NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

ERRORS OF COMMISSION IN PROBABILISTIC SAFETY ASSESSMENT

Working Group on Risk Assessment (RISK)
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) and the Republic of Korea (12th December 1996). 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 27 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, 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 2000

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 Ocline: 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 cooperates 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 blv. des Illes
92130 Issy-les-Moulineaux
France
ABSTRACT

This report looks at descriptions of the methods used to analyse errors of commission, descriptions of the findings from the analysis of errors of commission and provides general insights or lessons learned about errors of commission.
FOREWORD

The main mission of the Working Group on Risk Assessment (RISK) 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 considering evolving issues such as human reliability, software reliability, ageing issues, etc., as appropriate.

As a follow-up to CSNI report on Critical Operator Actions [NEA/CSNI/R(98)1] produced by the Working Group task group under Dr. Hirschberg, it was decided to initiate a further task addressing errors of commission. The task group through a series of meetings and discussions has carried out it objective in this report which describes various methods, provides findings from analysis and looks at general insights gained.

The principal characteristic of an error of commission in a PSA context is that its consequence is a state of unavailability of a component, system or function. This is in contrast to an error of omission, which is characterised by a lack of action, and therefore preserves the status quo of a system, component, or function. Thus an important error of commission is recognised by its consequence. In the PSA context, the most significant errors of commission are those that either, in addition to resulting in failure to perform some function, also fail, or made unavailable, other equipment or functions needed to mitigate the accident scenario, or otherwise exacerbate the situation.

This work represents the collective effort of the task group all of whom provided valuable time and considerable knowledge toward its production. In offering it thanks to these experts, the NEA Secretariat wishes to express to provide particular appreciation to Ms. Ann Ramey-Smith, U.S. Nuclear Regulatory Commission, who as task leader adroitly chaired the many meetings and provided overall co-ordination towards completing the report.

The Task Group members contributing to this report were:

Anna Grant (Canada)  Atilla Bareith (Hungary)  Bernhard Reer (Switzerland)
Jaroslav Holy (Czech Republic)  Sándor Czakó(Hungary)  Patrik Meyer (Switzerland)
Pekka Pyy (Finland)  Előd Hollo (Hungary)  David Hamblen (United Kingdom)
Reino Virolainen (Finland)  Mamoru Fukuda (Japan)  Jeremy Williams (United Kingdom)
Genevieve Baumont (France)  Ken Muramatsu (Japan)  Mark Cunningham (United States)
Jeanne-Marie Lanore (France)  Gerben Heslinga (The Netherlands)  Joseph Murphy (United States)
Pierre Le Bot (France)  Magiel F. Versteeg (The Netherlands)  Mark Rubin (United States)
K. Muramatsu (Japan)  Javier Yllera (Spain)  Ann Ramey-Smith (United States)
Johannes Mertens (Germany)  Bo Liwång (Sweden)  
Oliver Sträter (Germany)  Stefan Hirschberg (Switzerland)  

5
# TABLE OF CONTENTS

Abstract ................................................................................................................. 4

Foreword .................................................................................................................. 5

1. Introduction ......................................................................................................... 7
   A. Errors of Commission .................................................................................. 7
   B. Objectives of Task 97-2 ........................................................................... 7
   C. Approach ..................................................................................................... 8
   D. Organisation of Report ............................................................................... 8

2. Analysis Methods ............................................................................................... 9
   A. Summary Discussion of Analysis Methods .................................................. 9
   B. Questionnaire Response ............................................................................. 9

3. Conclusions and Recommendations .................................................................. 21
   A. Conclusions ............................................................................................... 21
   B. Recommendations for Future Development ............................................... 22

4. Key References .................................................................................................. 27

Appendix A. Attendees at Task 97-2 meetings ...................................................... 31

Appendix B. Questionnaire .................................................................................... 35

Appendix C. Contributions from Participating Countries ....................................... 37
   Czech Republic ............................................................................................... 39
   Finland ............................................................................................................. 57
   France (IPSN) ............................................................................................... 71
   France (EDF) ............................................................................................... 75
   Germany ......................................................................................................... 85
   Hungary ......................................................................................................... 131
   Japan ............................................................................................................. 147
   Switzerland .................................................................................................... 157
   The Netherlands (KEMA) ............................................................................ 177
   The Netherlands (SAVE) ............................................................................. 187
   United Kingdom ............................................................................................. 237
   United States ................................................................................................. 255
Chapter 1. Introduction

A. Errors of Commission

In February 1998 the report of an earlier task of Principal Working Group 5 (PWG-5), Task 94-1, was published. In many ways, the present effort of Task 97-2 was shaped by the human reliability modeling and data issues that were articulated in that report. That report, entitled "Critical Operator Actions - Human Reliability Modeling and Data Issues" [NEA/CSNI/R(98)1], discusses the definition of errors of commission.

One of the major criticisms of current PSAs is that they do not adequately address an important class of human system interactions, namely inappropriate actions, particularly those that might occur during the response to a transient or an accident, that place the plant in a situation of higher risk. This class of inappropriate actions is often referred to as errors of commission... The principal characteristic of an error of commission in a PSA context is that its consequence is a state of unavailability of a component, system or function. This is in contrast to an error of omission, which is characterized by a lack of action, and therefore preserves the status quo of a system, component, or function. Thus an important error of commission is recognized by its consequence. In the PSA context, the most significant errors of commission are those that either, in addition to resulting in failure to perform some function, also fail, or made unavailable, other equipment or functions needed to mitigate the accident scenario, or otherwise exacerbate the situation. Such an error introduces a dependency between events within a fault tree, or between functions on the event tree. However, an error of commission that fails a single function or system (e.g., by premature termination) can also be significant from a risk assessment perspective, if it provides a new mechanism of failure that cannot reasonably be expected to be included in the failure probability assigned for the function/system. This latter type of error does not introduce a new dependency between the events of the model, but increases the failure probability of the affected function... The modeling of errors of commission has historically been ruled as being out of scope in PSAs, probably because of a fear that including all possible errors of commission might lead to an increase in the size of PRA models to such an extent as to make their solution impossible. However, recent progress in understanding the causes of human error has indicated the possibility of developing approaches to deal with this problem in a rational and economical way (p 142-143).

With this perspective in mind, it was agreed that PWG-5 would initiate a human reliability task that would address errors of commission. Thus, Task 97-2 on errors of commission in PSA began its work.

