EUROPEAN
TECHNICAL SAFETY
ORGANISATIONS
NETWORK

TECHNICAL SAFETY ASSESSMENT GUIDE

EVENT REVIEW AND PRECURSOR ANALYSIS

ETSON/2013-002 January 2013

FOREWORD

Since the beginning of EUROSAFE initiative (1999), IRSN, GRS and Bel V (former AVN) have pursued the objective to advance the harmonisation of nuclear safety in Europe by comparing their safety assessment methodologies. Based on a long standing experience of more than 40 years, in spite of different national nuclear safety regulatory backgrounds, they have developed practical methods to perform safety assessments that presented sufficient similarities to encourage them to persevere in building a collection of common best practices. The first version of their common Safety Assessment Guide was thus approved in 2004.

The general Safety Assessment Guide (SAG), and its specialized guides, the Technical Safety Assessment Guides (TSAG), have been written by the members of the European Technical Safety Organisations Network with progressive improvements brought by the new members of ETSON.

The SAG provides general principles such as safety assessment objectives or transparency and traceability of the process, and describes the general process for performing the safety assessment of nuclear installations. The goal of this SAG is to set down the harmonized methodology applied by ETSON organisations to ensure a common quality of safety assessment and to develop higher confidence in delivered safety assessments.

The TSAG series consists of specialized guides dedicated to specific technical domains of importance to the safety of nuclear installations. They provide an overview of the available practical knowledge gained by Technical Safety Organisations (TSO) in conducting safety assessments covering these main technical issues (use of operating experience feedback, assessment of human and organisational factors, prevention of severe accidents, probabilistic safety assessment, etc.).

Each guide published by ETSON is updated according to the extension of experience gained as well as to the new requirements in nuclear safety.

The 2012 guides present the common views and practices of ETSON members:

- Bel V - Belgium
- GRS - Germany
- IRSN - France
- VTT - Finland
- UJV Rez - Czech Republic
- LEI - Lithuania
- VUJE - Slovakia
- PSI - Switzerland

With the contribution of ETSON associated members:

- SSTC - Ukraine
- JNES - Japan
- SEC NRS - Russia

CONTENTS

1 SCOPE

The purpose of the event reviews and precursor analyses is to draw lessons from events with safety significance occurring at plants during operation, surveillance and maintenance activities, including deviations from the normal performance of systems or human errors, which may be precursors to severe accidents. The aim of these lessons should be the reinforcement of the defence-in-depth and thus of the safety of the installations. The event reviews and precursor analyses are an indispensable part of the overall operating experience feedback process.

The event reviews and precursor analyses for safety-significant events are performed by two different organisations: utilities analyse the events first, and then regulatory bodies/Technical Safety Organisations (TSO) make their own review which leads to independent assessments.

The goal of this guide for event review is to provide an approach to deal with all the main issues of events and precursor analyses[1]. It also outlines 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 analyses.

The guide does not deal with the means needed to perform this kind of analysis, but with its main objectives.

It is intended to be used mainly by the technical safety organisations or regulatory body performing safety reviews of events.

1 Precursor events are identified by a PSA-based event analysis when applicable. The operational event is mapped on a probabilistic risk model of the plant in order to achieve a quantitative assessment of its safety significance.
This significance is provided by the conditional core damage probability (CCDP) or delta core damage probability (ΔCDP) calculation, given that the precursor event has happened. An event is commonly and widely considered as:
- a precursor beyond a threshold CCDP value of 10^{-6};
- an important precursor beyond a threshold CCDP value of 10^{-4};
- a significant precursor beyond a threshold CCDP value of 10^{-3}.

2 EVENT REVIEW APPROACH

2.1 Event reporting and event review systems

An appropriate event review to be performed by the regulatory body/TSO needs:

- a national reporting system : the regulatory body ought to establish a reporting system based on key criteria for events that have to be reported. Moreover, the utilities should develop procedures for the reporting of events and stipulate a time limit, a format and administrative arrangements for reporting, utilising a management system;

- a pertinent system of investigation specified by the regulatory body/TSO so as to provide a solid starting point for further assessments. This system must be organised through procedures specifying:
  - the scope of the review which should vary accordingly, depending on the case of a minor or major event;
  - the type of investigation that is appropriate for an event of any particular type;
  - the level of investigation which should be determined taking into account:
    - the consequences of the event (any injury to on-site personnel, a significant radiological release or an overexposure of personnel has occurred, plant operation exceeded the operational limits and conditions or was beyond the design basis of the plant, etc.);
    - a similar occurrence has taken place earlier at the same installation or at an installation of a similar type;
    - patterns that are unique, complex or not well understood.

