

Nuclear Safety

ISBN 92-64-02091-8

## **CSNI Technical Opinion Papers**

No. 6

*PSA-based Event Analysis*

© OECD 2004  
NEA No. 4409

NUCLEAR ENERGY AGENCY  
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

## **ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT**

Pursuant to Article 1 of the Convention signed in Paris on 14<sup>th</sup> December 1960, and which came into force on 30<sup>th</sup> September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became members subsequently through accession at the dates indicated hereafter: Japan (28<sup>th</sup> April 1964), Finland (28<sup>th</sup> January 1969), Australia (7<sup>th</sup> June 1971), New Zealand (29<sup>th</sup> May 1973), Mexico (18<sup>th</sup> May 1994), the Czech Republic (21<sup>st</sup> December 1995), Hungary (7<sup>th</sup> May 1996), Poland (22<sup>nd</sup> November 1996); Korea (12<sup>th</sup> December 1996) and the Slovak Republic (14<sup>th</sup> December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

## **NUCLEAR ENERGY AGENCY**

The OECD Nuclear Energy Agency (NEA) was established on 1<sup>st</sup> February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20<sup>th</sup> April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, the Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

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

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

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

### **© OECD 2004**

Permission to reproduce a portion of this work for non-commercial purposes or classroom use should be obtained through the Centre français d'exploitation du droit de copie (CCF), 20, rue des Grands-Augustins, 75006 Paris, France, Tel. +33-(0) 1 44 07 47 70, Fax +33 (0) 1 46 34 67 19, for every country except the United States. In the United States permission should be obtained through the Copyright Clearance Center, Customer Service, +1 (508) 750-8400, 222 Rosewood Drive, Danvers, MA 01923, USA, or CCC Online: <http://www.copyright.com/>. All other applications for permission to reproduce or translate all or part of this book should be made to OECD Publications, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

## COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

\*\*\*\*\*

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

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

Nuclear Safety Division  
OECD Nuclear Energy Agency  
Le Seine St-Germain  
12 blvd. des Iles  
92130 Issy-les-Moulineaux,  
France







## TABLE OF CONTENTS

Foreword .....	5
Perspective .....	9
Introduction .....	11
Background .....	11
General considerations .....	12
General methodology for the analysis of an event .....	13
Discussion .....	17
Conclusions and recommendations .....	20
References .....	21



## **PERSPECTIVE**

**Ashok Thadani**  
Chairman of CSNI

Nuclear safety regulation is traditionally deterministic, with prescriptive rules about design, operation and quality assurance. In general, conservative assumptions are used throughout, in order to compensate for the lack of knowledge of the events considered and the physical processes involved. Such an approach in many cases also serves to obtain substantial safety margins. The rules and regulations were conceived at a time that probabilistic safety analysis (PSA) was not well developed. Probabilistic considerations were nevertheless implicitly considered to conclude that certain accidents need not be considered in the design basis (e.g. pressure vessel rupture) and also resulted in requirements to consider single failure of an active component, but not a passive component following a postulated design basis accident.

Over the past 25 years since the issuance of WASH 1400, PSAs have in fact become an important supplement to the deterministic analysis in checking the safety level of a facility and in improving it by identifying design and operational weaknesses. Rapid advancement and new tools developed over the past 10 years have demonstrated the usefulness of PSA in many safety applications. A PSA, if properly used is an effective tool for supporting the decision-making process in the context of risk management of NPPs. This can be decision making by designers, operators or regulatory authorities.

A shift has occurred in the last few years in which the growth of the methodology has led to a large increase in use of PSA for regulation. The positive attribute of this shows how well PSA is evolving into a highly recognised tool to assist regulatory decision makers in their work. As more experience is gained, PSA becomes a valuable asset in many areas of nuclear power plant safety and hence the focus of PSA experts has turned towards PSA being used to improve the effectiveness of regulatory practices.

Both deterministic and probabilistic approaches have their strengths and weaknesses.