B. Objectives of Task 97-2

During the September 25, 1997 meeting of PWG-5, Task 97-2, consensus was reached on the goals of the task. Three general goals were identified: (1) to develop insights on errors of commission; (2) to apply methods for the quantitative and non-quantitative analysis of errors of commission; and (3) to identify data needs. It was agreed that those countries participating in the task would select an analysis method of their own choice and apply that method in the analysis of one or more events or cases, also of their own choice. The intent was to permit the maximum freedom to choose among
methods that may be under development and to choose events or cases of highest interest to the analyst. The findings from these analyses would then be shared to permit the development of insights on errors of commission. It was agreed that the product of Task 97-2 would be a report that generally contains three parts: (1) descriptions of the methods used to analyze errors of commission; (2) descriptions of the findings from the analyses of errors of commission; and (3) general insights or lessons learned about errors of commission. This report documents the products of the activities undertaken as part of Task 97-2.

C. **Approach**

A consensus was reached to undertake a number of specific tasks to fulfill the goals of the task. These include the following:

1. The first task was for each participant to select an analysis approach as well as one or more operating events (for retrospective analysis) or one or more accident scenarios (for prospective analysis) that had been or would be analyzed. These would form the basis of each participant’s input.
2. The second task was to provide written input to the Task 97-2 report. A questionnaire was used to solicit input is provided in Appendix B of this report.
3. Working meetings were conducted to exchange detailed comments on the report and to reach a consensus on conclusions.

One future activity of Task 97-2 is to conduct a workshop, tentatively scheduled for Fall 2000, on errors of commission, methods for their analysis, and data needs. The results of that workshop will be documented in a separate report.

D. **Organization of Report**

Chapter 2 of this report contains a brief introduction and an overview table that summarizes the methods that were used to analyze errors of commission. Chapter 3 provides some general insights regarding errors of commission and summarizes the findings from the participants’ analyses. Suggestions for future development are provided in the form of questions, many of which may be addressed in the upcoming workshop on errors of commission. Chapter 4 provides a listing of some key references for additional reading about errors of commission and human reliability analysis methods. Appendix A lists the names and addresses of attendees of Task 97-2 meetings. Appendix B contains the questionnaire that was used to guide written input to the report. Lastly, the contribution from each participating country is presented in Appendix C.
Chapter 2. Analysis Methods

A. Summary Discussion of Analysis Methods

The participants in Task 97-2 engaged in much discussion regarding what analysis method to use to investigate errors of commission. One approach considered was to conduct a bench-marking exercise. Such an approach would have resulted in a comparison of various methods for analyzing errors of commission. This approach was rejected for several reasons, including: (1) the next-generation HRA methods which participants wanted to use in the Task were in various stages of development and final documentation of these methods was not yet available; (2) such an approach would inordinately put the emphasis on methods comparison rather than on improving the understanding of errors of commission; and (3) information about a base case could not be made available to the level of detail needed to support analysis. It was decided, therefore, to allow participants to use whatever method they chose to analyze whatever event or scenario containing an EOC that was interest to them. The results of these analyses are included in this report.

The Task participants decided early in the effort to share information about their methods that, in many cases, were still developmental. The consensus was reached to allow a forum to "showcase" these new, evolving methods, rather than to subject them to any formal critique. This approach proved to be an excellent one because the participants became willing to engage in open and free discussion and debate about the methods and errors of commission, and resulted in both an improved understanding of errors of commission and improvement in the methods themselves.

Table 2.1 provides a summary description of the methods that were applied by Task 97-2 participants in studying EOCs. Appendix C presents more detailed descriptions of the analyses conducted (including descriptions of the method employed) by each participant country in response to a questionnaire.

B. Questionnaire Response

The participants in Task 97-2 provided information in response to a questionnaire designed to elicit information about analysis methods and errors of commission. These responses are provided in Appendix C. While not all participant countries and interested organizations provided questionnaire responses, their participation in discussions and reviews was nevertheless very helpful and is most appreciated.
<table>
<thead>
<tr>
<th>Analysis Method: ATHEANA (USA)</th>
<th>Analysis Method: ATHEANA (applied by Japan)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Underlying Concepts</strong></td>
<td><strong>Underlying Concepts</strong></td>
</tr>
<tr>
<td>Refer to NUREG-1624, May 1998, and NUREG-1624, Revision 1, Spring 2000. Also summarized in Appendix C of this report.</td>
<td>Refer to NUREG-1624, May 1998</td>
</tr>
<tr>
<td><strong>Steps and Procedures</strong></td>
<td><strong>Steps and Procedures</strong></td>
</tr>
<tr>
<td>1. Characterize the standard safety analysis and parameter conditions</td>
<td>1. HFE-identification is not always systematic</td>
</tr>
<tr>
<td>2. Identify deviations (physics, equipment failures)</td>
<td>2. Identification of mental factors as EFC is difficult.</td>
</tr>
<tr>
<td>3. Identify the mismatch between PSFs and scenarios</td>
<td>3. Quantification for probabilities P (UA/EFC) and P (recovery/UA/EFC) is not clear</td>
</tr>
<tr>
<td>4. Assess error mechanisms and strength of EFC</td>
<td>4. Retrospective analysis using ATHEANA is needed to learn how to identify mental factors as EFC.</td>
</tr>
<tr>
<td>5. Quantify</td>
<td>5. Simulator experiments are also useful to solve the above problem.</td>
</tr>
<tr>
<td><strong>Lessons learned</strong></td>
<td><strong>Lessons learned</strong></td>
</tr>
<tr>
<td>1. HFE-identification is difficult</td>
<td>1. HFE-identification is not always systematic</td>
</tr>
<tr>
<td>2. HFE-identification is not systematic</td>
<td>2. Identification of mental factors as EFC is difficult.</td>
</tr>
<tr>
<td>3. Guidance was unclear about the relationship between EM UA s and EFCs</td>
<td>3. Quantification for probabilities P (UA/EFC) and P (recovery/UA/EFC) is not clear</td>
</tr>
<tr>
<td>4. Difficulties to identify HFEs not associated with indication failures</td>
<td>4. Retrospective analysis using ATHEANA is needed to learn how to identify mental factors as EFC.</td>
</tr>
<tr>
<td>5. Resource intensive</td>
<td>5. Simulator experiments are also useful to solve the above problem.</td>
</tr>
<tr>
<td>6. Use of retrospective analysis for prospective analysis was unclear</td>
<td><strong>Application of Method</strong></td>
</tr>
<tr>
<td>Retrospectively: several events investigated</td>
<td>Retrospective application: Application to Davis-Besse event is underway.</td>
</tr>
<tr>
<td>Prospectively: several event sequences</td>
<td>Prospective application: Application for SGTR of Japanese 1100 Mwe PWR level 1 PSA is underway.</td>
</tr>
<tr>
<td>Underlying Concepts</td>
<td>Steps and Procedures</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Described in:</td>
<td>(NUREG-1642, Draft for Comment, May 1998)</td>
</tr>
<tr>
<td>NUREG-1624, May 1998</td>
<td>1. HFE identification</td>
</tr>
<tr>
<td>NUREG/CR-6093</td>
<td>2. UA identification</td>
</tr>
<tr>
<td>NUREG/CR-6265</td>
<td>3. EFC identification</td>
</tr>
<tr>
<td>NUREG/CR-6350</td>
<td>4. Quantification</td>
</tr>
<tr>
<td></td>
<td>(NUREG-1642, Draft for Comment, May 1998)</td>
</tr>
<tr>
<td>Underlying Concepts</td>
<td>Steps and Procedures</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>The approach taken in the full power study is based on the cause-effect mapping concept which relates the impact of a set of identifiable influencing factors on possible forms of error without specifying the exact mechanism of the influence. In all cases, however, the connection between the influencing factor and the mode of error is intuitive, obvious, or supported by operating experience, human factors research, or on literature on cognitive science. Error expressions in the response phase were classified into 3 types: (1) global misdiagnosis – selection of an incorrect procedure. The potential for mindset leading to a failure of the recovery action is an important factor in the assessment. (2) local misdiagnosis – a commission error at the level of an interaction with a system (e.g., incorrectly disabling a piece of equipment). (3) slip – unintentional EOC. Factors related to control panel layout.</td>
<td>1. Identification of the human system interaction that provides opportunities for errors to occur. The interaction may be a response to an unexpected change in plant condition or an essential part of a specific evolution. Such activities may lead to errors whose impact is immediately revealed or to errors that have latent effects (e.g., due to test or calibration activities) and only show up in transient conditions or as equipment malfunction in the shut-down mode. 2. Identification of the failure modes of function. Possible opportunities for errors and their impact on the plant can be obtained from an understanding of the activity and the context within which it is taking place. Operation and maintenance activities have systematically been reviewed. Post-accident activities have been categorized into cognitive responses (global and local misdiagnosis) and executions for which the proactive and systematic HAZOP style was followed regarding “what if” questions.</td>
</tr>
</tbody>
</table>
## Analysis Method: Borssele PSA (The Netherlands)

