Nuclear Safety ISBN 92-64-02157-4

CSNI Technical Opinion Papers

No. 4
Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants

Prepared by
Stefan Hirschberg, PSI, Switzerland

Comments by
George Apostolakis, USA
Attila Bareith, Hungary
Vinh N. Dang, Switzerland
Jaroslav Holy, Czech Republic
Manuel Lambert, France
Jeanne-Marie Lanore, France
Pierre Le-Bot, France
Johannes Mertens, Germany
Pekka Pyy, OECD/NEA
Ann Ramey Smith, USA
Bernhard Reer, Switzerland
Anthony Spurgin, USA
Olivier Sträter, Belgium
Magiel F. Versteeg, Netherlands

© OECD 2004
NEA No. 5068

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 14th December 1960, and which came into force on 30th 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 (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996); Korea (12th December 1996) and the Slovak Republic (14th 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 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th 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, 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. (33-1) 44 07 47 70, Fax (33-1) 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, (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

FOREWORD

The mission of the Working Group on Risk Assessment (WGRisk) is to advance the understanding and utilisation of probabilistic safety assessment (PSA) in ensuring continued safety of nuclear installations in member countries. In pursuing this goal, the Working Group shall recognise the different methodologies for identifying contributors to risk and assessing their importance. While the Working Group shall continue to focus on the more mature PSA methodologies for Level 1, Level 2, internal, external, shutdown, etc., it shall also consider the applicability and maturity of PSA methods for evolving issues such as human reliability, software reliability and ageing issues, as appropriate.

The WGRisk mandate states that: "The Working Group shall constitute a forum for exchange of information and experience of activities related to risk assessment in member countries. WGRisk shall prepare opinion papers on questions regarding the applicability of various aspects of risk assessment, results, insights and interactions with other analysis techniques to matters affecting nuclear safety or nuclear safety research. This shall include identifying and prioritising important regulatory issues requiring additional research."

In the late 1980s and early 1990s NEA/PWG5 (renamed WGRisk in 2000) issued several important statements on risk assessment. The paper on "The Role of Quantitative PSA Results in NPP Safety Decision Making" provided a major international consensus in this area and is still seen as an essential document. While developing and obtaining consensus on technical opinion papers is considered a very difficult task, the product is viewed as one of the most important aspects of the WGRisk programme of work.

This technical opinion paper is the result of the work of an expert task group. The task group developed a state-of-the-art report and held a workshop to further the discussions and derive this paper. The final products were reviewed and accepted by the members of WGRisk and the NEA Committee on the Safety of Nuclear Installations (CSNI).

The NEA Secretariat expresses its thanks to the WGRisk members listed below, who provided valuable time and considerable knowledge towards the development of this paper. The Secretariat also wishes to acknowledge the specific services of several key persons. Dr. Stefan Hirschberg and Dr. Vinh Dang provided clear insights on the objectives and overall co-ordination for completing the paper, editorial expertise and much of the basis for the in-depth technical analysis.

WGRisk members included: Dr. Jeanne-Marie Lanore and Mr. Manuel Lambert, IRSN, France; Mr. Pierre Le Bot and Ms. Hélène Pesme, EDF, France; Mr. Jan Holmberg, VTT, Finland; Mr. Magiel F. Versteeg, VROM, the Netherlands; Dr. Pieter De Gelder, AVN, Belgium; and the members of the WGRisk Human Reliability Task Group.

TABLE OF CONTENTS

TECHNICAL OPINION PAPER ON HUMAN RELIABILITY ANALYSIS IN PSA

Introduction

This technical opinion paper represents the consensus of risk analysts in the NEA member countries on the current state of the art of human reliability analysis (HRA) within probabilistic safety assessment (PSA) for nuclear power plants. The objective is to present to decision makers in the nuclear community a clear technical opinion of HRA status as implemented in industrial PSAs. The intended audience is primarily nuclear safety regulators, senior researchers and industry leaders. Government authorities, nuclear power plant operators and the general public may also be interested.