This Technical Opinion Paper provides the reader with a clearer understanding on both the benefits and disadvantages in using PSA to analyse operational events in order to facilitate better operational feedback. Some of the criticisms regarding the limited treatment of epistemic and aleatory uncertainties as well as the issue of completeness apply to both the probabilistic and the deterministic approaches. It is important that we continue to enhance the quality of the probabilistic techniques to more fully address these issues. However, it should be noted that the methodology is sufficiently mature for many applications both by the regulators and the operators to make more effective decisions. This Technical Opinion Paper addresses an important issue of what we are learning from operating experience. The paper describes how the PSA techniques can be used to analyze operational events or degraded conditions to better understand their risk significance which would lead to better informed decisions.

## PSA-BASED EVENT ANALYSIS

### Introduction

This Technical Opinion Paper represents the consensus of risk analysts and experts in the NEA member countries on the current state-of-the-art in PSA-based Event Analysis (PSAEA)\* for nuclear power plants. The objective is to provide a clear technical opinion on the current state of PSAEA to decision makers in the nuclear community. As such, the intended audience is primarily nuclear safety regulators, senior researchers and industry leaders. Government authorities and nuclear power plant operators may also be interested.

### Background

Operational experience feedback is since long an important pillar of the continued safe operation of nuclear power plants.

The final objective of this operational experience feedback analysis is to identify possible actions (design modifications or changes in operational conditions) that can be undertaken to avoid reoccurrence of this or similar events in future. Operational experience feedback consists in the analysis of operational events that occurred at the nuclear power plant (NPP) under consideration, or even at other NPPs.

Originally, the operational events were analysed within a “deterministic” approach. This approach consists mainly of an in-depth analysis of the operational event, to identify, amongst others, root causes, aggravating factors that occurred during the event, and possible actions to avoid reoccurrence.

---

\* In this paper, the term PSA-based Event Analysis (in short, PSAEA) will be used as a synonym for other frequently used terms such as: probabilistic event analysis, accident sequence precursor (ASP) analysis, probabilistic precursor analysis, precursor analysis.

For most NPPs, a Probabilistic Safety Analysis (PSA) is nowadays available. It is used in a complementary approach to the deterministic one for the overall safety evaluation of NPPs. Amongst several PSA applications that have been developed in the meanwhile, one application consists of the analysis of operational events. In the past, it has often been quoted as Accident Sequence Precursor analysis (mainly based on the programme originally developed in the US); afterwards other terms such as PSA-based Event Analysis (PSAEA) have been introduced.

Since many years now, the analysis of operational events is complemented by this probabilistic approach, which is the subject of this Technical Opinion Paper.

## **General considerations**

### ***Types of events to be analysed***

An event is categorised as a direct event (when it occurred at the plant for which the PSA is used for the analysis) or as a transposed event (when the event occurred at another plant). The analysis of a transposed event can be valuable to evaluate the relevance of events for another plant or plant design.

Three types of events can be distinguished:

- Real initiating event, where the operational event corresponds to an initiating event as modelled in the PSA, or that could be modelled in the PSA.
- Potential initiating event, where an actual plant disturbance that required the plant or operator to respond in some way did not lead to an initiating event. One example could be a failure in a support system that was recovered before the reactor tripped.
- Condition event, in which the ability of the plant to respond to any initiating event is compromised or in which the expected frequency of initiating events is changed. A condition-type event causes an increase in the instantaneous core damage frequency during a period of time.

### ***Requirements on the PSA model and preparing the PSA model for PSAEA***

There are of course some specific requirements for the PSA models in order to be suitable for performing precursor analysis, 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.

### ***Screening***

The selection of the operational events to be analysed with PSAEA is a first important issue, but is treated as a separate topic. The screening policy also depends on the objectives of the particular PSAEA programme. In general, however, qualitative and quantitative screening criteria are used in order to reduce the number of events to be analysed in detail. It is then assumed that screened-out events are either not safety significant or cannot be analysed with PSAEA. Screening criteria may include considerations on PSA scope and hypotheses, the number and nature of the challenged safety barriers, the occurrence of common cause failures, the additional unavailability of safety equipment, the duration of the event, etc.

### **General methodology for the analysis of an event**

The general methodology for the PSAEA-analysis of an event consists typically of the following steps.