<table>
<thead>
<tr>
<th>Underlying Concepts</th>
<th>Steps and Procedures</th>
<th>Lessons learned</th>
<th>Application of Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>related to control panel layout play an important role in the assessment.</td>
<td>3. Identification of the most significant error expressions. Screening was done on possible consequences, on likelihood, and by identifying recovery mechanisms. Due to the nature of the shut-down analysis itself, an initial screening on consequence is performed during the search for error expression. The error expressions identified are those that either result in an initiating event, or have a significant impact on the accident development or mitigation. Screening on likelihood is done by successfully identifying possible modes of error, and then searching for possible causes of the errors. The causes were expressed in terms of influencing factors for which the number and character were different in the power mode analysis and the non-power mode analysis.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Analysis Method: CAHR (Germany)

<table>
<thead>
<tr>
<th>Underlying Concepts</th>
<th>Steps and Procedures</th>
<th>Lessons learned</th>
<th>Application of Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Man-machine system including ergonomic, cognitive and explicit representation of communication. Strict distinction between observations, error classification, and cause attribution. Representation of all dependencies between observations, errors, and causes. Quantification by psychological scaling method established outside of HRA within the psychological literature. Quantification relies on two basic aspects: cognitive abilities and situational conditions, under which the abilities have to be used. All statements derived by the method can be traced back to the basis information (events). E.g., dependencies, recoveries, or organizational aspects can be traced back. Free text descriptions allowed as opposed to narrow taxonomy.</td>
<td>Retrospective 1) Event decomposition 2) Holistic analysis 3) Detailed analysis Prospective 1) Define situation of interest (not necessarily from PSA) 2) Define data base query 3) Build number of observations 4) Build number of errors 5) Build relative frequency of errors in situation 6) HEP estimate by Rasch model</td>
<td>Inter-rater reliability for development of data base queries not yet measured Quality of event descriptions must be improved through the use of a multidisciplinary team and improved data from the plant Currently high level of expertise required to apply method. Improved event analysis application currently under development. Inter-rater reliability study for event analysis quality currently in progress. Method needs search scheme for errors of commission (under development in concert with CODA) Psychological scaling model has analogies to other established logic models and mathematics Limited practical guidance available in the moment.</td>
<td>Retrospective application 1) Base study with 165 BWR events 2) 2nd study with 55 PWR events 3) Detailed application to Davis-Besse event 4) Application to aircraft events planned Prospective application 1) Assessment of accident management measure for a BWR 2) Assessment of selected actions during low power and shutdown for BWR 3) Precursor type analysis for Davis Besse (EOOs and EOCs) 4) Used as support to generate a qualitative behavioural model for EOCs</td>
</tr>
<tr>
<td>Underlying Concepts</td>
<td>Steps and Procedures</td>
<td>Lessons learned</td>
<td>Application of Method</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Action-centered error description: (1) The context determines whether a given action is appropriate; (2) Action characteristics provide perspectives on error-producing conditions (EPCs). Explaining errors by cognitive tendencies (CTs): typical practices and attitudes in human performance may be inappropriate under adverse contexts. Preventing errors by hazard cognition.</td>
<td>1. Compile a summary of the context of occurrences. 2. List the critical actions. 3. Identify action characteristics and performance conditions. 4. Derive improvements with emphasis on cognitive tendencies. 5. Verify the results.</td>
<td>Method user requirements: expertise in (1) PSA and (2) behavioral sciences. EOCs can be assessed by the same taxonomy as EOOs. Illustration by incidents should be extended (11 incidents were evaluated).</td>
<td>Applied to operating events. Predictive: analysis of one PSA sequence (1999). Three main analysis features: (1) action-centered EOC search (i.e., looking for scenarios where a given action is inappropriate; (2) using CTs for structured EPC identification; (3) using EPCs as an orientation for adapting THERP HEPs adapting THERP HEPs.</td>
</tr>
<tr>
<td>Underlying Concepts</td>
<td>Steps and Procedures</td>
<td>Lessons learned</td>
<td>Application of Method</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Does not assume a PSA model (but uses one if available)</td>
<td>Select human actions to be analyzed</td>
<td>No cognitive modeling in the scope; rather focus</td>
<td>No application yet; one planned</td>
</tr>
<tr>
<td>General approach not only focusing on EOCs</td>
<td>Identify potential COs</td>
<td>on observable team actions</td>
<td></td>
</tr>
<tr>
<td>Consistency between qualitative and quantitative analysis</td>
<td>Screen unimportant COs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traceability of quantification from qualitative analysis</td>
<td>Model the important COs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flexibility of underlying data – 3 different quantification approaches</td>
<td>Assess probability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PICs (probability increasing context – PSFs)</td>
<td>Explicit modeling of recovery</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Analysis Method: French PSA (France, IPSN)

