but not excessively conservative. In practice this is done by:

- Listing the characteristics of each event or sequence (time duration, probability, mission time, failure rate, recoveries);
- Determining those parameters which reflect the specific conditions of the precursor event.

The probabilities of the basic events, in the model which had happened during the incident are set to logical failed or a failure probability of one is used (see remark in 2.4.3). The probabilities of basic events which did not happen remain at the standard values of the reference PSA. In

certain cases the conditions of an incident can lead to a modification of the probabilities of events which did not happen, by increasing or decreasing the probabilities from the reference PSA, according to the favorable or unfavorable context of the incident, compared with the standard situation.

For equipment or operator degradations, detailed systems analysis or human reliability analysis may be required to get an acceptable level of detail and rigor in the revised failure probabilities. However, conservative screening or bounding values may be used as a first approximation. Only if the results indicate that the screening values have large impact, is more detailed analysis required.

Task 4, Initial evaluation: Recalculate conditional core damage probability for all appropriate sequences.

After assigning the appropriate failure data to the basic events and initiating events, the accident sequence conditional probabilities are calculated. Depending on the implications of the precursor event, the evaluation is done by manual or computerized calculation:

Manual calculation can be used for:

- First evaluation
- Conservative calculation
- Simple initiating event
- When the number of scenarios affected is limited or there is a dominating character of a few scenarios.

Calculation with computer is needed when:

- Precursor events affect numerous sequences
- Importance of temporary dependencies needs to be evaluated
- Complex combination of events is involved.

However, performing computerized calculation is not always directly possible. The analysis of certain incidents may necessitate model modifications which have to be carried out by the PSA model builders.

The result of the initial evaluation are accident sequence expressions (in terms of cutsets[3]) sorted according to their conditional probability. At this point, potentially important sequences which may be affected by incident recovery actions should be identified for the following task.

Task 5, Recovery actions: Determine potential recovery actions, model recoveries.

The objective of this task is the determination of appropriate recovery actions to be applied to the accident sequences in terms of cutsets based on the conditions of the incident, personnel available, and plant operating and emergency procedures.

[3] Cutsets are the minimal combinations of failure events used in PSA to logically represent accident sequences.

The determination of the recovery failure probabilities may require detailed analysis. Note that for component unavailability situations which have existed through several shifts, the recovery analysis should consider any significant variations in personnel and skills, or other factors which could impact recovery. The recovery actions credited in the original PSA should be reviewed to assure that the incident being evaluated does not impact the recovery action failure probabilities or render any recovery actions impossible.

Task 6, Evaluation: Calculate new importances including recovery actions, perform uncertainty, sensitivity analyses.

The objective of this task is to carry out the evaluation of conditional probabilities for the accident sequences, including the recoveries identified in the previous task. The evaluation should include analysis of uncertainties and calculation of importances, usually the Fussell-Vesely importance, risk reduction, and risk increase importances. The Fussell-Vesely importance indicates the percent contribution to the conditional accident probability involving the event, for which it has been calculated. The risk reduction ratio indicates the amount of reduction in the conditional accident probability to be gained if the considered event is assumed to be improbable (failure probability = 0.0). The risk increase ratio indicates the factor by which the conditional accident probability would increase if the event is assumed to happen with certainty (failure probability 1.0). For key modelling and other background assumptions, sensitivity studies should be carried out to obtain an appreciation of the variability induced by these assumptions.

Task 7, Extension: What would happen if the event occurs under different conditions and context?

An operational event occurs within a specific context and situation. The objective of this task is to ask the question what would happen if the event would occur under different conditions or in a different way. Typical parameters for which this question could be raised are the following:

- plant type
- initial condition of the plant
- chronology of events in the incident
- environment for common mode failures
- different human behaviour
- different context for human interactions.

The variation of parameters needs to be made with care, because for numerous incidents most of the parameters are fixed within the context and variation makes no sense.

A significant variation of the context, situation and conditions will usually require a complete re-analysis of the precursor event, which has to be carried out beginning with Task 2 of this procedure.

Task 8, Interpretation, conclusions, insights, corrective measures

The objective of this task is to interpret and document the precursor analysis. The analysis information and results are reviewed to determine key contributors in terms of dominant accident scenarios, important components or operator actions. The importance measures

obtained in the evaluation can be used to guide the review. In addition, the key features are identified that prevented the event from becoming more risk significant by using the risk increase importance measure. Corrective measures can be specifically designed and evaluated if required.

The quantitative interpretation is based on the evaluation of the conditional accident probability (risk index). The risk index enables precursor events to be ranked ensuring that the most important precursors are dealt with preferentially.

2.5. IMPLEMENTATION

In the model described here, two of the inputs to the event review panel (ERP) or similar forum are the outputs from qualitative deterministic analysis (the event investigation) and the quantitative PSA analysis. Consideration of both types of information provides a more objective basis for decision-making when it comes to select which of the recommendations to implement and to specify the timescale.

Assuming that all actions emanating from the ERP (corrective, preventive or reporting requirements), are entered into an action tracking system, a further function of the ERP is to provide a review of effectiveness, i.e. to monitor the timeliness of implementing corrective actions, and to adjust the priority of corrective/preventive actions if this becomes necessary in the light of recent operating experience; and to ensure that the completed actions have been successful in preventing recurrence of the event.

3. CASE STUDY

In this Chapter, the methodology described in Chapter 2 is demonstrated by analysing an event using both the deterministic and probabilistic approach.

3.1. BRIEF DESCRIPTION OF THE EVENT

Plant shutdown due to reactor coolant pump (RCP) bearing temperature high indication

On the 24 February at 22:20 hrs. the night shift noticed an increase in upper motor thrust bearing temperature of RCP No 2 (temperature detector TE 695 B). The PIS (Process Information System) recorded a continuous temperature increase from 57°C to 62°C during the last 17 hours with a tendency toward an increase in the rate of temperature change. Previous shifts had not noticed the increasing temperature. By replacing two input modules together with direct measurement of the signal from the process it was possible to confirm the authenticity of the PIS-indication. No transient was observed in the core cooling system. Temperatures of other RCP No 2 motor bearings were normal. For this reason the crew deduced that the temperature increase could be a consequence of thrust bearing wear or a failure of the temperature detector.

After continuous monitoring of the bearing temperature, which was rising all the time, the crew made the decision on the 25 February at 01:18 hrs. to reduce the load at a rate of 6 MW/min according to procedure GOP-3.1.300 “Power Operation”. Because the bearing temperature increased at a rate higher than predicted, the crew raised the load reduction rate to 12 MW/min (at 01:48 hrs.), which meant transfer to the Abnormal Operating Procedure AOP-SEC 8 “Rapid Load Reduction”, with simultaneous implementation of actions per procedure GOP-3.1.300. After 11 minutes, due to the fast increasing bearing temperature indication, the load reduction rate was raised to 20 MW/min and, almost immediately afterward, to 30 MW/min. (at 02:05 hrs.). All systems responded as expected. At 02:09 hrs. the bearing temperature reached 89°C, which led the crew to implement the procedure AOP PRI-4, “Reactor Coolant Pump Malfunction” and, accordingly, to trip the reactor manually (at a reactor power of 28%). After implementing the first four steps of procedure E0P-E-0, “Reactor Trip or Safety Injection” the RCP No 2 was stopped. The actions were continued according to the procedure EOP-ES-0.1 “Reactor Trip Response”, which later enabled stabilizing the parameters in MODE 3, Hot Standby at 09:26 hrs.

