Journal of Hazardous Materials 111 (2004) 81–87

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Probabilistic analysis of accident precursors in the nuclear industry

M. Hulsmans*, P. De Gelder

AVN (Association Vinçotte Nuclear), Walcourtstraat 148, Brussels 1070, Belgium

Available online 26 April 2004

Abstract

Feedback of operating experience has always been an important issue in the nuclear industry. A probabilistic safety analysis (PSA) can be used as a tool to analyse how an operational event might have developed adversely in order to obtain a quantitative assessment of the safety significance of the event. This process is called PSA-based event analysis (PSAEA). A comprehensive set of PSAEA guidelines was developed by an international project. The main characteristics of this methodology are summarised.

This approach to analyse incidents can be used to meet different objectives of utilities or nuclear regulators. The paper describes the main objectives and the experiences of the Belgian nuclear regulatory organisation AVN with the application of PSA-based event analysis. Some interesting aspects of the process of PSAEA are further developed and underlined. Several case studies are discussed and an overview of the obtained results is given. Finally, the interest of a broad and interactive forum on PSAEA is highlighted.

Keywords: Nuclear industry; Accident; Probabilistic safety analysis

1. Introduction

Since most nuclear power plants have now a probabilistic safety analysis (PSA) model available, it can also be used as a tool to analyse incidents. Such a probabilistic accident precursor study provides a complement to the root cause analysis approach by focusing on how an event might have developed adversely, and implies the mapping of an operational event on a probabilistic risk model of the plant in order to obtain a quantitative assessment of the safety significance of the event. This process is called PSA-based event analysis (PSAEA). In order to benefit from state-of-the-art PSA features but also to assure repeatability of the analysis, a comprehensive set of PSAEA guidelines was developed. This PSAEA procedure was established by an international project on behalf of—and involving—the nuclear regulatory bodies from six countries.

The PSAEA procedure defines prerequisites for the PSA model and code, and identifies input requirements such as information on plant status, event sequence chronology and causes. The procedure then elaborates details for the following tasks: pre-analysis tasks, understanding the event, modelling the event, quantification, 'what if' analysis, analysis and interpretation of results, and conclusions and reporting.

The PSA model has to be prepared for PSAEA so that state-specific plant configurations and scenarios available within the PSA can be used. Also, test and maintenance unavailabilities are to be used that represent the situation in the plant at a particular point in time.

The probability of core damage conditional to the occurrence of the event (conditional core damage probability, or CCDP) is the main severity measure used in the procedure for PSA-based event analysis. Real or potential initiating events at one side, and condition events at the other side, have different characteristics and are treated differently in that the latter require the calculation of an instantaneous core damage frequency (ICDF) prior to obtaining the CCDP.

Special attention is devoted to the analysis of what could have happened but what did not necessarily happen during the real event sequence. The so-called 'failure memory' approach is applied: all known failures that occurred during an event sequence will be modelled as failed basic events, but all known successes—such as known equipment and operator action successes—will be modelled by basic events with nominal—and not perfect—behaviour.

* Corresponding author. Tel.: +32-2-5280264; fax: +3225-2-80102.
E-mail address: mh@avn.be (M. Hulsmans).
URL: http://www.avn.be.

0304-3894/$ – see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2004.02.029

Furthermore, the paper describes the experiences of the Belgian Nuclear Regulatory Organisation AVN with the application and the use of PSA-based event analysis. Some interesting aspects of the process of PSAEA are further investigated and underlined. Some examples of studies are discussed, together with some of their particularities and an overview of the obtained results. Finally, the interest of a broad and interactive forum on PSAEA is highlighted.

2. Methodology for PSA-based event analysis

2.1. Overview

The PSAEA procedure was established [1,2,4] in the framework of an international project on behalf of—and involving—the nuclear regulatory bodies from six countries. As a part of the project, first feasibility tests have been performed with the support of a utility.

The PSAEA procedure aims at the best-estimate assessment of the safety significance of an operational event using the available PSA model. Obviously, not all operational events can be analysed by PSAEA. The preceding screening of candidate events for PSAEA, as well as the precise use of its results (e.g. to identify or prioritise corrective actions), are not included in the scope of this procedure.