To be up to standard, the event review should address at least the following key issues:

- description of the complete event sequence (what happened);

- determination of the deviations (how did it happen);

- cause analysis (why did it happen, including root causes);

- consequences assessment in order to evaluate the significance of the event;

- effectiveness of corrective actions and lessons learned.

These key issues are essential in order to homogenise the event reviews.

Moreover, any learning point should be clearly identified. For instance, additional information arising from event investigation may identify precursor errors[2], human fault, insufficient checks, latent and construction weaknesses that did not contribute to the event being investigated but which, nevertheless, might cause a future event and thus need preventive actions.

2.2 Minimum requirements for an efficient and comprehensive event review

In order to achieve an efficient and comprehensive event review and in addition to an active and pertinent national reporting system established by the regulatory body, the minimum requirements should be as follows in order to facilitate learning from events:

- screening of events, done as a selection of relevant events, primarily with regard to safety/radiation protection/environment/personnel and transport significance. Selecting the safety-significant events requires a screening at the regulatory body/TSO level in order to prioritise the actions to be performed (in-depth analysis, IRS selection, etc.). Furthermore, a dialogue with the utilities at the national level may be useful to finalise the first event prioritisation;

  Events should be regularly scrutinised by a multidisciplinary group with engineering, scientific, human performance and behaviour knowledge.

  Ranking of events should be considered in view of the number of events likely to be of interest and the resources needed to evaluate them.

- investigation and review of events using the deterministic approach;

- in-depth analysis of the most significant events using the deterministic approach;

- PSA (probabilistic safety assessment)-based event analysis (PSAEA, also referred to as risk-based analysis of operational events, or probabilistic precursor analysis): precursor analyses are useful in order to identify significant precursors of accidents and to recommend actions to prevent their recurrence.

2.3 Investigation and review of events

The objectives of the investigation and review of events are:

- to identify events that are actually or potentially significant for safety and their associated safety concerns and root causes, and to determine the adequacy of corrective actions taken to address the safety concerns;

- to find out emerging trends or patterns of potential safety significance;

- to assess how situations could have developed;

- to assess the applicability of events to other installations;

- to prevent the recurrence of similar events;

- to identify and possibly quantify events and conditions that are precursors to significant degradation and that could

2 Errors that may lead to significant events.

contribute to plant damage or releases of radioactive material;

- to create useful knowledge for the safety assessment of existing NPPs or new plant projects.

Events should be scrutinised by a multidisciplinary group: experts in reactor systems, human factors and operations, and specialists in mechanical, electrical or instrumentation and control systems are suitable. Additional members could be specialists in physics, plant operation, radiological assessment, health physics, chemistry, materials science, emergency preparedness or other specialised areas.

Events should be investigated and reviewed using deterministic and probabilistic approaches.

2.3.1
DETERMINISTIC APPROACH

2.3.1.1
Description of the complete event sequence (what happened)

The comprehensiveness of the description should be verified by the TSO or regulatory body.

The plant operating conditions and status prior to the event should be part of the event description, including relevant information about pertinent systems, surveillance, testing and maintenance in progress, failed structures and faulted systems or components.

The event description should include:

- the sequence of occurrences;
- automatically or manually initiated safety systems responses;
- the method of detection of the event;
- the date and approximate times for each occurrence;
- a description of the event from the operator's viewpoint (*i.e.* what he saw, did, understood or misunderstood).

In addition, any unique characteristics of the plant that influenced the event (favourably or unfavourably) should be described.

2.3.1.2
Determination of the deviations (how did it happen)

The aim of the review is to understand how the deviation resulted in a failure and why the expected result was not achieved.

In addition to the previous items of the event description, faults of systems and components, operator actions and procedural controls should be presented.

The narrative description should include:

- beneficial or adverse actions;
- the use of procedures and any procedural deficiencies;
- any aspect of the man-machine interface that contributed to the event.

2.3.1.3
Cause analysis (why did it happen)

The cause analysis of events induced by equipment failures or human errors performed by the utilities, should be verified and completed by TSO/regulatory body if needed.

The direct causes, root causes and causal factors of the event should be clearly described. Therefore, the reasons for equipment malfunctions, problems of human performance, organisational weaknesses, design and manufacturing deficiencies and other relevant facts should be included in the cause analysis.