The subsequent problems explained below made the original event (the manual trip) far more significant.

Three-inch steam pipe rupture following plant shutdown

Following the fast plant shutdown, Main Control Room (MCR) operators heard unusual noises from the turbine building (TB). The TB operator reported a steam leak. MCR operators consequently performed main steam isolation at 02:10 hrs., requiring both electrically driven Auxiliary Feedwater System (AFWS) pumps to be manually started (02:16 hrs.). After closure of the Main Steam Isolating Valves (MSIVs), a rupture was discovered in a 3-inch steam pipe knee. The failed section of piping was immediately isolated by valves on each side of the break point.

During the steam release in the turbine building, the failed pipework was moving/swinging from its original position and hitting the Fire Protection System (FPS) pipeline (sprinkler system). One section of FPS pipework became detached at a T-joint and water leaked out. The FPS standby pump then correctly started to top up water to the leaking system. This section of the FPS was then isolated. No equipment was adversely affected by water but a fire watch was established on that elevation.

The failed 3-inch steam pipe also caused deformation of a cable tray on a non-safety electrical train. Cables were briefly exposed to steam but visual inspection revealed that they had not been affected. The released steam also penetrated an electrical cabinet; some water condensing on the inside walls and draining inside the cabinet. The cabinet was cleaned and dried and visually inspected; no problems were found.

The plant has an erosion-corrosion programme in place. The program comprises preventive inspections of secondary side pipelines. The program was developed on the basis of recommendations from NUREG-1344 and, within the framework of the inspections made during the plant outages, every year about 60 to 80 components were inspected. Out of this, approximately 20% is of nominal diameter of less than 4". The line which was broken is within the scope of the inspection program. During the plant outage 2000, a part of this line was inspected and the smallest thickness measured was 5,90 mm. Since the results of inspections did not indicate an actual wearout trend, the inspection was not performed along the overall pipeline.

Power-operated relief valve operation

Due to a pressure rise in the secondary side resulting from the Main Steam Isolation Valve (MSIV) closure, Steam Generator Safety Valve No 1 had opened and closed twice. It is expected that small pressure increases would be controlled by automatic operation of a Power-Operated Relief Valve (PORV), however, it could not be confirmed that the PORV had actually performed this function. Approximately one hour after MSIV closure, bypass valves were opened and steam dumped to the main condenser (03:10 hrs.).

Auxiliary feedwater system (AFWS) pump problems

On the 25 February, following the reactor trip, at 02:16 both AFWS motor-driven pumps (MDPs) were started. Pump 2B was stopped at 02:26 and restarted again at 04:58. At 09:30 the temperature of the axial bearing on Pump 02B reached 137°C, while the temperature of the axial bearing on Pump 01A was 84°C. Due to the unusual temperature increase, both motor-driven pumps were stopped and the turbine driven pump 03C was started. As a priority measure, the axial bearing of Pump 02B was replaced and the gap of the “balancing drum” was reduced from 0,11 mm to 0,05 mm. At the restart of the pump on 26 February at 06:00, the temperature stabilized upon 7 hours of pump operation at 71°C.

From the Process Information System (PIS) indication it could be seen that the temperature of the axial bearing of Pump 01A would have increased to values beyond 84°C if pump operation had continued. A working order was issued and the gap of the “balancing drum” was reduced from 0,10 mm to 0,06 mm. The temperature then stabilized at 76°C, following six hours of operation.

Overheating of axial bearings on AFWS MDPs has occurred in the past on several occasions. Experience showed that overheating of axial bearing could be prevented by reducing the gap of the “balancing drum”. Pump manufacturer's instructions were to set the gap at 0,002" – 0,005" (0,0508 mm–0,127 mm). However, actual experience demonstrates that a gap of 0,11 mm already causes overheating of pump's axial bearing.

How long did the condition described above for the two electrically driven AFWS pumps exist? The problem could be detected in the periodical tests of the AFWS. However, it appeared that in the periodical tests during power operation the pumps are run for 15 minutes only and via a recirculation line to the condensate tank. Therefore, it was concluded that the condition would probably not be detected by following the testing procedures used prior to the incident.

3.2.QUALITATIVE ASSESSMENT

The deterministic event analysis is presented in Figure 4 in the form of an Event and Causal Factors Chart.

Reactor scram due to fault of temperature detector TE 695 B

In the terminal box of the motor of Reactor Coolant Pump No 2 all junctions were checked and all actual resistances were measured on all three temperature detectors (thrust bearing upper shoe, lower shoe and upper radial bearing). The resistance of the impaired detector (TE 695 B) was found to be significantly higher than of the other two.

Simultaneously, ferrographic analysis of both RCP oil samples was performed, which has shown that the concentrations of wear particles in both samples were normal. Based on all information gathered and on the fact that all other parameters on RCP No 2 were normal during the transient, it was concluded that the TE 695 B high indication was false.

Root cause:
No procedural guidance on bearing temperature parameters inspection at shift hand over. In addition, chosen bearing temperature alarm settings were not reached to alert operators of changing trends in a timely manner to allow for the gradual reactor shutdown.

Three-inch steam pipe rupture

At the damaged knee the thickness of the line wall was smaller than 1 mm. The cause of wall thinning was found to be erosion on the steam line of a diameter of 3 inches (7.6 cm). The wall got so thin that the knee broke following the pressure transient, which caused the steam blowdown into the turbine building atmosphere. During the shutdown, the affected part of the line was replaced together with the associated knees. Also, the thickness of the pipe wall was measured along the overall pipe length and no deviations were found on the straight parts. All other knees were also checked. At four knees, wall thickness was measured to be smaller than allowable. These pieces were also replaced.

The cable trays impacted by the steam leak were systematically tested and checked for possible mechanical or thermal damage, and equipment connected to them monitored for possible malfunctions. Also all breakers in the cabinet penetrated by the released steam were inspected and tested.

Root cause:
Failure of the surveillance programme to detect wall thinning of pipe knees ≤ 4-inch diameter.

Power-operated relief valve operation

The need was identified to establish why it did not function, and a mechanical problem due to sticking was suspected.

Auxiliary feedwater system (AFWS) pump problems

The high bearing temperatures were the result of overload of the bearings caused by increased tolerances (gaps) in the balancing drums.

The problem should have been detected in the periodical tests of the AFWS. However it appeared that in the periodical tests during power operation the pumps were run for 15 minutes only and via a recirculation line to the condensate tank. It was therefore concluded that the condition would probably not be detected following the testing procedures used prior to the incident.

Root causes:
The "balancing drum" clearance on both motor driven AFWS pumps were out of adjustment. The monthly testing of AFWS was too short to stabilize bearing temperatures, and so could not detect the overloaded bearings.