The PSAEA procedure defines prerequisites for the PSA model and code, and identifies input requirements suitable for incident investigations. It elaborates details for some pre-analysis tasks, understanding the event, modelling the event, quantification, 'what if' analysis, analysis and interpretation of results, and conclusions and reporting. As to the quantification, it explains the different characteristics and calculation treatment employed for real—or potential—initiating events and condition events, in order to obtain the probability of core damage conditional to the occurrence of the event.

2.2. Basic concepts and preliminaries

2.2.1. Types of events

The analysis of three different types of operational events is covered:

- Real initiating event, defined as an event that corresponds to an initiating event as modelled in the PSA. An initiating event will challenge one or more safety systems.
- Potential initiating event, which is a plant disturbance that required the plant or the operator to respond in some way, but which did not lead to an initiating event. One example could be a failure in a support system that was recovered before the reactor tripped. The treatment of real and potential initiating events is however quite similar.
- Condition event, during which the ability of the plant to respond to an initiating event is compromised (which corresponds to a certain loss of defence in depth) or during which the expected frequency of initiating events is increased. During its duration, a condition-type event causes an increase in the instantaneous core damage frequency.

Also, an event is either a direct event (if it is mapped on the PSA of the plant in which it actually occurred) or a transposed event (if it is mapped on the PSA of another plant).

2.2.2. Risk measures and event importance measures

Distinction has to be made between the following risk (= core damage) measures to be derived from the PSA model:

- The cycle-averaged core damage frequency (CDF), which is a mean core damage frequency during a typical calendar year (all plant states averaged);
- The instantaneous CDF, which is specific to a particular plant state and configuration;
- The baseline CDF, calculated by setting all test and maintenance unavailabilities of the instantaneous CDF to zero.

The following event severity measures are considered:

- The conditional core damage probability: for an initiating event, the CCDP is the conditional probability of core damage given the event. For a condition event, the CCDP is the increase of the core damage probability due to the event (increase in the instantaneous core damage frequency (ICDF) multiplied by the duration of the condition).
- The instantaneous core damage frequency: it applies only to condition-type events, is used as an intermediate step in the calculation of the CCDP.

2.2.3. Failure memory approach

The modelling approach of probabilistic event assessment is consistent with what has been termed as the 'failure memory' approach. The aim of a PSAEA is to assess what else could have happened in an incident, but which did not necessarily happen during the incident, and that would lead to core damage. This implies a different treatment in the modelling of the observed successes and failures during the incident.

All failures observed in the event (either equipment failures or failed operator actions) are to be modelled as such in the event analysis. This means that the corresponding basic events are to be failed, e.g. by setting their failure probability to one. Partial failures (equipment that did not perform correctly) are also modelled as such, for instance increasing their failure probability.

The system and operator action successes, however, should be ignored when the event is evaluated. Their failure probabilities should keep their nominal values in the PSA. If, to the contrary, successes would really be modelled as zero failure probabilities, one would always find the trivial

result that—a posteriori—the CCDP has been zero since core melt did not actually happen.

2.2.4. Preliminaries

There are of course some specific requirements for the PSA models in order to be suitable for performing PSAEA, such as a full documentation of the model and the existence of sufficient quantification capabilities of the computer code. These requirements will however be fulfilled in most state-of-the-art PSAs.

Before starting event analysis, a number of activities on the PSA model to be used are needed. These are, for instance, ensuring suitable quality in the model quantifications, compilation of information on both PSA study and plant maintenance scheduling, or screening criteria considerations.

Also, an assessment of an event transposed from one plant to another plant entails careful consideration of information, e.g. the chronology of the event, plant status, human factors or test and maintenance unavailabilities.