<table>
<thead>
<tr>
<th>Underlying Concepts</th>
<th>Steps and Procedures</th>
<th>Lessons learned</th>
<th>Application of Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator experiments (directly, building statistical models) used to identify and quantify EOCs</td>
<td>Identification based on PSA analysis (key functions, operator actions); analysis of simulator data is also part of identification process</td>
<td>Direct quantification from simulator results without analysis supports PSA but not plant improvement / discussion of results.</td>
<td>900 MW and 1300 MW PWRs full power and shut down</td>
</tr>
<tr>
<td>Models used that include diagnosis curves and PSFs for both EOOs and EOCs</td>
<td>Qualitative analysis using PSFs for non-observed actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit of analysis includes explicitly recovery by safety engineer</td>
<td>Detailed analysis of dependencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplistic inclusion of emergency team</td>
<td>Quantification using adapted THERP when no statistical / simulator-data is available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Underlying Concepts</td>
<td>Steps and Procedures</td>
<td>Lessons learned</td>
<td>Application of Method</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>No EOC definition or use. System analysis perspective for which the emergency operating system is the unit of analysis. Operation is explained by CICAs (Configuration and reading of situation, subsumes procedures, operators and control capabilities and their combination) Assumes a rational operator No error taxonomy SFP= scenario failure probability of scenario happens given some CICAs Recovery not modeled separately</td>
<td>Identification and definition of the Human Factor mission through functional analysis from the PSA Breakdown requirement for Strategy Diagnosis Situation / Action Analysts think out failure scenarios for Strategy Diagnosis Action Analysts quantify each scenarios condition Verify consistency and integrate HF mission analysis into event tree</td>
<td>Analyst has to find all conditions that are relevant for CICAs. Analyst's expertise is the main issue. Collective experts' work is better.</td>
<td>Currently applied to N4 PSA</td>
</tr>
<tr>
<td><strong>Analysis Method:</strong> Paks nuclear power plant HRA in low power &amp; shutdown PSA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td><strong>Underlying Concepts</strong></td>
<td><strong>Steps and Procedures</strong></td>
<td><strong>Lessons learned</strong></td>
<td><strong>Application of Method</strong></td>
</tr>
<tr>
<td>Approach not limited to EOCs (more general)</td>
<td>1. Identify potential errors through an integrated analysis of human actions, systems, and processes</td>
<td>No mechanistic application of EOC and EOO categories</td>
<td>Low Power and Shutdown PSA for NPP Paks</td>
</tr>
<tr>
<td>Attempt to take an account of contextual conditions as represented by performance influences</td>
<td>2. Develop an understanding and description of contextual conditions for human-system interactions, qualitative evaluation</td>
<td>Transparent and credible description of contextual conditions is difficult</td>
<td>Review and analysis of inadvertent primary circuit dilution faults for VVER reactors</td>
</tr>
<tr>
<td>Use of a decision tree concept</td>
<td>3. Model human-system interactions by the use of a decision tree</td>
<td>Formal approaches to quantification methods can be tailored to specific needs relatively easily (integration with the decision tree concept), but &quot;validation&quot; of estimates is still an open issue</td>
<td></td>
</tr>
<tr>
<td>A holistic approach (as opposed to a very fine decomposition of human actions)</td>
<td>4. Quantify error probability (return to previous steps, if needed)</td>
<td>Need to better relate to plant experience through the use of feedback from retrospective analysis</td>
<td></td>
</tr>
<tr>
<td>Analysis Method: SHARP (applied by the Czech Republic)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Underlying Concepts</td>
<td>Steps and Procedures</td>
<td>Lessons learned</td>
<td>Application of Method</td>
</tr>
<tr>
<td>Refer to “Systematic Human Action Reliability Procedure (SHARP)”, Palo Alto: Electric Power Research Institute, June 1984</td>
<td>1. Identification 2. Screening 3. Qualitative analysis 4. Formal representation 5. Integration into PSA model 6. Quantification</td>
<td>Classic framework for HRA Doesn’t specify quantification method For post-accident errors, decision tree method provided insights, was helpful for errors in information processing; ASEP for errors in execution; THERP for pre-accident errors EOCs leading to initiating event was quantified using THERP. Application does not ensure complete identification of EOCs Simulator data was found as helpful to support HRA.</td>
<td>PSA Level 1, ShutDown-PSA for two plants in Czech-Republic For EOCs, man-induced LOCA</td>
</tr>
</tbody>
</table>
Chapter 3. Conclusions and Recommendations

Many insights into errors of commission (EOCs) were derived from the activities of Task 97-2. Some of these observations are listed below. Table 3.1 provides a summary of findings concerning errors of commission for the various analysis methods applied. While there are differences in findings, some general conclusions about errors of commissions can be reached.

A. Conclusions

A distinction can be made between two kinds of human errors: (1) predicted ones that were considered in the design so that defenses against the error are put in place during the design phase; and (2) those errors that were not predicted in the design phase. The challenge is to predict performance failures that were not accounted for in the design, many of which are EOCs. More specifically, there are two types of EOCs: a) those seen in simulator exercises and in operational events b) those that have not been identified and that may have a high consequence. It is recognized that PSAs do include EOCs that were suggested by operating experience, simulator studies, and searches of normal and emergency operating procedures. EOCs have not been included, however, in a systematic and comprehensive manner. General conclusions are provided below.

Conclusions Regarding Methods to Study EOCs

- Rational identification of EOCs is difficult.
- The structure of current PSA (i.e., event trees and fault trees) may be too fixed for a real analysis of EOCs.
- The slip/mistake distinction is not very helpful for understanding EOCs.
- Although it may be helpful in identification, the distinction between EOCs and EOOs may not be useful from the point of view of analysis.
- Cognitive dissonance may be a useful psychological concept for the analysis of EOCs.
- Quantification procedures must take into account that EOCs have multiple contributors that are interrelated. The applicability of very simple quantification models to the quantification of EOCs is not straightforward.

Plant Procedures

- Procedures are correct for an analyzed case (nominal). It is impossible to address all the conditions in procedures, which may lead to right or wrong operator priorities.
- Crew performance is in most cases a function of procedure adequacy for the situation rather than a function of transient difficulty per se.
- A strong mismatch between the situation, procedure, and training does not necessarily lead to a higher error probability; that is, there is no clear linear relationship. A small mismatch can cause high probability errors.
- Errors in procedure transfer will increase the likelihood of EOCs, as will errors in interpreting if-then logic statements. When more than one logic statement is included in a procedure step, the likelihood of human errors is increased.
Plant Contexts

- Plant modifications can cause subtle interactions and dependencies between systems that can become vulnerable to single human errors.
- A mismatch between plant conditions and PSFs increases the likelihood of EOCs.
- Traditional PSFs such as ergonomics, communications (fuzzy statements), double negations in procedures, tool problems etc. have been implicated in errors.
- A mismatch between expected and actually available time may lead to EOCs.