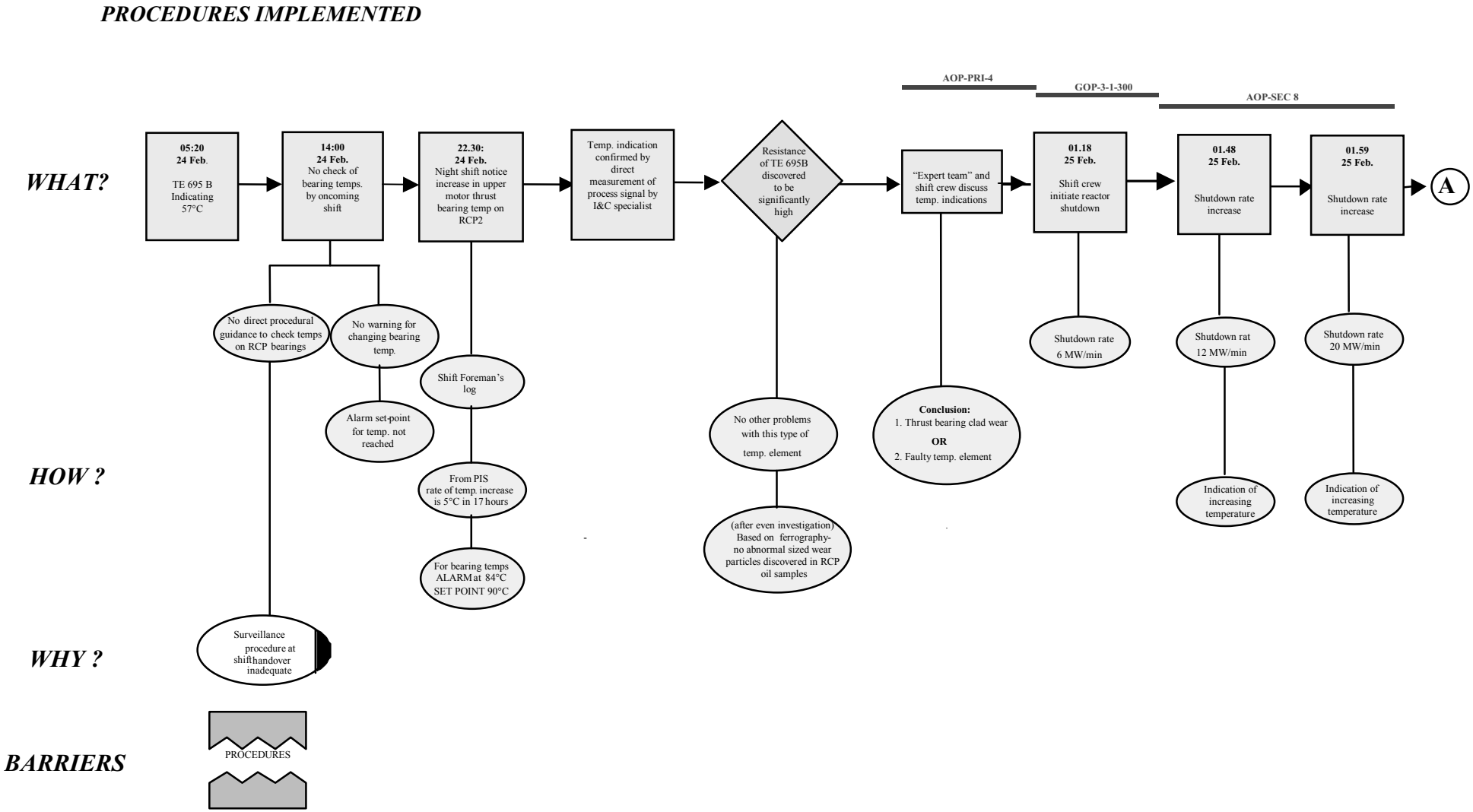


FIG. 4. Event and causal factors chart

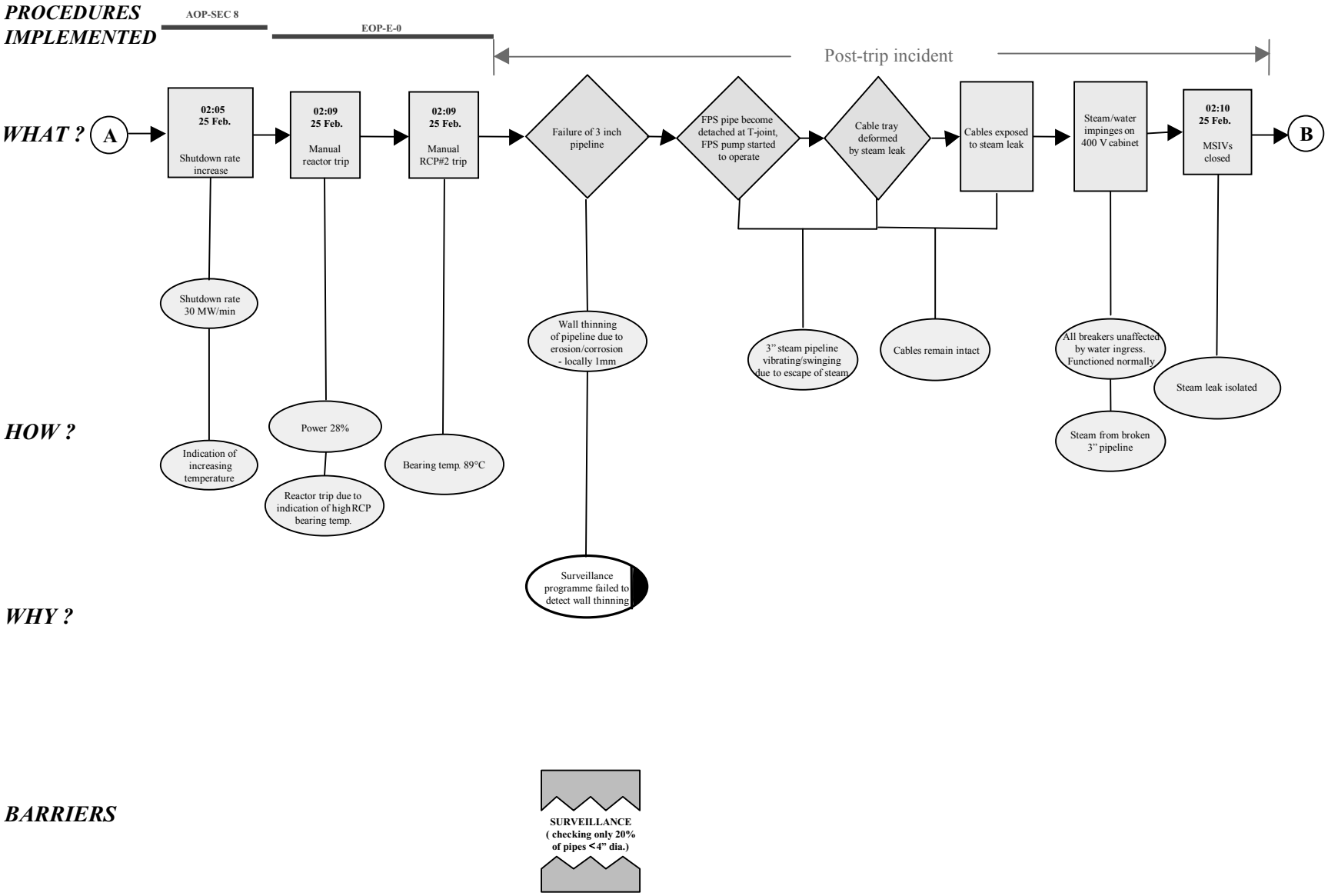


FIG.5. Manual Reactor Scram following an Increase in Indication of RCP2 Motor Upper Bearing Temperature