2.3. Major steps

2.3.1. Understanding the event

To develop a suitable timeline diagram, the analyst should first develop a sequence of basic events that constitute the incident, placing occurrences such as the initial conditions of the reactor, any demand for reactor trip, any demands on frontline systems or operator actions following a demand for reactor trip or a demand for power reduction, any action that should have been performed by the operator but was not performed, any change in the plant operational state defined in the PSA, and the final conditions of the reactor. Later in the analysis the sequence of events is completed with more information.

An important task is the identification of the event phases. An event may consist of one or more phases of type initiating event, potential initiating event or condition, which may lead to multiple quantifications.

In addition, the plant operational state (POS) must be determined for the incident. The POS for a real or potential initiating event phase is the POS existing at the initiation of the event phase. A condition event may span over more than one POS, in which case the incident analysis may be divided in as many cases as needed to obtain an accurate picture of the risk during the adverse condition. A challenging condition may persist not only for more than one POS, but also for many years (up to the total operation of several plants since construction).

The event is represented at component level on the timeline diagram to include:

- Expanded information on initial conditions, including information on components known to be failed, degraded or on preventative maintenance at the initiation of the event.
- Component failures that caused failures at system level should be identified and included on the timeline.
- If any failed components were later recovered by the operator, the recovery should be included on the timeline.
- Unrevealed failures (failures of standby components that were not demanded during the incident).

2.3.2. Modelling the event

Modelling the event consists of:

- Identifying the event trees to be used for modelling the event phase.
- Checking that the (part of the) model to be used for analysis does not contain any inappropriate simplifications.
- Identifying the basic events in the PSA model that are to be modified in order to map the event. In some cases, it may be necessary to make allowances for discrepancies between the PSA level of detail and the level of detail with which the event was reported.
- Making model modifications and identifying the appropriate data settings.

Special provisions are made for the modification of the model to include common cause basic events that appeared during the previous analysis task. Other delicate point is the modelling of human actions. While it is not recommended that in the course of a PSAEA the existing human error probabilities are modified, some peculiarities of the event may recommend its modelling, for instance if available times are quite different from the assumed PSA value. The modelling of operator recoveries must also be properly assessed. Recovery actions that were performed by the operators, however, should be modelled according to the failure memory approach.

2.3.3. Quantification

A preliminary quantification is performed to provide initial information on the event and to allow to identify particular aspects that may require further attention. The failure memory approach is applied and the recovery actions associated with demanded failed components are modelled. The preliminary quantification is used to assess the leading cut-sets and basic events whose fractional contribution to core damage frequency is remarkable.

The information obtained from the preliminary quantification is used to investigate whether further analysis of recovery actions is necessary. The need to improve the modelling of important recovery actions is evaluated.

The conditional core damage probability is calculated once all information on the event has been introduced in the model. Its value determines the safety significance of the event.

2.3.4. ‘What if’ analysis

The structured analysis of sensitivity issues is an important task in the final assessment of an incident. A number of ‘what if’ analyses are proposed, such as variations of plant operational state; unavailable equipment; common

cause failures; poor operator performance; particular operator and system failures; modelling of a similar event in a different location; modelling with a missed test. For every 'what if' case, a separate quantification is performed.

2.3.5. Final steps

Analysis and interpretation of results may include the identification of the dominant contributors to the risk, the investigation of the sensitivity of the results to any (reasonable) change in the data used, and the study of the effect of analysis uncertainties on the results obtained using the sensitivity and importance analysis modules of the PSA computer code.

A full report presents an overview of the performed analyses and highlights the conclusions. It presents in particular:

- The best-estimate conditional core damage probability for the event.
- The identification of 'what if' scenarios that were more risk significant than the base case. These give an indication of the potential risk from a similar reoccurring event, under slightly different circumstances or in a slightly different manner.
- Conclusions from the analysis and interpretation of results.
- Feedback to the PSA model. This should comment on the possibility or even the convenience to modify the PSA model to reflect any changes that should be made to improve it, for instance to remove undue assumptions observed in mapping the event.