Why HRA?

Human performance may substantially influence the reliability and safety level of complex technical systems. For this reason, HRA constitutes an important part of PSA. Adequate treatment of human interactions in such studies is one of the keys to understand accident sequences and their relative importance to overall risk. The main objectives of HRA are:

1. To ensure that the key human interactions are systematically identified, analysed and incorporated into the safety analysis in a traceable manner;
2. To quantify the probabilities of their success and failure.
3. To provide insights that may improve human performance. Examples include: improvements of man-machine interface, procedures and training, better match between task demands and human capabilities, increasing prospects for successful recovery, minimising the impact of dependencies between human errors etc.

By adopting a structured and systematic approach to the assessment of human performance, it is possible to provide greater confidence that the safety and availability of complex technological systems such as nuclear power plants is not unduly jeopardised by human performance problems.

HRA development in PSA context

Historically, the focus of PSAs has been on modelling of hardware and its impact on the plant safety level. The human component was from the beginning included in the models but was initially treated quite superficially. This was partially due to the level of knowledge and limited availability of relevant data. The first priority of PSAs has been to identify hardware deficiencies. Numerous PSA-based hardware backfits were implemented, frequently resulting in core damage frequency (CDF) reductions and in many cases simultaneous increases of the relative importance of human errors. This pointed to the necessity of upgrading the HRA part of PSA towards higher standards in terms of scope and depth of the analysis. Uses of HRA techniques have matured in the last few years thus allowing HRA to reach a more central status in the current PSAs. This may be attributed to more attention being paid to qualitative analyses of the performance context with regard to key factors such as procedural guidance, recovery opportunities and dependence on preceding human errors; to increased experience in applying the analytical approaches; and to the positive impact of more extensive and efficient review procedures. While the balance between hardware and human performance modelling has been much improved, the state-of-the-art PSAs are still somewhat hardware-centred. A transition to more human-centred PSAs is desirable but is likely to be relatively slow, partially due to some inherent limitations in probabilistic analysis of human performance as well as substantial time lag between advances in human performance research and their implementation in industrial PSAs.

PSA-experience on the risk significance of human interactions

Errors associated with human interactions that occur prior to an initiating event (such as maintenance and testing) have usually not been found among the dominant risk contributors. This includes for example miscalibrations or failures to restore valves to the correct positions after testing and maintenance. The significance of such errors is normally quite low due to their recoverability and the robustness of the plant design. At the same time, some PSAs exhibit a limited explicit modelling of latent errors and reject them on the basis of qualitative arguments. Both nuclear and non-nuclear incidents and accidents illustrate that latent human errors in combination with other human errors and equipment failures, may lead to catastrophic consequences. This indicates a need to pay more attention to latent errors, particularly with regard to the treatment of dependencies, and possibly to reconsider the modelling of this type of human interactions in PSAs.

Human interactions that initiate a scenario (human-induced initiators) are seldom explicitly identified in PSAs and analysed in terms of specific causes. Often experience-based frequencies of initiating events are assumed to reflect these interactions. However, this may not be an adequate representation. Experience shows that human interactions may contribute to both a specific type of initiator (e.g. LOCA – loss of coolant accidents) and the failure of a subsequently required safety function (e.g. safety injection). Such Common Cause Initiators call for explicit modelling of the associated human interactions due to the potential for severe additional degradation of safety.

Most PSAs focus on modelling human actions taken by plant staff after the initiating event. Some of these actions are frequently among the most dominant risk contributors. Since abnormal scenarios occur rarely, experience-based data for this category of interactions are scarce. The current PSAs normally model procedure-driven actions in response to an accident sequence (in the failure space referred to as errors of omission). Apart from a few limited-scope applications, aggravating actions (also referred to as errors of commission) are not systematically treated in industrial PSAs. Methods for their treatment are currently emerging and will be a subject of a separate technical opinion paper. Some approaches do not distinguish between errors of omission and commission when analysing procedure-driven actions but rather address overall failures according to a systemic approach.