Consequences

- Many EOCs have harmless consequences and need not to be modeled in PSAs.
- Some EOCs are significant to PSA because they introduce new accident sequences, dependencies and failure modes.
- It is unclear whether there is a difference in recovery likelihood between EOCs and errors of omission.

B. Recommendations for Future Development

Task 97-2 activities have resulted in the following recommendation for future development:

1. To more realistically model human behavior in PSA, there is a need to better understand how operators actually work. There needs to be a move toward human-centered analysis to support human reliability analysis (HRA) rather than an equipment-centered analysis. Such a shift may result in new event trees and accident sequences.
2. Regarding quantification, it would be most helpful to establish a database that includes the qualitative aspects of EOCs. Such a database would identify EOC-specific performance shaping factors. Be clear that such an HRA database would not simply provide estimates of human error probabilities. Rather, what is needed to support quantification is a better understanding of how to identify and analyze EOCs.
3. There is no clear consensus yet on the best means to quantify the conditional human error probability given an error forcing context or an error opportunity. Additional work in improving knowledge to support quantification is needed.
4. Guidance would be helpful for standardizing the documentation of error opportunities/error forcing contexts.
5. The role of traditional task analysis in the identification and analysis of EOCs is unclear. Guidance in this area would be helpful.
6. The behavioral sciences have information to offer to understand the resolution of conflicts between alternative choices in decision making. HRA methods should continue to incorporate knowledge from the behavioral sciences to support human error identification, analysis, and quantification.
7. HRA methods development should continue to improve guidance and procedures for identifying likely EOC opportunities and for screening important EOCs.
Table 3.1 Findings Concerning Operator Performance and Errors of Commission

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Summary of findings from analyses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATHEANA (USA)</td>
<td>A retrospective analysis of operating events indicated that the mismatch between plant conditions and assumptions of the procedures and training and other PSFs is an important contributor to non-random human errors. Some contributors to errors (including errors in recovery) discovered through retrospective analysis include:</td>
</tr>
<tr>
<td></td>
<td>1. limited available time to complete task or recover error</td>
</tr>
<tr>
<td></td>
<td>2. unfamiliarity with task (e.g., first time that drain-down to mid-loop had taken place)</td>
</tr>
<tr>
<td></td>
<td>3. unfamiliarity with use of instrumentation</td>
</tr>
<tr>
<td></td>
<td>4. task conflicts (e.g., The shift technical advisor must fill out state paperwork during events but also remain cognizant of plant state and operations.)</td>
</tr>
<tr>
<td></td>
<td>5. poor human factors design (e.g., instrumentation placed on back panels)</td>
</tr>
<tr>
<td></td>
<td>6. complicated plant state (e.g., in Ft. Calhoun example, false fire alarms, air compressor lost, minor flooding)</td>
</tr>
<tr>
<td>ATHEANA (as applied by Japan)</td>
<td>1. A trial application of ATHEANA for level 1 PSA (1998), taking steam generator tube rupture as an example, indicated that the identification of human failure events (HFEs) to be analyzed in level 1 PSA and the identification of mental factors as error forcing context (EFC) are not always clear in NUREG-1624 Draft for Comment, May 1998. Therefore, NUPEC continues the trial application using NUREG-1624 final report from the viewpoints of HFE screening process and identification of mental-related EFC.</td>
</tr>
<tr>
<td></td>
<td>2. In parallel with the trial application, in order to grasp how mental factors should be treated as EFC in ATHEANA, NUPEC makes event analysis on Davis-Besse accident using ATHEANA, where feed and bleed operation was bypassed and the recovery of AFWS was given priority.</td>
</tr>
<tr>
<td></td>
<td>3. Apart from the above prospective analyses, NUPEC has experimentally investigated elements and factors of EFC, where performance shaping factors (PSFs) including mental factors were taken into account as EFC as well as plant conditions. Examples of PSF elements identified are operating procedures, practices/rules, mental workload and so on. EFC coping factors, such as team skill dimensions and indirect supportive information, are also investigated as an important EFC element.</td>
</tr>
<tr>
<td>ATHEANA (as applied by The Netherlands)</td>
<td>Applied ATHEANA (1998) in a retrospective way to assess an incident that took place in a chemical plant. More than one EOC and EOP was analyzed. Dependencies among several underlying causes were observed. These inter-related underlying causes were:</td>
</tr>
<tr>
<td></td>
<td>1. Aspects related to safety culture (i.e., operators were not expected to ask questions.)</td>
</tr>
</tbody>
</table>
|   | 2. Insufficient training (i.e., operators did not know the possible consequences of off-specification conditions.)  
3. Aspects related to quality assurance (i.e., no well-defined instructions including no well-defined instructions for checking for bade lay-out of procedures.)  
4. Biases (i.e., a bias was observed that operators got used to a certain pattern.)  
5. Slips and misunderstanding in communications. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CAHR (Germany)</td>
<td>The slip-mistake distinction was not very helpful for error of commission discussions. Likewise, skill-rule-knowledge taxonomy in isolation is not a good predictor of behavior. However, cognitive dissonance is a useful concept. Stronger event signatures with clear event indication (from the operator’s perspective) are responded to differently than weaker signatures with less clear indication. The stronger the mismatch between the situation and what is in the mind of the operators via training and their procedures does not directly result in higher probability for error. There is not a linear relationship. Occasionally, smaller mismatches can cause higher error probabilities. Misunderstandings in communications are one of the major sources of commission errors. Regarding latent factors, workers may not care or be aware of some issues regarding configuration. For example, they may believe that trains are not cross-tied, which while true during normal operations is not the case in low power situations.</td>
</tr>
</tbody>
</table>
| CODA (Switzerland) | Various EPCs were identified, e.g., 19 different EPCs for the Davis Besse (1985) incident. Three main groups of EPCs:  
1) Dynamic features implied by the scenario, e.g., fast change of system parameters  
2) Interface features, e.g., important indication on back panel  
3) Preceding human performance, e.g., initiation of a recovery action Cognitive tendencies were useful for identifying EPCs. Exposure time seems to be a basic contributor in the sense of a boundary condition. Correlation hypothesis: the longer the time when an opportunity for the error persists, the higher the error likelihood. Many EOCs have minor consequences. It is important to point to errors that are precursors of severe consequences. Two recovery constraints in the sense of boundary conditions include hardware and time needed for error correction. Caution should be taken before assuming that slips are more likely to be recovered than mistakes. Slips should be considered in terms of dependency and likelihood of multiple failures. This is why slips are more or less important. |
**FACE (Finland)**

For maintenance data, there are many commission errors that only result in omission of a system function. This is for simple as well as dependent failures.