#### ***Pre-analysis activities***

This pre-analysis task is the initialisation of the analysis process of the event. It collects the information initially available on the event.

Further, the objectives of the analysis are identified, taking into account any boundary conditions that might exist for the analysis (limited information, manpower effort, ...).

### ***Understanding the event***

The analyst should first develop a clear understanding of the events that constitute the incident, 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 actions that should have been performed by the operator, but were not, any changes in the plant operational state defined in the PSA, and the final conditions of the reactor.

This task often leads to the development of a timeline diagram that summarises the analyst's understanding of the event, in a form suitable for inputting to later activities in the event analysis. It may contain several event phases, when an event spans over more than one plant operational state (POS).

The event is represented at component level so that a link can be established with the PSA model mapping later in the analysis. The following information is typically considered: initial conditions, including information on components known to be failed, degraded or on preventative maintenance at the initiation of the event, any failed components later recovered by the operator, potential for common cause failures, etc.

### ***Modelling the event***

Modelling the event (also often called “mapping of the event on the PSA model”) consists typically of: identifying the event trees to be used for modelling the event phase(s), checking that the models to be used for the analysis of the event do not contain inappropriate simplifications, identifying the basic events in the PSA model that must be modified in order to map the event, making model modifications (e.g. due to the fact that the relevant operator recovery actions are often not considered in the base PSA model) and identifying the appropriate data settings.

### ***Quantification***

The quantification task contains typically the following steps: a preliminary quantification that provides initial information on the event and allows the analyst to identify particular aspects that may require further attention, an investigation whether further analysis of recovery actions is adequate, final quantification.

For quantification, the failure memory approach is followed: all failures observed in the event (either equipment failures or failed operator actions) are modelled as such in the event analysis; partial failures (that is, equipment that did not perform correctly) are also modelled as such, for instance raising their probability of failure. However, the system and operator action successes are “ignored”, i.e. their nominal failure probabilities are applied. [If they would not be ignored, their failure probability would be set to zero and the CCDP (see below) would be zero for all events in which no core damage occurred.]

The most frequently used event severity measures are:

- the conditional core damage probability (CCDP), representing the probability of core damage conditional on the incident occurring;
- the instantaneous core damage frequency (ICDF), which is only an appropriate measure of severity for a condition-type event, and is used as an input to the calculation of the conditional core damage probability due to the event.

#### ***“What if?” analysis***

This task is optional. It provides a structured analysis of sensitivity issues of an incident. A number of “What if?” analyses are proposed, among them, variations of plant operational state; unavailable equipment; common cause failures; generally poor operator performance; operator and system failures; modelling of a similar event in a different location; modelling with a missed test.

“What if?” analyses are often useful to yield a more complete picture of the potential safety issues involved. In practice, not all possible sub-events and alternative conditions can easily be formulated in strict probabilistic terms: as their occurrence probability remains unquantified, they cannot be included in one overall probabilistic model to yield one global CCDP figure. If they are potentially relevant, they need therefore to be addressed as a “What if?” case: an alternative case that is quantified separately.

So “What if?” analyses can be used to identify and to assess credible scenarios that differ from the event sequence or from the particular conditions that prevailed in the occurred incident and which have unquantified occurrence probabilities, but which might induce a – perhaps significantly – higher CCDP. They might generate additional insights that are relevant for the definition of appropriate corrective actions.

Finally, “What if?” analyses can also be used to evaluate the impact of proposed corrective actions.

### ***Analysis and interpretation of results***

This task typically includes: the identification of the dominant contributors to the risk from the event, investigation of the sensitivity of the results obtained to reasonable (achievable) changes in hypotheses or the values of the data used, study of the effect of analysis uncertainties on the results obtained.

### ***Conclusions and reporting***

The final report presents an overview of the analysis as performed, documents all modelling steps, and highlights the conclusions obtained. In particular, it presents typically: the estimated risk from the event, the identification of significant “What if” scenarios, conclusions from the task of Analysis and Interpretation of Results. This detailed documentation is primarily oriented towards the PSA-specialists (for review purposes, traceability of the analysis, etc.). An executive summary is very recommendable. The latter is especially valuable for non-PSA specialists (plant inspectors, decision makers, etc.) who are more interested in lessons learned from the event analysis and potential remedial actions to be taken.