3. AVN application of PSAEA

3.1. Trial application

After having contributed to the initial development of the PSAEA guidelines, AVN applied this approach to two events [3] that occurred at Belgian pressurised water reactors. These pilot studies demonstrated the applicability of the PSAEA method in general and its applicability to the models of the Belgian state-of-the-art PSAs in particular. Obtained insights include the following:

- Actual event sequences can be quite complex and might require the modelling of subsequent event phases. One might also have to take into account that, after an incident, the plant may spend significantly more time in a particular plant state (the so-called 'safe state') than it would have spent normally, a condition which can however involve substantial additional accumulation of risk.
- Some events can be regarded as condition events as well as (potential) initiating events.
- As expected, the consideration of relevant 'what if' questions enabled the identification of potential areas for safety improvement in various domains of the nuclear power plant, and often also the quantitative assessment of particular modifications that can be considered as an option. Examples are: alternative configurations or priority rules for safety equipment shared on site level, preventive or mitigating measures to be considered for inclusion in technical specifications for safety equipment or in procedures, awareness of the impact of some test intervals, appropriateness of automatic actions (e.g. start logic) with unintended adverse impact on (other) safety missions, appropriateness of specific operator instructions.

3.2. Objectives

The objectives of the current PSAEA program of AVN are mainly focused on (1) the determination of the quantitative importance of a few well-selected operational events per year, and—if sufficiently significant—on (2) the subsequent identification of potential safety issues for improvement (based on the real best-estimate case as well as on relevant 'what if' questions). AVN considers the identification of potential safety issues for improvement to be among the most important outcomes of the study, because they have the chance to lead to improvements and to make a real difference.

In addition, the experience gained with the performance of this first PSA application is used to enhance the awareness of typical risk figures associated with both exceptional and more common events, and to feedback on the PSA model itself, where found appropriate.

3.3. Process of PSAEA

The PSAEA process is being integrated in the larger process of follow-up of operating experience, and involves the following phases: screening and selection of reported events, analysis of events, internal review by PSA specialists as well as plant inspectors and staff members involved in experience feedback, presentation of the analyses to the utility for comment and for further consideration, and follow-up of identified safety issues for improvement (if appropriate).

Among the issues that are felt to be important to communicate to non-PSA experts in order to get a correct grasp of the objectives and the context of AVN's PSAEA program, the following can be mentioned:

- When performing PSAEA, the assumptions applied in the PSA model, as well as the PSA limitations, have to be taken into account. In order to allow a correct interpretation of the numerical results, the analysis report should clearly document the detailed modelling assumptions of the event and should identify relevant PSA hypotheses that are particularly restrictive (if any). On the other hand, however, it is in most cases not feasible to modify fundamental underlying PSA hypotheses for the purpose of one particular PSAEA study.
- Some useful criteria are given to help with the interpretation of these numerical values. A high CCDP implies

a high importance for experience feedback. On the other hand, however, a low CCDP value does not necessarily imply a low importance for experience feedback. Recurrent small events or small events that indicate a lack of safety culture or configuration control, for instance, can nevertheless—and fully legitimately—be regarded as important for experience feedback. At this point, the complementarity of the classical and the probabilistic approaches to event analysis appears.

3.4. Examples of PSAEA

3.4.1. Wiring error compromising normal power supply to three safety trains

In the aftermath of the troubleshooting of another event (spurious safety injection signal during a protection logic test in the shutdown state), a wiring error was discovered in 1998. The wiring error dated from a modification in 1995, and caused loss of voltage on the 6.6 kV bus upon ESFAS[1] signal actuation. The wiring error was not revealed by the modification validation test (too limited scope of the validation test) nor by the periodic tests (particular position of emergency diesel generator control switch did not allow to detect this error). This wiring error existed in the three safety trains (common cause failure).

This event is considered as a long lasting condition event (2.6 years): failure of the normal power supply to the 6.6 kV bus in case of any safety injection signal (manual or automatic). Relevant plant modes are the power states and intermediate shutdown. The condition event is an important accident precursor since it implied a large CCDP of 1E-4 over all relevant plant states and over its entire duration.

An identical modification has been performed in another unit at the same site. The utility was asked to verify the absence of the same wiring error in the other unit.