It may be failure events may not be the fault of instrument technicians but are the result of other maintenance activities.

---

**French PSA (France IPSN)**

Procedures are correct for (match) the nominal case. It is impossible to write all conditions into procedures (to make them absolutely complete). Several strategies exist to solve the same safety function.

Some contributors to errors:
- Plant conditions are not what is expected
- Conflict of priorities; operator priorities are sometimes correct and sometimes are not depending upon plant conditions.
- Mismatch between available time and perceived time; i.e., crews vary in whether they respond quickly or slowly to the event (e.g., how much checking is performed, how many phone calls are made). This is true for omission as well as commission errors.
- Misinterpretation of the procedure source.

Two types of EOCS:
1) those noted from simulator runs
2) those that have been imagined only but are of high consequence

Many errors of commission are not interesting. Functional analysis is the starting point for determining interesting EOCS. Collecting operating experience is also important and should be used to support the analysis by suggesting the ways that errors of commission happen.

---

**MERMOS (France EDF)**

Assumptions: No distinction between omission and commission errors. Individual errors are taken into account as they could create a situation that could lead to a mismatch between operation system (crew + interface + procedures) and safety requirements (= failure).

**Individual errors**
- procedures tests – double negations and two logical statements embedded led to wrong answers on a test
- tunnel effects with conjectured procedures lead to failure to anticipate
- spurious signal resulted in lost time

**Failure (operation system error)**
- mismatch between operator’s culture and designer’s culture led to operation system not working
- insufficient emergency culture makes it impossible for the operation system to read the situation (e.g., TMI2) or leads to no recovery of design failure
- team organization deficiencies result in no orientation for the operation
| **Paks HRA in LP&S PSA (Hungary)** | Within the low power and shutdown PSA for the Paks NPP, five generic mechanisms have been identified by which water of low boron concentration can be added into the primary circuit (and the core). Some of these mechanisms can develop as a result of inappropriate human actions (including errors of commission); others are equipment failures.

An examination of operational events revealed 13 events that were of interest from the point of view of the dilution phenomenon. These events were mostly precursors to a dilution fault. The event reports analyzed were not sufficiently detailed with respect to the HRA needs (cause analysis, evaluation of contextual conditions). Expert opinion was needed to identify underlying human related causes of dilution faults.

After a formal screening analysis 21 dilution scenarios were selected for refined quantification. These scenarios involved 11 different operator errors: 9 of them were errors of commission and 2 errors of omission.

Recoveries were found important and feasible in a number of cases, but difficult to quantify.

Initiatives have been made to improve the analysis methods used with emphasis on further analysis of plant experience for the purpose of providing data and insights for both qualitative and quantitative error analysis. |

| **SHARP (applied by Czech Republic)** | Analysis sessions were conducted as part of requalification training. When random errors occurred, causes of errors were classified. The project initially was for HRA, but the scope was enlarged to include helping to validate procedures.

Simulation exercises appeared more valuable than pure SHARP exercise. Both EOOs and EOCs were seen during simulator exercises. In fact, EOCs were more plentiful than omissions (of 29 documented errors, 20 were classified as EOCs.)

**Influences on operator performance:**

1. Procedures allow for non-nominal conditions; critical safety function approach to maintaining the plant
2. Communications related to 35% of errors.
3. Insufficient parameter specificity, i.e., what does it mean that "parameter is either increasing or stable"?
4. Procedure steps containing double negation posed problems for all crews.
5. False signals will lead to EOC – 5 out of 6 crews were unable to determine that an SFAS signal received was incorrect.
6. Errors in procedure transfer will ensure the occurrence of an EOC.
7. Errors in interpreting whether parameter criteria have been met can be caused by communication failures.
8. Errors in interpreting “If, then” logic statements lead to commission errors.

The hypothesis that stress from failure would influence additional failures was unsubstantiated by the data. To some extent the crew was unaware that they had committed an error. |
Chapter 4. Key References

The following references are recommended reading because they cover much of the breadth of thinking about errors of commission and related topics over the past several years. This list is not exhaustive, but rather provides a sample of some of the key references. The reader is referred to the questionnaire responses provided in Appendix C for a more complete set of references.

Key References


### Appendix A. Attendees at Task 97-2 Meetings

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization/Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Muramatsu</td>
<td>JAERI, Tokai-Mura, Naka-Gun, Ibaraki-Ken 319-11, Japan</td>
</tr>
<tr>
<td>Jeremy Williams</td>
<td>HM Principal Inspector, Nuclear Safety Directorate, St. Peter's House, Balliol Road, Bootle, Merseyside L20 3LZ, United Kingdom</td>
</tr>
<tr>
<td>Tavier Ylera</td>
<td>PSA Specialist, Consejo de Seguridad Nuclear (CSN), Justo Dorado 11, E-28224 Madrid, Spain</td>
</tr>
<tr>
<td>Mark Rubin</td>
<td>PSA Branch, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, USA</td>
</tr>
<tr>
<td>Csuha Sandor</td>
<td>Psychologist, Nuclear Power Station, Paks, Hungary</td>
</tr>
<tr>
<td>Jaroslav Holy</td>
<td>Data and HRA Specialist, Department of Risk &amp; Reliability Analysis, NRI Rez, 25068 Rez, Czech Republic</td>
</tr>
<tr>
<td>Reino Virolainen</td>
<td>Chief Inspector, STUK-Radiation &amp; Nuclear Safety Authority, P. O. Box 14, FIN-00881, Helsinki, Finland</td>
</tr>
<tr>
<td>Elod Hollo</td>
<td>Director of Nuclear Engineering Division, VEIKI Institute for Electric Power Research, Gellerthegy U. 17, Budapest, H-1016, Hungary</td>
</tr>
<tr>
<td>Bernhard Reer</td>
<td>Safety Engineer, Paul Scherrer Institut, CH-5233 Villigen PSI, Switzerland</td>
</tr>
<tr>
<td>Gerben Heslinga</td>
<td>Senior Consultant, KEMA Connect, Utrechtseweg 310, NL-6800 ET ARNHEM, The Netherlands</td>
</tr>
<tr>
<td>Patrick Meyer</td>
<td>Acting Section Head PSA, Swiss Federal Nuclear Safety Inspectorate (HSK), CH-5232 Villigen - HSK, Japan</td>
</tr>
<tr>
<td>Mamoru Fukuda</td>
<td>Senior Engineer, NUPEC, Fujita Kanko Toranomon Bldg, 7F, 17-1, 3-chome Toranomon, Minatoku, Tokyo, Japan</td>
</tr>
</tbody>
</table>