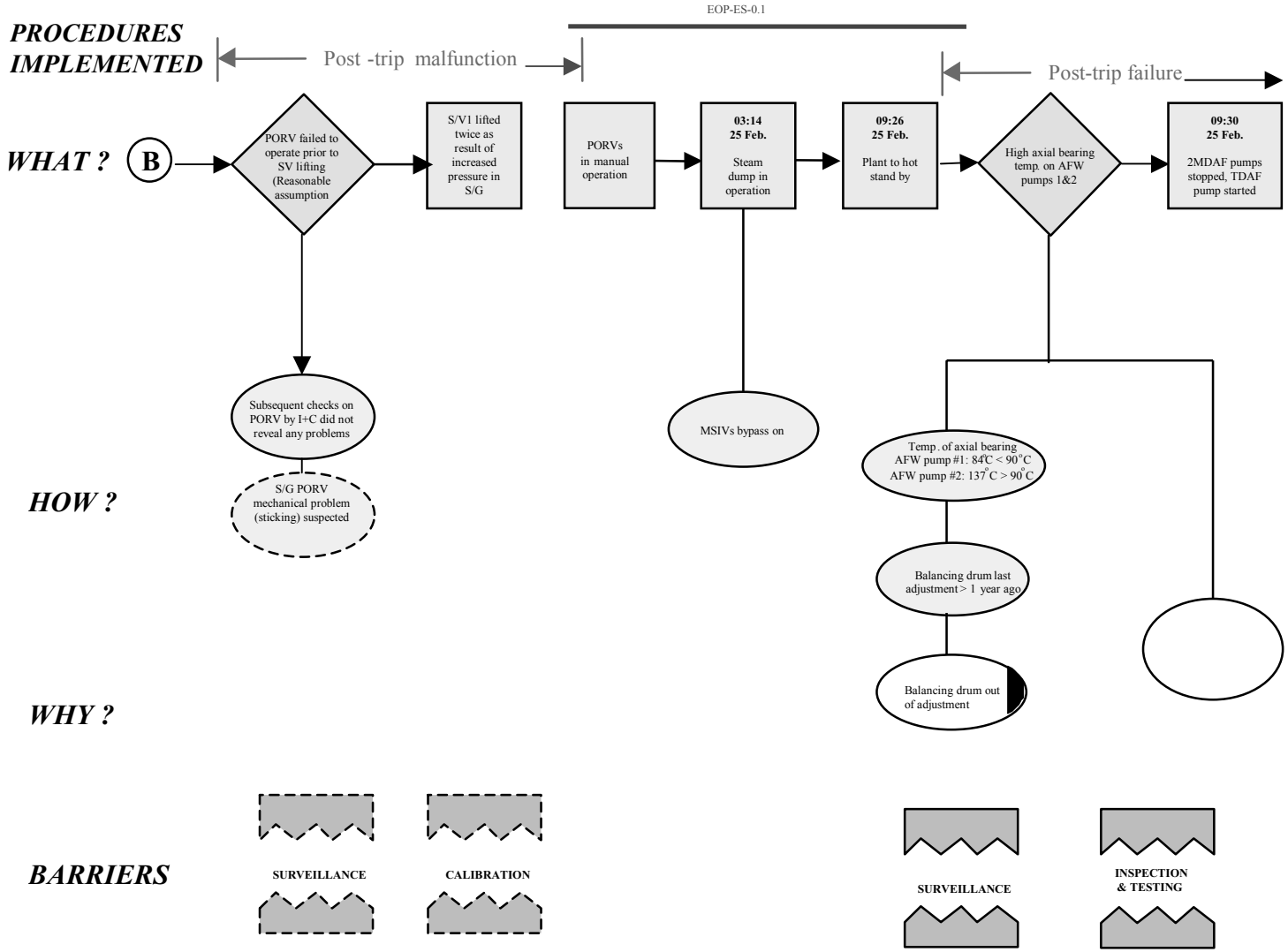
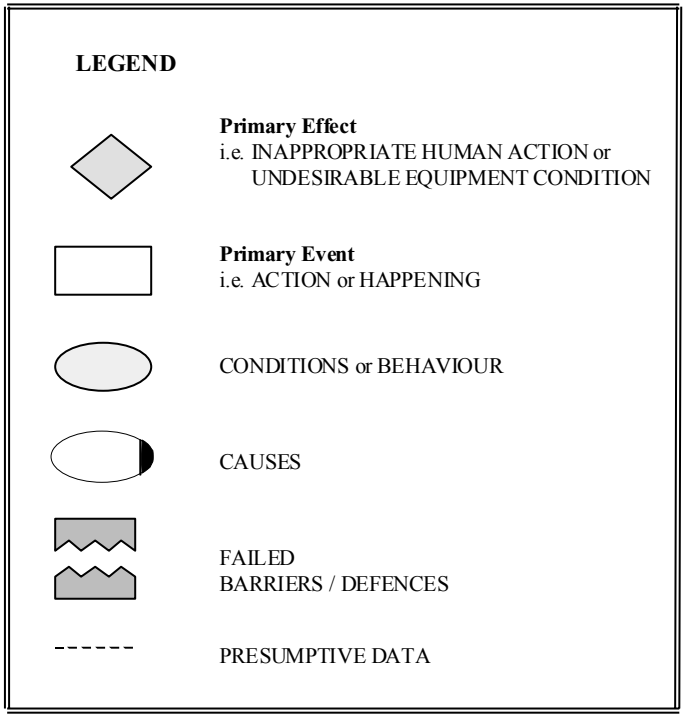


FIG. 6. Manual Reactor Scram following an Increase in Indication of RCP2 Motor Upper Bearing Temperature

Legend for Figures 4., 5., 6.



3.3. QUANTITATIVE ASSESSMENT

The basis for the PSA-based assessment is the base case PSA for the reference NPP. The assessment follows the procedure as outlined in Section 2, sub-section 2.4 and was carried out in two steps:

1. Preliminary analysis of the operational event using conservative assumptions.
2. Refined assessment, using the additional information obtained after the preliminary analysis and replacing overly conservative assumptions by more realistic ones.

3.3.1. Preliminary analysis of the operational event

Task 1, Precursor event review and analysis: Understanding the event, identify causes, important factors and develop the context of the event in terms of the PSA perspective.

The results of the deterministic event review and analysis are presented in Section 3.2. The description below is restricted to information relevant for the PSA perspective.

Initial status of the plant

Regarding the initial status of the plant, safety related systems are of concern which are unavailable because of maintenance, repairs or tests. A detailed investigation showed that at the time of the incident there were no significant outages of equipment, systems, supplies and supports relevant for safety or related to the PSA model.

Initiating event

The malfunction of the RCP bearing temperature sensor was the trigger event for the overall operational event. It resulted in a plant trip which is considered to be the initiating event from the PSA perspective.

Malfunctions of temperature sensors used for equipment protection are not rare events in NPPs. The plant operating staff has correctly handled this event using and following appropriate procedures. For the continuation of operation, additional surveillance was put in place to monitor the RCPs. Thus, from the PSA perspective, the initiating event was classified as a general transient initiator for the PSA based assessment. The following additional considerations were made:

- Recurrent malfunctions of temperature sensors of the RCPs and other similar equipment, which could result in a plant trip due to an increased failure rate of temperature or other sensors. These could result in an increased frequency for plant trips. The plant had investigated this question and no systematic degradation of the reliability of such devices had been detected. For the particular temperature sensors of RCPs, the plant had been informed about similar events in other plants. In summary, it was judged that this problem did not have the potential to significantly increase the frequency of associated plant trips.