3.4.2. Air binding of an RHRS[2] pump during intervention at midloop conditions

During the cold shutdown state, the plant was in the process of decreasing primary coolant inventory level towards midloop conditions. Eventually, an undershoot of the midloop primary coolant level occurred and led to air intake of the operating residual heat removal pump. Upon the triggered level drop alarm, the running residual heat removal pump was stopped immediately and a low pressure safety injection pump was manually started in order to restore the primary coolant level. The PSAEA analysis showed that for this initiating event the CCDP was in the range of 1E-4 > CCDP > 1E-6. The event was therefore regarded as an accident precursor.

[1] ESFAS: Engineered Safety Feature Actuation System.
[2] RHRS: Residual Heat Removal System.

3.5. Summary of PSAEA results to date

Since 1997, all reported events on Belgian nuclear power plants have been screened by AVN for PSAEA. Screening criteria include qualitative importance criteria as well as feasibility considerations (like scope of PSA, availability of data). In general, about 8–10% of the reported events are selected for PSAEA analysis. The following events have been quantified (listed in order of decreasing CCDP) [5,6]:

1. Total loss of service water during a short period (two subsequent initiating events).
2. Risk of internal flooding of auxiliary feedwater system equipment (condition event).
3. Wiring error compromising the operability of normal power supply to all three safety trains (condition event; see first example above).
4. Inadvertent primary coolant level drop during midloop operation (initiating event).
5. Air binding of a residual heat removal pump during intervention at midloop conditions (initiating event; see second example above).
6. Loss of suppletion of auxiliary feedwater tanks while emptying suppletion tank to the condenser (considered as a potential initiating event).
7. Main feedwater isolation check valve stuck open (condition event).
8. Unavailability of turbine driven auxiliary feedwater pump, and two reactor trips (condition event and initiating event).
9. Uncontrolled dilution of the primary circuit during start-up (initiating event).
10. Same event as 6, but considered as a condition event.
11. Automatic start of auxiliary feedwater system unavailable during plant start-up (condition event).
12. Unavailability of auxiliary feedwater system automatic flow control by common cause failure (condition event).
13. Simultaneous unavailability of two out of three component cooling system trains (condition event).

The first eight events listed above yielded CCDP values greater than 1E-6 and are therefore considered as accident precursors. The first three events yielded CCDP values greater than 1E-4 and are therefore considered as important accident precursors.

Fig. 1 shows a summary of the results of all PSAEA studies mentioned above. The graph contains the order of magnitude of the best-estimate CCDP (in decreasing order), and—for condition events—also the best-estimate ICDF. Moreover, it shows the order of magnitude of the CCDP induced by several credible ‘what if’ cases (which—in some cases—induce a considerably larger CCDP than the best-estimate calculation, and which therefore should also be considered when discussing the safety issues involved). It is felt that such representations can help demonstrate both the absolute and the relative safety significance of an event.

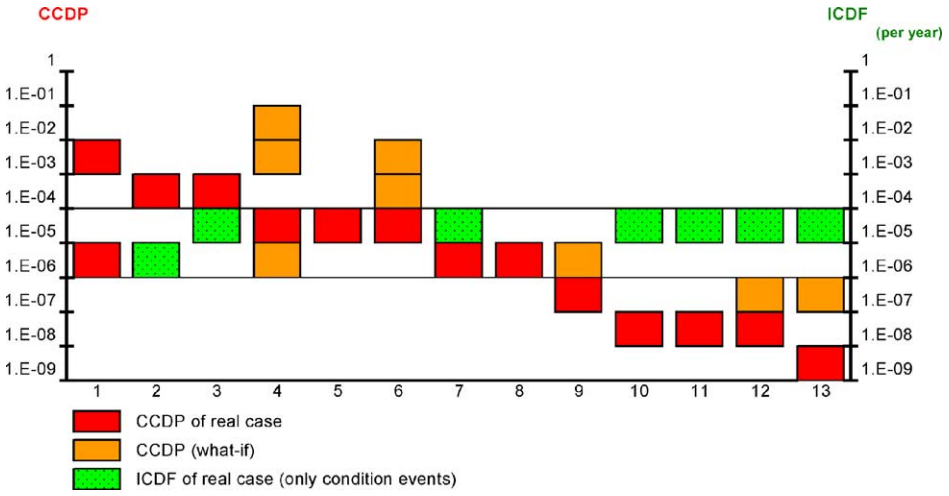

Fig. 1. Summary of PSAEA results to date (orders of magnitude).