Appendix A
D.J.A. Hamblen  
Safety & Reliability Engineer  
Magnox Generation Group  
British Nuclear Fuels Limited (BNFL)  
Berkeley Centre  
Berkeley, Gloucestershire  
England

Mark Cunningham  
PRA Branch Chief  
Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555  
USA

Anna Grant  
Atomic Energy Control Board  
Reliability & Risk Assessment  
280 Slater Street, Station B  
Ottawa K1P5S9 Ontario

Joseph Murphy  
Special Assistant to the Director  
Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555  
USA

Ann Ramey-Smith  
U.S. Nuclear Regulatory Commission  
Probabilistic Risk Analysis Branch  
T-10E50  
Washington, D.C. 20555  
USA

Magiel F. Versteeg  
Inspector Reactor Safety  
Dutch Nuclear Regulatory Body (KFD)  
P.O.Box 90801  
2596 LV The Hague  
The Netherlands

Genevieve Baumont  
IPSN/DES/SECCA  
BP 6  
92265 Fontenay-aux-Roses CEDEX  
France

Jeanne-Marie Lanoré  
IPSN/DES  
BP6  
92265 Fontenay-aux-Roses CEDEX  
France

Johannes Mertens  
Institute for Safety Research and Reactor Technology  
Forschungsgelaende Juelich  
D-85748 Garching  
Germany

Oliver Straeter  
Gesellschaft fur Anlagen un Reaktorsicherheit (GRS)  
Forschungsgelaende  
D-85748 Garching  
Germany
Attila Bareith  
VEIKI Institute for Electric Power Research  
Gellerthegy U. 17  
Budapest, Hungary H-1016

Pekka Pyy  
VTT Automation  
P.O.Box 1301  
02044 VTT  
Finland

Pierre Le Bot  
Electricité de France (EDF)  
Research & Development Division  
Safety & Reliability Branch  
1 Avenue du General de Gaulle  
92141 Clamart CEDEX  
France

Stefan Hirschberg  
Paul Scherrer Institute  
Systems/Safety Analysis Section  
Nuclear Energy Research, Safety  
CH-5232 Villigen PSI  
Switzerland

Bo Liwang  
Statens Kärnkraftinspektion (SKI)  
Department of Plant Safety Inspectorate  
Klarabergsviadukten 90  
S-106 58 Stockholm  
Sweden

Mamoru Fukuda  
Nuclear Power Engineering Corporation (NUPEC)  
Safety Analysis Division I  
Institute of Nuclear Safety  
Fujita Kanko Toranomon Bldg., 7F  
17-1, 3-Chome Toranomon  
Minato-Ku, Tokyo 105  
Japan
Appendix B. Questionnaire Form for PWG-5 Task 97-2

Respondent's name:
Affiliation:
Mailing address:
Country:
Telephone:
Fax:
E-mail:

1. Describe the method used to analyze errors of commission, including
   1a. A statement of the purpose and scope of the method used in the analysis:

   1b. A description of the underlying concepts of the analysis method used (that is, reference to human sciences, if relevant):

   1c. A summary of the steps taken or the procedure used for conducting the analysis:

2. Describe in detail the event or sequence analyzed:

3. Describe the findings from the analyses, including
   3a. Findings regarding the method used, especially theoretical insights, practical lessons learned (e.g., software requirements, expertise requirements, resource requirements), and data input and output:

   3b. Findings regarding errors of commission, especially contributors to these errors and consequences of these errors in the event or accident sequence analyzed:

4. Provide definitions of terms and parameters used in responses to the questions listed above.

5. Provide thoughts on the relevance of the analyses method and findings to PSA:

6. Propose a list of key references for inclusion in the task report.
Appendix C: Contributions from Participating Countries
Input from the Czech Republic:
Using SHARP for Analysis of Errors of Commission

Jaroslav Holý
Nuclear Research Institute, Czech Republic

with input from

Stanislav Husák
Nuclear Research Institute, Czech Republic

Bengt Lydell
RSA Technologies, California, USA

Purpose

The purpose of the following document is to present information about using SHARP for analysis of specific kinds of errors of commission in S-PSA for NPP Dukovany and make contribution to the Task 97-2 report, according to the agreement made in Task 97-2 meeting in Budapest.

1. Introduction - the Concept of 'Error of Commission'

The concept of error of commission becomes a very important subject of human reliability analysis performed within current PSA projects and applications of PSA models. Some basic conclusions connected with this concept reached at a number of international fora can be simplified and shortened writing down the following insights

- errors of commission are very important
- errors of commission are not usually studied in HRAs
- errors of commission can be hardly studied using common HRA methodologies
- it is necessary to developed quite new approach for analysis of errors of commission
- a new approach ATHENA should be used for analysis of errors of commission.

The main goal of the following text is to describe the course, methodology and some preliminary results of S-PSA project for VVER-440/213 nuclear power plant Dukovany located in Czech Republic and this way:

- support point 1
- not quite agree with point 2
- discuss point 3 and 4
- make some comments to point 5.

The following information is based on a brief extract from the materials developed for the purposes of NPP Dukovany S-PSA project. The project started in 1996 and the preliminary results were released in October 1997. At present, the preliminary results are being updated.
2. Basic Methodological Approach Used for NPP Dukovany S-PSA

During the whole course of analysis performed in frame of PSA-1 for NPP Dukovany, the SHARP approach\(^1\) was followed in general. Some of SHARP’s steps were modified to optimize them for Dukovany case taking into account the scope and resources of the PSA project, as well. In the S-PSA project, some other modifications of approach were performed to address new insights obtained either during PSA Study for NPP Temelin (another NPP located in Czech Republic) or through independent review of HRA for NPP Dukovany PSA-1.

The basic elements of SHARP are similar in PSA-1 and S-PSA case. The goals of each step are as follows:

- Definition: To ensure that all different steps of human interactions are adequately considered in the study.
- Screening: To identify those human interactions that are significant to the operation and safety of the plant.
- Qualitative Analysis: To develop a detailed description of important human interactions by defining the key influence factors necessary to complete the modeling.
- Representation: To select and apply techniques for modeling important human interactions in logic structures (such methods can help to identify additional significant human actions that might impact system fault trees and even event trees).
- Impact integration: To explore the impact of significant human actions identified in the preceding steps on the system logic.
- Quantification: To apply quantification methods to assign probabilities for various interactions examined, determine sensitivities and establish uncertainty ranges.
- Documentation: To include all necessary information for the assessment to be traceable, understandable and reproducible.