In the framework of feedback of operating experience, one may also suggest solutions or improvements in order to reduce the probability of occurrence of similar event sequences or to reduce their associated risk. The behaviour of the plant in case of reoccurrence of the event after having performed these improvements can often be quantified and hence be used by decision makers as safety argument.

In countries with a PSAEA programme of large amplitude, a statistical processing of the results can be performed in order to monitor risk and to discern trends.

PSAEA can also generate feedback concerning the PSA model itself, such as suggestions to extend or improve the model, to remove undue assumptions observed in mapping the event, etc.

## **Discussion**

The OECD/NEA is very active in the field of operational experience feedback for NPPs. Within the Working Group on Operating Experience (WGOE, formerly PWG 1), event reporting and related discussions on operational experience feedback has a long tradition. Within the Working Group on Risk Assessment (WGRisk, formerly PWG 5), PSAEA is part of the working programme since many years. In the past, common meetings of WGOE and WGRisk on PSAEA have been organised, with the aim to bring together the end-users (mainly represented by WGOE) and the people involved in the methodological development and in performance of PSAEA (mainly represented by WGRisk). It led to the organisation of a Joint WGOE/WGRisk Workshop on Precursor Analysis. The discussion in this Technical Opinion Paper is to a large extent based on this Workshop [1].

### ***Benefits of PSA-based Event Analysis***

Now that PSAEA has been applied since many years in the operational experience feedback process in several countries [2] and since PSAEA is considered a mature application of PSA, the benefit of the use of this probabilistic approach in complement to the deterministic one, is no longer at stake. PSAEA indeed provides additional insights and possibilities compared to deterministic event analysis, as for example:

- it provides some quantitative measure of risk importance of the event with sometimes surprisingly high or low values;
- it is particularly suited (compared to the deterministic approach) for evaluating the importance of events with multiple failures and/or unavailabilities;
- it gives valuable insights in the lines of defence left for that specific event;
- it helps to determine the appropriate level of attention that should be devoted to the follow-up of an event;
- the methodology allows to consider quite complex events or combinations of events;
- it can be used to help identifying and to evaluate the adequacy of potential corrective measures;
- it gives the possibility to study “what if” scenarios and to identify safety issues that might have been overlooked or underestimated;

- it can be used for trending of plant or industry performance over time;
- the results can be used to confirm or monitor a level of safety; and
- the analysis serves the purpose of identifying outliers that need special attention.

### ***Development and harmonisation of methodology***

In some countries, large organisations have developed their own approach to PSAEA. In other cases, several countries joined forces to develop a common procedural framework. Several fora allow to exchange (sometimes detailed) technical information on the methodology of PSAEA. The exchanges and common efforts have led to some harmonisation, although differences (will) remain.

Harmonisation between programmes has certainly taken place in the move from simplified models to more sophisticated ones. Indeed, in the past, simplified models were extensively used for PSAEA. With the improved computation capabilities, and also due to user's needs inside and outside the PSAEA programmes, the probabilistic models have become more developed. In many cases, the full scope and state-of-the-art living PSA models are now used for PSAEA. No optimum level of detail for the models can be prescribed. At one hand, simplified models could be used in some cases, although the need of an in-depth modelling of all dependencies, in particular for support systems (cooling systems, electrical systems, I&C, instrument air, ...) should be emphasized. At the other hand, even when using full scope PSA models, improvement or extension of the existing PSA model to some degree for a correct modelling of a particular event, is sometimes needed.

Nevertheless, on-going exchanges of information on PSAEA also point out that methodological aspects may still differ from programme to programme, often determined by differences in the objectives of the PSAEA-programme.

Examples of such issues are: the analysis of long-lasting events (impact evaluated over the whole time span or over one year), events applicable to many plants (impact to be multiplied by number of plants or to be evaluated per plant), degraded events, etc.