- Clarification of the implications of temperature sensor malfunctions. The RCP bearing temperature measurement has three set points:

1) Warning
2) Alarm
3) Urgent alarm

There is no RCP automatic trip associated with that temperature measurement.

Non-opening of the SG PORVs (Steam Generator Power Operated Relief Valves or atmospheric steam dump valves) early in the transient

Because of the reactor and RCP trip, there was a short pressure increase on the secondary side which, together with the isolation of the main steam lines, resulted in the opening of an SV (Safety Valve) on the secondary side. The SV successfully closed afterwards. Typically, the SG PORVs should open at a pressure set point well below that of the SVs. Typically, the SG PORVs have a block valve upstream which can be closed in case of malfunctions of the PORVs. It appears that during this transient, the SG PORVs valves did not open initially. Subsequent tests showed however that the valves themselves were operational.

The potential implications of this behaviour of the SG PORVs were discussed also with regard to the PSA models. There are mainly the two following aspects in this respect:

SVs in general have a relative high probability of not reclosing after opening (typically 1.0E-02 per opening). Thus, a stuck open SV could create a non-isolable steam leak on the secondary side.

The SG PORVs are controlled by an electronic device which provides the necessary functions for steam blowdown and pressure control for the secondary side. As mentioned above, the SG PORVs also have set points for opening (and reclosing) below the SVs in order to limit a pressure increase on the secondary side and to prevent the opening of SVs. The explanation for the non-opening of the SG PORVs during the early pressure peak could be that it might have been caused by delays in the response of their electronic control system. Although this aspect was not regarded to be of primary importance, a better understanding of the course of the related events and equipment response should be developed using plant records on the transient, or by using thermohydraulic analysis results for similar transients.

High bearing temperatures in the electrically driven AFWS (Auxiliary Feedwater System) pumps

After reactor trip, the two electrically driven AFWS pumps were used to feed the steam generators for heat removal via the secondary side. A more detailed description of the events and issues related to the AFWS pumps is given in Section 3.1.

The following two questions regarding the modelling of AFWS pumps in the PSA were discussed:

1). Would the bearing problems have resulted in the failure of the two pumps during the required mission time as specified in the PSA?

The required mission time of 24 hours in the PSA was also discussed. For normal reactor shutdown, after a few hours the pressure on the primary side is lowered below the RHR (Residual Heat Removal) pressure limit. Thus, further cooldown is carried out with the RHR system. Staying at hot standby however requires continued operation of the AFWS pumps. As a result, it was concluded that the 24 hours mission time is adequate. The question whether or not the two pumps would have run for the required mission time could not be answered with certainty. Thus, in the first initial quantitative evaluation, the two electrically driven pumps were assumed to fail during the mission time of 24 hours.

2). How long did the condition described above for the two electrically driven AFWS pumps exist?

The problem could be detected in the periodical tests of the AFWS. However, it appeared that in the periodical tests during power operation, the pumps are run for 15 minutes only and via a recirculation line to the condensate tank. Therefore, it was concluded that the condition would probably not be detected by following the testing procedures used prior to the incident. For the preliminary quantitative evaluation therefore, an exposure time of approximately one year was assumed.

Break of a steam line, of a diameter of 3 inches (7.6 cm), that pertained to the feedwater system (preheater, steam extraction) in the turbine building

A steam line of the feedwater system (diameter: 3 inches (7.6 cm)) had a longitudinal break in a pipe bend. As a consequence the piping of the fire water system (sprinkler system) was detached from a T-piece and a water leak from the fire water system developed. Both leaks were isolated after a short time. Nevertheless, limited steam and water flooding onto equipment took place during this time.

After the leak, a check was made of the damage caused by the flooding on nearby equipment. In particular, a nearby combined 400V bus and equipment motor control center for a number of devices was considered. A nearby cable tray with cables was also checked. Plant staff concluded that there was no significant damage to the equipment mentioned.

Further questions regarding implications and effects of the water and steam flooding were raised. These questions included:

- What equipment could have been affected or disabled?
- The extent and completeness of the checking carried out for damage assessment.
- The adequacy of follow-up checks and tests regarding potential damage.

As a probably over-conservative assumption for the preliminary quantitative assessment, the main feedwater and condensate systems were also assumed to be unavailable following plant trip.

Task 2, Mapping of the precursor on the PSA, logic representation: Relate the event and its implications to the PSA model. PSA models adequate? Revise, extend if necessary.

For the preliminary PSA-based assessment, it was concluded that the PSA models are adequate and no extensions are required. The general transient event tree can be used to estimate the

CCDP (Conditional Core Damage Probability) given the initial reactor trip and the assumed failure of the two electrically driven AFWS pumps. As the duration of the latent unavailability of the two AFWS pumps was estimated to be one year, the corresponding CCDP contribution was estimated with the base case PSA model, using an exposure period of one year. The additional unavailability of the main feedwater system, following plant trip for general transients, was estimated with the help of a general transient event tree for which the main feedwater system is assumed to be unavailable.

Task 3, Quantification: Estimate failure probabilities, if required perform human reliability analysis (HRA), adapt PSA reliability models.

For the preliminary quantification the following assumptions were made:

1. Failure of the two AFWS electrically driven pumps was conservatively assumed.
2. Exposure of the conditions for the AFWS pumps was assumed to be one year as a simplification for the preliminary quantification. More precisely, these conditions most probably had remained undetected since the last revision, or about half a year.
3. The non-opening of the SG-PORVs during the initial phase of the event was not included in the preliminary assessment.
4. Very conservatively, it was assumed that the main feedwater system could be unavailable after plant trip as a consequence of the break of the 3 inch (7.6 cm) steam line that pertained to the feedwater system.

No additional failure probabilities or changed failure probabilities had to be estimated, and no adaptation of HRA (Human Reliability Analysis) was necessary for the preliminary quantitative assessment.

Task 4, Initial evaluation: Recalculate conditional core damage probability for all appropriate sequences.

The general transient event tree (initiating event designator TRA) was used to estimate the CCDP (conditional core damage probability) given the initial reactor trip and the assumed failure of the two electrically driven AFWS pumps. The frequency of the initiating event TRA (general transient) in the base case PSA is about 3 per year which was changed for this quantification to one per year. For the CCDP calculation, the TRA event tree was then evaluated alone.

The preliminary quantification including the assumed failure of the two electrically driven AFWS pumps for the transient results as expected in a significant CCDP demonstrating that the event would require more refined assessment (e.g. consideration of recoveries, realistic assessment of the potential failure of the two AFWS pumps etc.).

As the latent unavailability of the two AFWS pumps was assumed, as a simplification, to last one year, the corresponding CCDP contribution could be estimated with the base case PSA model using the base case PSA initiating event frequencies.

The estimation of the overall PSA model CCDP contribution with the exposure time of one year for the unavailability of the two AFWS pumps showed that also other initiators than the general transient significantly contribute to the CCDP. This highlights the importance of the exposure times for such kind of latent failures.

The assumed additional unavailability of the main feedwater system, following plant trip for general transients, was estimated with the help of a general transient event tree already available in the PSA, for which the main feedwater system is also assumed to be unavailable.

The additional estimate taking into account that, after plant trip the main feedwater system potentially could be unavailable induced by the effects of the steam line break, also resulted in a substantial contribution to the CCDP, demonstrating the need for a refined modelling.

3.3.2. Refined assessment

Task 5, Recovery actions: Determine potential recovery actions, model recoveries.