Finally, positive operator contributions in terms of recoveries are of high safety importance. Such actions need to be appropriately represented in the human interaction model in order to generate a realistic risk profile for the plant.

Modelling and quantification approaches

Key elements of HRA include:

- identification of human interactions to be considered;
- screening of interactions important to risk;
- task analysis to identify the factors that primarily influence the performance;

- quantification including assignment of probabilities, assessment of uncertainties and investigation of sensitivities; and
- if needed, identification of effective measures to reduce the adverse safety impacts of human performance and to improve prospects for success.

Although numerous HRA quantification techniques have been developed and applied over the years, there does not exist one universally accepted methodology with a firm theoretical basis. Three approaches to quantification can be distinguished: (1) Decomposition or Database Techniques, involving decomposition of tasks to a level for which some reference data are available and can be adjusted according to the specifics of the task; (2) Time Dependent Methods, assuming that human error probability is a function of the time available to respond to an event; (3) Expert Judgement Based Techniques utilising expert knowledge. Most quantification methods used today attempt to approximately account for the effect of Performance Shaping Factors (PSF), i.e. factors influencing human performance. This is complicated by the fact that PSFs are interdependent but the interaction effects are extremely difficult to evaluate. Moreover, the use of PSFs rests on a simplified vision of human behaviour, which relies on defined classes of generic situations whose application for specific cases can be problematic.

Current HRAs frequently employ combinations of several techniques above and demonstrate the benefits of appropriate mixing and matching of these methods.

HRA data

The main sources of data include: internal and external event reports, near-miss reports, violation records, maintenance reports, plant log books, interviews with plant personnel, Handbooks (primarily Swain’s and Guttmann’s HRA Handbook), expert judgement and simulator exercises.

For latent errors associated with regularly performed maintenance and testing activities, plant experience can directly provide relevant information. The availability of data for post-initiating event operator actions is very limited; in this context both qualitative and quantitative information is needed. A combination of simulator studies with expert judgement methods has emerged as an attractive approach to extend the information basis. The usefulness of simulators to support HRA goes much beyond direct generation of human reliability data since simulators remain the only option for observing human performance in a variety of hypothetical scenarios. Given the discrepancy between the conditions for simulator exercises on the one hand and the real demand situations on the other hand, simulator applications require careful interpretation of the observations.

Difficult issues

The main weaknesses of current HRA methods used in industrial PSAs include:

- Limited representation of the cognitive aspects of human performance. While the contextual factors driving execution errors are usually well understood, this applies to a lesser extent to diagnosis and decision errors. This shortcoming concerns both the identification of driving factors in specific performance contexts and the quantification of their impacts. In fact, the limited representation of cognitive aspects of human performance in HRA methods tends to reflect lacking (or insufficiently formalised) knowledge of human behaviour.
- Significant differences in quantitative results from different analysts (using the same method) or from uses of different methods.
- Partially excessive reliance on expert judgement, due to scarcity of empirical human performance data, in particular for serious accident situations.
- Lack of adequate identification, explicit representation, and quantification of actions with potential adverse effects on plant conditions (errors of commission).
- Limited accounting for dependencies among actions.
- No explicit account for the impact of organisational and management aspects; some PSFs may, however, manifest such factors.

The uncertainties associated with human actions, particularly those occurring after an initiating event, are significantly higher in comparison to what is typical for hardware failures.

HRA-based safety insights

In spite of the serious limitations of current HRA methods, within their scope of applicability the HRAs have been highly successful in terms of identifying significant deficiencies related to human performance. These findings are in most cases considered as robust in spite of the normally large numerical uncertainties. Numerous modifications resulting from HRAs include, for example: new procedures, revision of procedures or technical specifications, revised training, installation of additional hardware and operator support systems or automated capabilities, and modifications of systems (including actuation logic).