The analysis results cover a wide spectrum of event severity. They have been submitted to the utility for consideration and follow-up. In addition to the specific conclusions for each event, relevant insights have been gained regarding for instance event modelling and the interpretation of results. The following observations are made:

- Results are sensitive to the particular human reliability assessment, especially for recovery actions after initiating events.
- In some cases where the reference PSA model is dominated by a penalising scenario, other scenarios have not always been developed in great detail. If the event to be analysed, however, corresponds with one of the latter scenarios, the resulting PSAEA model might tend to be oversimplified and has to be interpreted with caution.
- The potential issues for safety improvement relate to: preparation of interventions (safety assessment, planning, instructions), configuration control, safety culture and questioning attitude, plant configuration during midloop operation, midloop operation practices, appropriateness of alarms and associated instructions, up-to-date character of procedures.

3.6. Other experiences with PSAEA

In order to ensure a close contact with other experiences and developments in this field, AVN has taken the initiative to organise an annual meeting on PSAEA in the nuclear industry. The interaction with a wide audience of other practitioners and stakeholders has not only advanced the understanding of many technical issues, but it has also contributed to the evolution of a broader view on the process itself of PSAEA by a nuclear regulatory organisation.

Among the topics of interest for such a forum are the objectives of a PSAEA program (which have an unexpectedly large influence on the particular technical approaches to event analysis, and a reiteration on which can help in directing further research), the process itself of PSAEA (different stakeholders have different roles; there are programs of very different amplitude and screening practices; how are results presented to decision makers, and how is feedback and follow-up organised?), the technical approaches to PSAEA, the harvest of the latest findings, and most importantly the presentation of case studies to illustrate technical topics of interest and to invite for discussion.

4. Conclusion

PSA-based event analysis has matured beyond the stage of R&D and has increasingly become a part of the AVN process of feedback of operating experience. It constitutes in fact the first PSA application—after the overall safety evaluation itself—for the Belgian nuclear power plants.

Acknowledgements

The PSAEA methodology was initially established by Enconet Consulting as contractor of an international project. Sponsoring and feedback was provided by regulatory organisations in Belgium (AVN), Canada (the former AECB), the United Kingdom (NII), Spain (CSN), Sweden (SKI) and Switzerland (HSK).

References

[1] Enconet Consulting, A Framework for the PSA-Based Analysis of Operational Events, Final report, April 1997.
[2] P. Boneham (Enconet), The Benefits of Using PSA to Enhance the Feedback of Operational Experience at Nuclear Power Plants, in: Proceedings of the COPSA '97 Conference, Edinburgh, October 1997.
[3] M. Hulsmans, P. De Gelder (AVN), P. Boneham (Enconet), Using State-of-the-art PSA to Support Operational Event Analysis in NPPs:

Methodology, Experience and Insights, PSAM 4, New York, September 1998.
[4] M. Hulsmans, P. De Gelder (AVN), E. Meléndez Asensio, R. Muñoz Gómez (CSN), Development of Guidelines for PSA-based Event Analysis (PSAEA) in an International Project, in: Proceedings of the OECD Workshop on Precursor Analysis, Brussels, March 2001.
[5] M. Hulsmans, P. De Gelder (AVN), Application and Use of PSA-based Event Analysis in Belgium, in: Proceedings of the OECD Workshop on Precursor Analysis, Brussels, March 2001.
[6] M. Hulsmans, B. Tombuyses, P. De Gelder (AVN), Application and Use of PSA-Based Event Analysis in Belgium, PSAM 6, San Juan, Puerto Rico, June 2002.