DIRECT OR IMMEDIATE CAUSES

These comprise failures, actions, omissions or conditions which immediately produced the event (*i.e.* the direct initiator or event).

ROOT CAUSES

They may provide an explanation of why the immediate cause occurred. They are the most basic causes of an event that can reasonably be identified.

To be considered as a root cause, the cause needs to meet one of the following criteria:

- the event is likely to recur;
- the event would not have occurred if the causes had not been present;
- or the problem will not recur as a result of the same cause if the cause is corrected.

CAUSAL FACTOR

A causal factor contributes to the event occurrence. In opposition to a root cause, the correction of a causal factor does not eliminate the recurrence of the event in future but reduces the probability of its recurrence.

The purpose of the analysis of human factor aspects in an event is to use established knowledge about basic human behaviour so as to understand the contributory and influencing factors that have led to an error, or may have predisposed someone to make an error, either of omission or of commission.

Human failures may reveal that choices that have been made concerning organisation, man-machine system, workplace characteristics or training were inappropriate. Corrective actions should enhance complementarities between individual factors (knowledge, motivation, etc.), collective factors (organisation of work, co-operation inside teams or between teams) and external factors such as characteristics of tasks to manage, information supports (procedure, man-machine interface, etc.) and technical components of workplaces (communication tools, etc.).

When an event investigation reveals shortcomings in human performance, it is important to specify the inappropriate human actions taken (*i.e.* the response as well as the causes). The objective is to evaluate technical, organisational, or human barriers which have been designed to prevent or to deal with inappropriate human action.

The aim should be to provide both the technical details of the event and the lessons concerning human and organisational performance in a way that can be understood and potentially applied to other situations. Latent weaknesses in any of the organisational factors in place to help workers to perform their tasks properly (*e.g.* in the planning and scheduling of work, training, supervision, work practices, written instructions and the work environment) are likely to lead to errors.

It is important that investigations respond to the three following questions:

- how does a person or a work team usually perform in a specific situation?
- what went wrong or what was different from usual at the day of the event?
- what would have been useful or helpful to manage more appropriately the context of the event in order to prevent its occurrence?

Consequently, information about previous malfunctions and clear explanations about detection and measures taken should be provided.

The analysis should consider and resolve the following issues:

- what was the nature of the human error: *e.g.* a cognitive error or was there an error in the application of procedures or misunderstanding between different people?

- were human deficiencies in the use of procedures characterised either in terms of failure to follow an approved procedure or in the use of a procedure that contained erroneous instructions, or were they associated with an activity or task that was not adequately covered by a procedure?

- did unusual characteristics of the working location, such as heat, humidity, noise, radioactivity levels, accessibility or signage contribute to the problem with human performance?

- were there any ergonomic issues, or

issues relating to engineering for human factors?

- which type of personnel was involved (such as a licensed operator, an unlicensed operator, supervision and management staff, or contractor personnel)?

- did any organisational or technical barriers fail to foresee, detect or manage human error itself?

Analysis of human performance also implies to identify good practices or organisational measures which were necessary to manage risks during the event. Indeed, it is important for safety to underline or strengthen all means which have had a positive effect during the event.

2.3.1.4
Consequences assessment in order to evaluate the significance

The safety assessment should be focused on the safety consequences and implications of the event. After the prior phase whose aim is to ascertain why the event occurred, the assessment should analyse whether the event would have been more serious under reasonable and credible alternative conditions:

- actual consequences;

- potential consequences (what could have happened);

- remaining defence-in-depth lines and influence on defence-in-depth barriers.

These consequences include radiological consequences, if any, to on-site and off-site personnel and the environment, damage to the plant, etc.

2.3.1.5
Effectiveness of corrective actions and lessons learned

The TSO/regulatory body should verify the adequacy and the pertinence of the corrective actions defined by the utilities. Notably, the effectiveness of corrective actions should be proved generally with the objectives to correct the situation, to prevent a recurrence of an event or to enhance safety. The corrective actions should be directed towards the root causes and the causal factors, and should be aimed at strengthening the weakened or breached barriers that failed to prevent the event. Moreover, the corrective actions should be defined with the aim to improve equipment, human performance or managed processes, for example by:

- modifications to equipment and the implementation of additional devices and means to prevent the recurrence of the same or similar events;

- improvements of procedures and administrative measures, and additional checks and control;

- rectifying deficiencies revealed in the documentation for operation;

- training personnel to perform jobs properly;

- making changes to the working environment, to the planning and scheduling of work and to the organisation and its decision-making processes.