The models and assumptions used for the preliminary quantification were discussed and refined in the light of the information gained from the extended investigation after the preliminary assessment. This included the following extensions:

- Refinement of the failure model for the two AFWS MDPs including recovery actions
- Refinement in the modelling of the main feedwater and condensate system regarding consequential damage due to the steamline break
- Modelling of the non-opening of the SG-PORVs during the initial phase of the operational event.

These refinements are described below.

Task 6, Evaluation: Calculate new importances including recovery actions, perform uncertainty, sensitivity analyses.

In this task, the evaluation of the refined model for precursor analysis is carried out. Uncertainty and sensitivity analysis can be used to develop an understanding regarding uncertainties in the different parts of the models, whereas sensitivity analyses are used to discuss the impact of modelling assumptions, such as the probability of failure of the two AFWS MDPs during the required mission time. These analyses are described below.

Task 7, Extension: What would happen if the event occurs under different conditions and context?

In this task "What if" questions are asked. For the event investigated here, the following factors could be varied:

- initial condition of the plant
- chronology of events in the incident
- environment for common mode failures
- different human behaviour.

Due to project limitations, this task was not carried out.

Task 8, Interpretation, conclusions, insights, corrective measures

For the refined PSA-based assessment, the models assumptions used for the preliminary assessment were refined and extended. An additional discussion regarding the completeness of the investigation was carried out, in particular regarding other hazards than internal events. The base case PSA includes the following types of hazards (using current PSA terminology and conventions):

- Internal events which are caused by plant equipment failures and plant staff errors. Traditionally it also includes loss of the external electrical grid.
- Internal fires and floods ("area events").
- External events such as seismic hazards.

In principle, all the hazards and PSA parts should be included in the precursor event analysis. In order to limit the effort and following widely used practice, only the internal events part was used. A discussion of this limitation showed that an extension of the analysis to the full PSA scope would not change the results significantly in a relative sense, and would thus not increase the insights in a way which would justify the considerably increased effort required.

As for the preliminary assessment, the probabilistic model basically consists of two parts, resulting in two different contributions. In one part, the event sequences of the operational event are directly modelled with the help of the applicable general transient event tree to obtain the CCDP caused by the event scenario. As the operational event also revealed additional malfunctions of equipment and systems required after initiating events, these malfunctions were introduced in the overall PSA model to estimate the impact of those malfunctions for all internal events scenarios. In this second part of the assessment, the base case PSA initiating event frequencies were used and an exposure time of one year was assumed, as a conservative simplification, to estimate the probability for initiating events during the exposure time. The exposure time of one year is based on the fact that most of these deficiencies would only have been detected during the revisions and tests carried out in connection with refueling outages. For the second contribution type, only those sequences should be evaluated which contain the affected equipment. As an approximation, this is carried out by subtracting the base case PSA result from the evaluation result to retain only the contribution from those sequences which contain the affected equipment.

The initiating event "plant trip" used for the probabilistic assessment corresponds to the initiating event of the general transient event tree applicable to the operational event. The malfunction of the thermocouple measuring the bearing temperature of the RCP can be regarded as the trigger event for the plant trip. According to experience from a number of different NPPs, malfunctions of thermocouple elements and other measuring equipment for protection of operational devices are responsible for a significant contribution to plant trips. Malfunctions of operational devices and systems, controls, errors of operation and maintenance staff and other factors, also make a contribution to the frequency of plant trips. To establish a model for such events is in general impractical and not usually done. Therefore, the frequency of plant trips is estimated in PSAs, usually based on statistics alone. The significance of the trigger event "malfunction of the RCP bearing temperature thermocouple" was therefore evaluated with a sensitivity study for the initiating event "plant trip", as described below.

The refined overall results are as follows. The refined assessment defines three cases with varying degrees of conservatism for the malfunctions under consideration. Including the base case these three cases are denominated as follows:

- Base case, corresponds to the base case PSA and does not include failures, malfunctions and effects observed during the operational event;
- "Low" conservatism regarding modelling of effects and malfunctions observed during the operational event;
- "Medium" conservatism regarding modelling of effects and malfunctions observed during the operational event;
- "High" conservatism regarding modelling of effects and malfunctions observed during the operational event.

The following effects and malfunctions are modelled with varying degrees of conservatism:

- Steam generator PORVs not opening during the initial pressure peak;
- Malfunction of AFWS motor driven Pumps 1 & 2;
- Secondary side steam line break with consequential effects and damage.

For the overall event scenario the event sequence is first modelled with the applicable event tree for general transients, putting the initiating event (plant trip) to a probability of one and introducing the malfunctions and effects as observed during the event scenario:

Base case CCDP1: 2.16E-06 (this evaluation and the value do not play a role in the evaluation, they are only given for comparison purposes)

CCDP1"low": 1.21E-05
CCDP1"medium": 3.01E-05
CCDP1"high": 9.28E-05

Second, the PSA model is evaluated assuming an exposure time of one year for effects and malfunctions:

Base case CCDP2: 3.17E-05
(Initiating event probabilities calculated with base case frequencies and an exposure time of one year, everything else left unchanged)

CCDP2"low": 3.38E-05
CCDP2"medium": 4.00E-05
CCDP2"high": 9.22E-05

Retaining only the malfunctions or effects observed:

ΔCCDP2"low": CCDP2"low"- base case CCDP2 = 3.38E-05-3.17E-05 = 2.10E-06
ΔCCDP2"medium": CCDP2"medium"-base case CCDP2 = 4.00E-05-3.17E-05 = 8.30E-06
ΔCCDP2"high": CCDP2"high"- base case CCDP2 = 9.22E-05-3.17E-05 = 6.05E-05

Total, specific applicable scenario and overall model:

CCDP“low”: CCDP1”low”+ΔCCDP2“low”= 1.21E-05 + 2.10E-06 = 1.42E-05
CCDP“medium”: CCDP1"medium"+ΔCCDP2“medium”=3.01E-05+8.30E-06 = 3.84E-05
CCDP“high”: CCDP1 "high"+ΔCCDP2“high”=9.28E-05 + 6.05E-05 = 1.53E-04

These results confirm the outcome of the preliminary assessment in that the operational event under consideration is significant and merits further consideration.

The following paragraphs contain the assessment and interpretation for the individual important issues of the operational event.

Thermocouple malfunction causing plant trip

The malfunction of a thermocouple element measuring the bearing temperature of an RCP caused the plant trip and therefore can be regarded as the trigger event, initiating the event sequence considered here. For estimating the CCDP in the PSA model, the probability of the applicable initiating event “plant trip” was set to one in the related event tree “TRA”, general transient.

In order to obtain an impression of the impact of the thermocouple malfunction and of the subsequent plant trip, a sensitivity analysis has been carried out with the base case PSA for internal initiating events. The sensitivity analysis is carried out as follows:

- Sensitivity factor of overall result (CDF), when an event probability (or frequency in our case) is changed by a factor of 10.
- Factual increase of the overall result (CDF), if the event probability is increased by a factor 10.
- Factual decrease of the overall result (CDF), if the event probability is decreased by a factor of 10.

The results for the initiating event of the general transient event tree are as follows:

- Percentage contribution to overall CDF for internal initiating events: 21.1%.
- Base case CDF: 3.17E-05 per year for internal events.
- Sensitivity factor for the general transient initiating event: 3.4.
- Overall CDF with the plant trip frequency increased by 10: 9.3E-05 per year.
- Overall CDF with the plant trip frequency decreased by 10: 2.7E-05 per year.