Outlook

The developments of HRA are driven by the needs of new PSA applications and by the awareness of the limitations of current approaches. The following needs can be identified:

1. In spite of increased maturity of HRA, there are still quite large differences in the implementation of the frequently used methods. Much can be achieved by consequent use of best practices. The current trend towards risk-informed regulation calls for improved homogeneity in the ways the standard methods are applied. Also, HRAs have been focused on full power Level 1 PSA for internal events. Scope extensions should include an improved analysis of human interactions associated with external events and with Level 2 PSA. The latter is particularly important in the context of accident management studies. PSA extensions to cover low power and shutdown modes of operation and uses of PSA to support operational activities (such as maintenance planning, configuration management, surveillance test arrangements) call for a more extensive and truly plant-specific modelling of maintenance and test activities.

2. Recognising the limitations inherent in rare event studies, there have been surprisingly few attempts to validate the HRA methods that are currently widely used. While the limitation of these methods to treat errors of commission is inherent, it is likely that in the medium-term perspective they will continue to be predominantly used in industrial PSAs. For this reason validation within their scope of applicability should be encouraged.

Validation studies may address the accuracy of probability predictions in scenarios for which statistical data are available or variability in the results obtained by different practitioners employing same method. However, it is necessary to be aware of the limitations of a purely statistical validation of a HRA method because contrary to the reproducible systems behaviours, human behaviour is prone to some unforeseeable variations that are extremely difficult to model.

3. The improved treatment of decision-based errors is a major emphasis of recent and current efforts to develop HRA methods. Three main approaches (and combinations of these) can be identified: (a) Methods based on the analysis of operational experience; (b) Simulator-based methods (including decision tree method); and (c) Methods based on cognitive theory (aiming at evaluating not only what errors occur but also why they occur). Since the statistics based on simulator studies and/or operational experience is likely to remain highly limited for the purpose of quantification, all these approaches will still require a significant degree of expert judgement. The qualitative and quantitative validation of cognitive models is a great challenge; validation studies may address the accuracy of predictions of conditions forcing appropriate or inappropriate decisions.

4. Systematic treatment of errors of commission (EoCs) and of dependencies among actions requires consideration of the preceding operator errors, including their detailed causes. EoCs related to "decision" errors, that is, errors in situation assessment (diagnosis) and intention formation as well as in response selection, tend to be most important, particularly within a sequence of preceding decisions and executions. This underlines the need to carry information about decision-based errors in order to properly assess the success of subsequent actions. The knowledge of the full context of an action, in terms not only of the plant state but also of the evolution of the cognitive state of the operators, is necessary. Systematic consideration of detailed error causes extends considerably the complexity of the analysis and is not practically feasible in full scale within the current PSA framework. Nevertheless, some of the approaches mentioned above offer a promising limited-scope treatment of EoCs within the current PSA framework. The development of dynamic approaches, based on different forms of simulation, could support the treatment of EoCs in the longer term.

5. Another line of development addresses the consideration of organisational and management aspects. While some quantification approaches have been proposed, there is currently no consensus within the PSA community whether one should strive for extensive and explicit integration of these aspects within PSA or instead recognise the limitations of PSA in this respect and accept that their comprehensive treatment is not a part of the PSA framework. If integration is preferred, these aspects can be dealt with in one of two ways: adding this dimension to existing models or creating new methods whose theoretical bases directly integrate these aspects.

References

NEA/CSNI (ed.), *Critical Operator Actions – Human Reliability Modelling and Data Issues*, NEA/CSNI/R(98)1, OECD Nuclear Energy Agency, Paris, February 1998.

NEA/CSNI (ed.), *Errors of Commission in Probabilistic Safety Assessment*, Final Task Report of a group of experts of the Working Group on Risk Assessment, OECD Nuclear Energy Agency, NEA/CSNI/R(2000)17, Paris, June 2000.

NEA/CSNI (ed.), "Building the New HRA: Errors of Commission – from Research to Application", OECD/NEA Workshop, Rockville, MD, USA, May 7-9, 2001.

NEA/CSNI (ed.), "Building the New HRA: Strengthening the Link Between Experience and HRA", OECD/NEA Workshop, Munich, 28-30 January 2002.