Therefore, one should remain very careful when trying to compare numerical results amongst different PSAEA programmes. For instance, it is well known that many different risk measures are used in the different PSAEA programmes. They cover for instance risk measures related to particular events

(ICDF, CCDP, event importance, ...) or risk measures related to all plants within a given country (e.g. Annual ASP index, ...); most countries use risk measures with respect to core damage, while others reflect a risk of reaching beyond design basis conditions. A harmonisation of these aspects is not strictly needed, since they may depend on the objectives of the PSAEA programme, but each application should clearly define and describe the risk measures used. Further, other aspects such as different approaches in the hypotheses on the (un)availability of components, on potential common mode failures, etc., strengthen the need to be careful when comparing numerical results amongst different PSAEA programmes.

There are several reasons to remain careful when using PSAEA for looking at trends. Indeed, changes over time in screening criteria, in analysis methodology and in PSA scope and hypotheses, the move from simplified to very detailed models, and periodic updates of the PSA models, all lead to the need of a very careful attitude when considering trend analysis.

A potential future development in methodology, which should be considered, especially in view of adequate risk ranking, is the extension of PSAEA towards PSA level 2. Indeed most risk measures as discussed above focus on core damage risk (provided by PSA level 1), while risk measures linked to release frequency and magnitude are more appropriate for the evaluation of radiological consequences. This methodological extension would allow a better ranking of events involving containment bypass aspects (e.g. steam generator tube rupture events, containment isolation degradation, etc.).

### ***Complementarity and further integration of the deterministic and probabilistic approaches***

The complementarity of both approaches is clear. At one hand, a good probabilistic analysis of an event cannot be done without a preceding detailed deterministic analysis, i.e. of the root cause(s) of the event. At the other hand, the probabilistic approach quantifies the potential consequences, and may therefore especially provide valuable additional insights in the importance of the event and of similar event scenario's. While the deterministic approach focuses mainly on the root causes of an event, the probabilistic approach gives information (also quantitatively) on the remaining lines of defence for that event.

Further, the need to preserve the application of both approaches in the operational experience feedback process is also clear, since some events remain difficult for probabilistic treatment. For instance, for events where the root

causes are strongly linked to organisational factors, the impact on the global plant performance (increased human error probabilities, increased failure or unavailability probabilities, etc.) is difficult to quantify.

A further integration of deterministic and probabilistic event analysis is an objective of the operational experience feedback process in many countries. However, no precise recommendations on how to achieve this are pointed out today. It is suggested that this should be a further point of interest for both working groups WGOE and WGRisk [1].

One aspect which might be considered in this context is whether event reporting (for instance via INES, ...) should be more risk informed. It is clear that INES was developed as a fast information system towards the public, and that this option does not allow waiting for results of more sophisticated analyses. However, important discrepancies between INES ranking and the ranking based on risk measures are observed regularly and should attract appropriate attention. In some countries investigations are ongoing to include risk measures more systematically in operational event ranking.

## **Conclusions and recommendations**

The use of PSAEA in the operational experience feedback process is nowadays widely accomplished. This approach has shown its benefits, especially in combination with the deterministic approach.

Over years, some harmonisation in the methodology and its application has been observed. Remaining differences, their reasons and their impact on results are better understood. However, a continuation of the intensive international exchange of experience with this approach remains highly recommendable.

An extended use of level 2 PSA for evaluating particular events (especially those with containment bypass or degradation in containment isolation aspects) should be recommended.

It is further recommended that the OECD Working Groups WGOE and WGRisk should continue to join efforts in the field of further integration of the deterministic and probabilistic approaches.

## References

- [1] NEA (2003), “Proceedings of the Joint WGOE/WGRISK Workshop on Precursor Analysis”, held in Brussels, 28-30 March 2001, report NEA/CSNI/R(2003)11.
- [2] NEA (2002), “The Use and Development of Probabilistic Safety Assessment in NEA member countries”, report NEA/CSNI/R(2002)18.



OECD PUBLICATIONS, 2 rue André-Pascal, 75775 PARIS CEDEX 16  
Printed in France.