The results above demonstrate that, first the CDF contribution from the general transient event tree behaves proportional to the frequency of the initiating event as expected, and second that the sensitivity regarding the overall CDF is much less than proportional, because of the other contributors which remain unaffected by a change in the general transient initiating event frequency. More important, the limited decrease of the CDF when the general transient initiating event frequency is reduced by a factor of 10, shows that only a limited gain is possible by reducing the general transient initiating event frequency.

The frequency of the initiating event for the general plant transient in the base case PSA model is 3 plant trips per year. This relatively elevated value includes the higher number of plant trips in the first operational years. The number of plant trips per year has substantially decreased in recent years. Therefore, and considering the sensitivity results discussed above, the possible reduction of the overall CDF by further reducing the number of plant trips, is considered to be small.

Steam generator PORVs not opening during the initial pressure peak

The main function of the steam generator PORVs is to provide a controlled secondary side steam relief path for plant cooldown, in case steam relief to the condenser is not available (preferred path). The opening of steam generator PORVs on pressure set points which are below those of the safety valves, is not regarded as an important function in the PSA. This is because there are only a few transient types for which opening of the safety valves would be avoided by opening of the SG PORVs. The related issue here is that safety valves which cannot be isolated after opening, may stay stuck open and thus create a scenario similar to a secondary side steam leak. For the base case PSA, this kind of scenario is considered to be included in the steamline and feedline breaks, for which a relatively high initiating event frequency of about 1.0E-02 per year is taken into account. For estimating the CCDP of stuck open safety valves in the event sequence considered here, the base case result for SLB (steamline/feedline break) event tree can be used as follows:

- Lifting of safety valves as observed: probability set to one;
- Safety valve stuck open after opening: 1.0E-02 (rough estimate).

The potentially reduced reliability of SG PORVs for controlled steam relief for plant cooldown via the secondary side is modelled with a factor multiplying the base case failure probability. Three different values for these factors are used on a judgmental basis, the largest having a value of 3.

For estimating the impact of the SG PORV function alone, the sub-events not related to the PORVs were set to nominal, and the most pessimistic judgmental factors (corresponding to "high" in the modelling conservatism scheme explained above) regarding the non-opening of the SG PORVs were used. The results are as follows:

Stuck open safety valves as a consequence of the non-opening of SG PORVs:

CCDP from the applicable steamline / feedline event tree SLB: 2.80E-07
(with an estimated initiating event probability of 1.0E-02 as derived above)

The CCDP from the overall model assuming one year exposure time is estimated as follows:

Base case model: 3.17E-05
(Initiating event probabilities calculated with base case frequencies and an exposure time of one year, everything else left unchanged)

With the additional SG PORV failure factor described above: 3.17E-05

Thus, there is no noticeable impact on CCDP due to a reduced reliability of the SG PORV function.

The total CCDP therefore is: 2.80E-07

According to the estimated CCDP, the observed non-opening of SG PORVs, and the potential decrease in the reliability of the function of the PORVs, do not have a significant impact. The reason is that, first there are multiple means for carrying out steam relief for cooldown, and second that failure of this function is dominated by failures of equipment providing feedwater to the steam generators.

The most noticeable contribution comes from stuck open safety valves not reclosing after opening. According to this CCDP, a malfunction of SG PORVs or a degradation in the SG PORV function is not a significant sub-event.

Malfunction of AFWS motor driven Pumps 1 & 2

The event and conditions regarding the AFWS motor driven pumps (AFWS MDPs) are considered to be not directly connected to the initiating event of the transient being considered, but have been obviously existing for some time before the event, and they became apparent only during the transient. The PSA based evaluation considers the malfunction of the AFWS MDPs both, for the applicable event tree which is the general transient event tree "TRA", and for other initiating events where the AWFS MDP play a role within the overall model for internal initiating events. The event tree TRA is evaluated to directly obtain the CCDP given the initiating event, to include the additional models describing the AFWS MDP issue. The overall model with the changes, is evaluated assuming an approximate exposure time of one year, using the CDF as the measure for the risk implied by operating the plant during that time period and subjected to all initiators at their base case frequency.

The additional model to depict the observed malfunction of the AFWS MDPs consists of a probability P_t for having a substantial increase in bearing temperature as observed during the transient. As this increase was actually observed, this probability is set to one for the CCDP estimate with the general transient event tree TRA. For the overall model, this probability is reduced on a judgmental basis into three cases with different degree of conservatism which correspond to the three degrees of conservatism ("low", "medium" and "high" as explained above), to account for different conditions and circumstances valid for other scenarios and for the total time frame of one year. The probability P_t is multiplied with a recovery probability which describes intermittent start-stop operation of the two AFWS MDPs to keep the bearing temperatures at an acceptable level. The recovery term is composed of two contributions:

(1) an increased start and run failure probability for this cyclic operation procedure, based on the nominal pump failure parameters but increased by a judgmental factor, and
(2) a human error probability for failing this procedure.

In the PSA, the whole failure expression is mapped into one event in which both AFWS MDPs are failed simultaneously.

Regarding the evaluation of the overall PSA model to estimate the impact of the AFWS MDPs malfunction alone, the sub-events not related to the AFWS MDPs were set to nominal

and the most pessimistic judgmental factors (corresponding to “high” in the three level modelling conservatism scheme) regarding AFWS MDP malfunction were used.

The results are as follows:

CCDP from the applicable general transient tree TRA: 3.00E-05
(base case CCDP: 2.16E-06, initiating event probability set to one)

The CCDP from the overall model assuming one year exposure time is estimated as follows:

Base case CCDP: 3.17E-05
(Initiating event probabilities calculated with base case frequencies and an exposure time of one year, everything else left unchanged)

With the additional AFWS MDP malfunction model described above: 7.25E-05
Retaining only the malfunctions or effects observed: 7.25E-05–3.17E-05 = 4.08E-05

The estimated overall CCDP therefore is 3.00E-05 + 4.08E-05 = 7.08E-05

According to the estimated CCDP, the AFWS MDP malfunction is a significant event which would require detailed investigation and consideration of corrective actions. The impact of the malfunction is significant not only for the directly applicable event scenario — the general transient event tree TRA, but also for other initiating events and related scenarios.

According to this CCDP, the AFWS MDP malfunction is a significant sub-event. Compared to the other issues which appeared subsequent to the initiating event, it is the most important one. A part of the impact is directly related to the particular initiating event. Another important part relates to the pre-existent exposure to potential initiators which require the AFWS.

Secondary side steam line break and of the consequential effects and damage

A feedwater system steam line of a diameter of 3 inches (7.6 cm) had a longitudinal break in a pipe bend. As a consequence, the piping of the fire water system (sprinkler system) was damaged mechanically and a water leak from the fire water system developed. Both leaks were isolated after short time. Nevertheless, limited steam and water flooding onto equipment took place during this time. A thorough check was made of the damage caused by the flooding on nearby equipment. In particular, a nearby combined 400V bus and equipment motor control centre for a number of devices was considered. A nearby cable tray with cables was also checked. It was concluded that there was no significant damage to the equipment mentioned.