The TSO/regulatory body should deserve a particular attention to the priority attributed to the corrective actions since generating too many actions may overwhelm the intended benefits and may result in some important actions being left pending for too long. In addition, the actions may be immediate, interim or long-term with a need for detailed evaluation.

Consequently, factors that a regulatory body/TSO should consider in the review of corrective actions proposed by the utility include the following:

- whether the proposed corrective action addresses the fundamental problem?

- what adverse consequences may result from the implementation of the corrective action?

- whether the corrective action is compatible with other corrective actions that have been previously implemented?

- whether the corrective action has been taken before and with what results?

- whether the corrective action is an interim solution or a conclusive solution?

- for plants at which risk assessment techniques are used in formulating corrective actions, whether the quantification of safety improvement is appropriate?

- whether the corrective action is scheduled, taking into account the base level of risk and the incremental improvement that may be attributed to the corrective action?

Furthermore, a tracking process should be implemented to ensure that all corrective actions are completed in a timely manner.

The identification of lessons learned from an event is an important task to prevent recurrence at other components or systems, at different conditions, or at other installations. All corrective actions should be taken into account, with a specific focus in order to assess their applicability to other plants.

2.3.2
PROBABILISTIC APPROACH: PSA-BASED EVENT REVIEW

The aim of a PSA-based event review is to identify precursors. A precursor to potential severe core damage is an event or condition that could have been severe if plant conditions, action by personnel or the extent of equipment failure or faulting had been slightly different from the actual circumstances.

The PSA-based event review provides a complement to the deterministic approach in the event review. It implies the mapping of an event on a probabilistic risk model of the plant in order to obtain a quantitative assessment of the safety significance of the event: this review produces a quantitative assessment of the likelihood of reactor core damage if additional failures or human errors would occur. It permits to prioritize the occurred events according to their conditional probability of core damage.

A benchmark system between utilities and regulatory bodies (or the technical support organisation when existing) is recommended to compare the list of precursor events and the quantification results and, further, explain discrepancies.

2.3.2.1
Methodology for a probabilistic review

The steps to carry out a precursor analysis are detailed in Reference [1] and in Appendix 1.

- a level-1-PSA model should be used. This model should be sufficiently comprehensive 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. When some events reveal unexpected sequences or sequences previously considered as non-relevant, the PSA model may be completed. In this case, the precursor event analysis could involve modelling of missing accident sequences, missing component failure modes, or restoring accident sequences that were originally truncated or screened out;

- a re-analysis of the PSA is performed to evaluate the conditional core damage probability under the condition that the operational event has occurred. The concept of conditional core damage probability (CCDP) calculation provides a useful measure of safety significance of operational events given that the precursor event has happened; sometimes, PSA model needs to be adapted to take into account component failure not included in the existing model. An event is commonly and widely considered as a precursor if its CCDP has a value higher than 10^{-6}.

Two types of events are analysed for a PSA-based event review:

- events involving an initiating event of the PSA (if modelled): the accident scenarios to be analysed is developed from this initiating event. The analysis consists of an assessment of the failure probability of the lines of defence limiting the consequences of the event;

- events involving the unavailability or a degradation of equipment or systems (degradation of lines of defence): if the event is related to one (or several) safety functions, a systematic survey of the principal scenarios influenced by the precursor event needs to be done; all the initiating events which require the affected safety functions need to be identified. The analysis consists of an assessment of the probability of all these scenarios making use of the respective lines of defence.

Precursor events which involve both types are also possible. In this case, both types of impacts need to be included in the analysis in a combined manner.

2.3.2.2
Usefulness of probabilistic analyses

In addition to the numerical value for the risk significance of an operational event, the precursor analysis increases the understanding of the plant vulnerabilities given the event occurrence. Moreover, a PSA-based event review may support deterministic event reviews at the previous stages of investigation:

- quantitative analysis of the safety significance of nuclear plant events can be a very useful measure when it comes to prioritise the events. If an event is already modelled in the existing PSA and is sufficiently significant based on a rough risk estimate, an in-depth analysis of the event should be performed;

- regarding in-depth analysis, PSA-based event evaluation provides a quantitative measure for judging the significance of events and the main contributors to these events (conditions and other influences such as human performance).