The steam line break and subsequent damage and effects could result in the failure or an increased unavailability of systems in the turbine building. Regarding systems considered in the PSA, mostly the main feedwater system could be affected in this way. Accurate modelling of such effects would require an extended investigation and associated modelling work. For the purpose here, an additional failure event regarding the post trip use of the main feedwater system with estimated probabilities was developed. For the general transient event tree TRA, which is directly applicable to the event sequence considered here, three cases with an increase in the unavailability of the main feedwater system of 30%, 100% and 200%

compared to the base case model were assessed on a judgmental basis (the cases corresponding to the “low”, “medium” and “high” in the three level modelling conservatism scheme). For the overall model, this probability was reduced again into three cases with different degree of conservatism, to account for different conditions and circumstances valid for other scenarios, and for the total time frame of one year.

Regarding the overall PSA evaluation for estimating the impact of a reduced availability of the main feedwater for post trip use, the sub-events not related to the affected main feedwater system remained at the base case values and the most pessimistic judgmental factor regarding the unavailability of the main feedwater system was used (corresponding to “high” in the three level modelling conservatism scheme).

The results are as follows:

CCDP from the applicable general transient tree TRA: 8.00E-06

(nominal CCDP: 2.16E-06, initiating event probability set to one)

The CCDP from the overall model assuming one year exposure time is estimated as follows:

Base case CCDP: 3.17E-05
(Initiating event probabilities calculated with base case frequencies and an exposure time of one year, everything else left unchanged)

With the additional unavailability of the main feedwater system for post trip use: 3.50E-05
Retaining only the malfunctions or effects observed: 3.50E-05–3.17E-05 = 3.30E-06

The estimated overall CCDP therefore is 8.00E-06 + 3.30E-06 = 1.13E-05

The impact regarding CCDP due to the potentially reduced reliability of the main feedwater system for post trip use, is of medium significance. The main reason for the medium significance is that main feedwater requires normal AC power supply and may require operator actions.

Figure 7 presents the PSA significance assigned to separate primary effects.

Primary effect (see ECFC)		*SIGNIFICANCE ACCORDING TO PSA*
1	***Thermocouple malfunction causing plant trip***	The malfunction of the RCP bearing temperature measuring thermocouple caused the plant trip which is the initiating event for the applicable event tree of the PSA. Sensitivity analysis shows that the overall CDF is not particularly sensitive to a change in the frequency of plant trips. Moreover, the possible reduction in the overall CDF by further reducing the number of plant trips is limited. The plant has a surveillance program in place which monitors equipment like the thermocouple considered. No unusual increase of malfunctions or failures was observed in recent years.
2	***Secondary side steam line break and the consequential effects and damage*** - Failure of a steam pipeline (diameter: 3 inches, 7.6 cm) in the Turbine Building - FPS pipe becomes detached at T-joint. (FPS pump started to operate) - Cable tray deformed	CCDP due to the steam line break and potential damage and effects is estimated as: 1.13E-05. This estimate is based on conservative assumptions regarding a reduced availability of the main feedwater system due to consequential damage. According to this CCDP the steam line break and subsequent damage and effects have a medium significance.
3	***Steam generator PORVs not opening during the initial pressure peak*** SG PORVs failed to operate prior to SV lifting	CCDP due to the observed not opening of SG PORVs and a potentially reduced reliability of SG PORV function: 2.80E-07 The most noticeable contribution is coming from stuck open safety valves not re-closing or stuck open after opening. According to this CCDP a malfunction of SG PORVs or degradation in the SG PORV function is not a significant sub-event. It should be pointed out however, that the investigation regarding the behaviour of the SG PORVs during the event sequence is still ongoing.
4	***Malfunction of AFWS motor driven pumps 1 & 2*** High axial bearing temperature on AFWS pumps 1 & 2	CCDP due to the initiating event and the AFWS MDP malfunction alone: 7.08E-05 Based on the most pessimistic judgmental factors regarding modelling of the AFWS MDP malfunction but including a recovery action. According to this CCDP the AFWS MDP malfunction is a significant sub-event. Compared to the other issues which appeared subsequent to the initiating event it is the most important one. A part of the impact is directly related to the particular initiating event, another important part relates to the pre-existent exposure to other potential initiators which require the AFWS.

FIG. 7. Table showing the PSA significance assigned to primary effects.

4. CONCLUSIONS

The overall process outlined in this publication needs to be carefully organized and synchronized. The deterministic and probabilistic activities are significantly different in nature and effort. For example, carefully planned steps of screening with adequate PSA based methods need to be utilized in order to make the process practical.

The exercise showed that the effort and time required for the deterministic and probabilistic operational event assessment may differ from stage to stage. Deterministic assessment permits unresolved issues to be initially treated as presumptions, whereas PSA has always to find a way to model such issues.

The process can establish a common basis for understanding, discussion and investigation, synergistically bringing together non-PSA and PSA staff contributions.

The process provides a good example of the application of PSA to ensure necessary focus on safety related issues in events and corrective/preventive actions.

ACKNOWLEDGEMENT

The procedure on PSA based precursor analysis has been generated in an earlier IAEA activity and has been adopted and modified for this publication. Contributors to this work were:

Dubreuil Chambardel, A.	EdF, France
Hoertner, H.	GRS, Germany
Minarick, J.W.	SAIC, USA

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).

[2] Dubreuil-Chambardel, A., Francois, P., Pesme, H., Maliverney, B., An Operating PSA Application at EdF: The Probabilistic Incident Analysis, Proc. Probabilistic Safety Assessment and Management, ESREL'96, PSAM III, Crete, Springer, London (1996)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Methodologies for Analysis of Safety Incidents at NPPs, IAEA-TECDOC-1278, Vienna (2002).

ABBREVIATIONS

AOP	Abnormal operating procedure
CCDP	Conditional core damage probability
CDF	Core damage frequency
ECFC	Event and causal factor chart
EOP	Emergency operating procedure
ERP	Event review panel
FPS	Fire protection system
GOP	General operating procedure
HRA	Human reliability analysis
I&C	Instrumentation and control
IRS	Incident Reporting System
MCR	Main control room
MDAF	Motor driven auxiliary feedwater (pump)
MDP	Motor driven pump
MSIV	Main steam isolating valve
OE	Operating experience
PIS	Process information system
PORV	Power operated relief valve
RCP	Reactor coolant pump
SG	Steam generator
SLB	Steamline break
SV	Safety valve
TB	Turbine building
TDAF	Turbine driven auxiliary feedwater (pump)
TRA	General transient identifier in the PSA of the reference plant

CONTRIBUTORS TO DRAFTING AND REVIEW

Dusic, M.	International Atomic Energy Agency
Ferjancic, M.	Slovenian Nuclear Safety Administration
Gubler, R.	Ingbuero Gubler, Switzerland
Janezic, A.	Slovenian Nuclear Safety Administration
Koncar, M.	Slovenian Nuclear Safety Administration
Kostadinov, V.	Slovenian Nuclear Safety Administration
Levstek, M.	Slovenian Nuclear Safety Administration
Muehleisen, A.	Slovenian Nuclear Safety Administration
Spencer, A.	Alan Spencer Services, United Kingdom
Spiler, J.	Nuclear Power Plant, Krsko
Stimpson, D.	D. Stimpson & Associates, United Kingdom
Stritar, A.	Slovenian Nuclear Safety Administration
Strucic, M.	Nuclear Power Plant, Krsko
Vrbanic, I.	Nuclear Power Plant, Krsko
Vojnovic, Dj.	Slovenian Nuclear Safety Administration

CONSULTANTS MEETINGS

19–23 November 2001

2–6 December 2002

10–14 March 2003

10–14 November 2003