The efficiency of some corrective/preventive actions can be estimated by taking into account the information and insights derived from PSA-based analyses. This tool can also provide useful information for the prioritisation of corrective actions.

2.3.3
CONCLUSION AND RESULTS FROM AN EVENT REVIEW

The outcome of the application of the event review approach described above should be:

- identification of the significant events for safety and their root causes;

- evaluation of the effectiveness of the corrective actions;

- finding out emerging trends or patterns of potential safety significance;

- identification and possibly quantification of events that are precursors to significant degradation;

- further utilisation of operating experience feedback through:
  - wider consideration of trends;
  - dissemination and exchange of event information and generic lessons learned;
  - continuous monitoring and improvement of programmes for operating experience feedback;
  - a storage, retrieval and documentation system for information on events.

3 CONCLUSION

3.1
Event review objective

The objective of the event review approach is to detect every safety-significant event. The identification of lessons learned from an event is an important task to prevent recurrence at other components or systems, at different conditions, or at other installations. Furthermore, PSA-based event review by extrapolating precursor events to accident scenarios with serious consequences will provide valuable insights about serious incidents on the basis of events that had no real safety significant consequences.

The examination of events leading to a value of conditional core damage probability (CCDP) superior to a given criterion (10^{-6}) requires special attention. Furthermore, the efficiency of some corrective actions can be estimated depending on the CCDP value.

3.2
Building an operating experience feedback

Building an effective operating experience feedback system (Reference [2]) is necessary to draw lessons and reinforce the defence-in-depth and thus the safety of the installations.

Well-defined reporting criteria aim at the homogeneity and the relevance of the operating experience feedback data:

- Trending and review to recognise emergent problems (*e.g.* recurrence examination, comprehensive data collection)

The aim is to identify an abnormal trend early enough so that the utilities can initiate follow-up investigations and take corrective actions to prevent a more significant event. A system should be applied that enables events to be characterised. Trend data should be reported, providing useful information for 'early warning' of abnormal trends and in order to help in gaining understanding of the factors that may be responsible.

- Utilisation, dissemination and exchange of information on operating experience

For instance, information from international operating experience feedback should be reviewed in order to consider aspects such as "generic" implications that apply to the plant, whether there are similar practices at the plant that predispose it to similar events, the possible prior occurrence of a similar event, reported actions taken that are applicable to the plant. Moreover, the lessons learned should be shared nation-wide and internationally. International operating experience feedback systems and working groups should be established at the pertinent international organisations. In addition, bi-lateral exchange of operating experience should be performed with neighbouring countries.

- Reviewing the effectiveness of the experience feedback process

Several steps in the operating experience feedback process are necessary. These steps are on the plant level, the utility level, the national level, and the international level. Some aspects for review are the timeliness of the reporting, the sufficiency of the event analysis as well as the implementation and effectiveness of the actions taken.

4 REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Precursor Analyses – The Use of Deterministic and PSA Based Methods in the Events Investigations Process at Nuclear Power Plants, IAEA-TECDOC-1417, Vienna (2004).

- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, A system for the Feedback of Experience from Events in Nuclear Installations, IAEA Safety Standards Series nº NS-G-2.11, Vienna (2006).

APPENDIX

PROCEDURAL TASKS IN PSA-BASED EVENT REVIEW [1]

1. Precursor event review and analysis

- understanding the event;
- identifying causes, important factors and developing the context of the event in terms of the PSA perspective.

2. Mapping of the precursor on the PSA, logic presentation

- relating the event and its implications to the PSA model;
- are PSA models adequate?
- revising, extending if necessary.

3. Quantification

- estimating failure probabilities;
- if required, performing human reliability analysis;
- adapting PSA reliability models.

4. Initial evaluation

- recalculating conditional core damage probability for all appropriate sequences.

5. Recovery actions

- determining potential recovery actions;
- modelling recoveries.

6.
Evaluation

- calculating new importances;
- performing uncertainty and sensitivity analyses.

7.
Extension

- what would happen if the event occurred under different conditions and context?

8.
Interpretation, conclusions, insights, corrective measures

ETSON

EUROPEAN
TECHNICAL SAFETY
ORGANISATIONS
NETWORK

ETSON SECRETARIAT - GRS
Forschungszentrum, Boltzmannstr. 14,
85748 Garching, Germany
Phone +49 221 203 8700
www.etson.eu

Association n° W921001929