2.1 Definition of Human Related Primary Events of NPP Dukovany S-PSA Model

Three methods of investigation can be suggested for searching for human related primary events (anyone or all of them may be used within SHARP):

- the identification of human activities associated with equipment identified in the event and fault trees
- an examination of related past events and plant emergency procedures
- examination of the event and fault trees with a classification scheme of how human enters into an accident sequence, in order to assure that all possible types of human interaction are

---

considered, the following classification scheme is used very often:
- type A action, pre-accident action etc. - before an initiating event, plant personnel can affect availability and safety by inadvertently disabling equipment during testing or maintenance
- type B action, contributor to IE - by committing some error, plant personnel can initiate an accident
- type C action, post-accident action - plant personnel, attempting to follow procedures can make an error that leads to failure to terminate the accident
- recovery action - improvising partly or in total, plant personnel can (not) restore and operate initially unavailable equipment to terminate an accident.

The identification of human activities associated with individual pieces of equipment was the preferred way of searching for human related primary events in NPP Dukovany PSA-1 project. The original version of SHARP provides the user with the following questions to help him to identify potential human errors
- Could operators induce an initiating event by working on or using the systems?
- What major tasks must the operator perform on the particular system to start it, stop it, or maintain it?
- Could the operator affect the redundancy or diversity of the system or function in any way?
- If the automatic functions fail, could the operator act as a backup?
- Is the system tested? What important failure modes of the system are addressed in the test?
- If the system is under repair, is the technical specification time limit for system unavailability less than the repair time?

It can be seen that this identification scheme can be used not only for errors of omission, but also for errors of commission. A correct and sufficiently comprehensive response to questions No. 1 and No.3 should significantly help to identify errors of commission whereas their potential for identification of errors of omission is much lower. For this type of errors, the remaining questions, i.e. No. 2, 4, 5, and 6 are determined.

The potential for occurrence of errors of commission is different for human interventions from the individual categories defined by SHARP.

The first category of pre-accident failures represents errors of omission (by misposition of valves during maintenance, the process of changing the position of valve to transfer the system into maintenance status and omission of restoration of original valve position before system transfer back to operation is meant).

The second category, on the other hand, represents almost exclusively errors of commission, because plant personnel must do, in simple words, something in addition to normal activities to cause initiating event. The potential for extra actions is significantly reduced during operation on nominal power, but is pretty high during shutdown. Both categories of type B events analyzed in detail for NPP Dukovany during S-PSA project, i.e. man-induced LOCAs and boron dilution events, contains very typical representatives of errors of commission.

The broad category of errors in plant response to initiating event (type C actions) contains both types of errors
- errors of omission as well as errors of commission. In general, both categories can be studied by means of current HRA methods. The problem with errors of commission can be that there is no universal particularly systematic approach for identification of those errors so that the issue of completeness of set of errors of commission has to be discussed.

Finally, recoveries, as usually defined, incorporated into PSA model, and analyzed, are supposed not to contribute to errors of commission very much, for they usually represent well defined activity focused on restoration of operation of given unavailable piece of equipment. However, there is significant potential for errors of commission here (start of operation of not required system potentially leading to problems, blockage of operation of component necessary for start of operation of another component with not quite favourable consequences etc.). This potential is normally not studied and cannot be incorporated into PSA model using standard approaches preferring analysis of recovery actions within late phase of development of PSA model using the most important minimum cut sets obtained on the base of initial quantification.

The last possibility of identification of human related failure events was also used in NPPDukovany S-PSA. The database SIS containing safety important events was searched through and some relevant records were found. As an example, the event of man-induced LOCA type can be mentioned, when some primary circuit water was lost due leakage through main isolation valve into drained down loop and, consequently, through main circulating pumps having been repaired. This event has got some significant errors of commission features (actions normally not allowed under the given circumstances were performed).

2.2 Screening of less important human related primary events

There is no reason to separate errors of omission and errors of commission from point of view of screening, should any from the following variants of screening be performed

- judgment based screening
- rough (coarse) screening
- fine (detailed) screening.

The approximate quantification methods providing conservative numerical values for fine screening are appropriate for both types of errors. Perhaps, the level for screening out the individual primary events representing errors of commission should be set in a different (more conservative) way from the level for screening errors of omission, because the level of explicitness of description of actions from either category is different (errors of omission are generally more simple to be defined and described from point of view of consequences than errors of commission).

2.3 Qualitative Analysis of Important Human Actions.

In SHARP, two primary goals of detailed qualitative human reliability analysis are defined:

- to postulate, what operators are likely to think and do and what they might do in a given accident sequence
to postulate how an operator’s performance may modify or initiate an accident sequence.

Both these primary objectives cover either errors of omission and errors of commission and there is no reason why this part of SHARP could not be used for both categories of errors.

In the description of process of qualitative analysis typical for SHARP, the key role of prediction of operator performance and possible human error modes is pointed out. The process of qualitative analysis is broken down into four key stages in SHARP:

- information gathering
- prediction of operator performance and possible human error modes
- validation of predictions
- representation of output in a form appropriate for the required function.

During the process of information gathering, SHARP requires insights concerning operator’s decision making in similar situations to be sought and any operation that appears to be prone to mistakes which could initiate an accident sequence to be determined. This should help to identify possible specific modes of human interaction that may initiate new sequences. The types of errors observed help to focus on the type of cognitive processes involved.

The spectrum of factors influencing operator reliability during low power and shutdown operation was similar to the PSA-1 case in Dukovany S-PSA, but a relative importance of the individual factors was found to be different. For example, the importance of performance shaping factor stress (due to lack of time)A decreased due to prolongation of time, control room staff has at disposal (the course of transient is less dynamic due to much less residual heat produced during shutdown). However, the general conclusion about influencing factors (PSFs) is that the factors potentially initiating occurrence of errors of commission rather than errors of omission are relatively much more important in low power and shutdown regimes than during operation of nominal power. This is primarily caused by the general strategy of operation during shutdown, where there is much less room for automation of operation on one side, and much more improvisation is typical, on the other hand. In addition, the response to the occurrence of non-standard status is made more difficult and more variable by the fact that almost no emergency procedures are used during the shutdown period and also by blocking many alarms and automatic responses of equipment during transfer of the unit from full power to shutdown status. However, a favorable feature of shutdown operation from point of view of risk (and potential for occurrence of errors of commission) is the fact that many of potential causes of problems, configurations of equipment, failure states etc. are not possible to happen here so that the control room personnel has to work with substantially smaller number of variants during diagnosis acts.

As for the process of prediction of operator performance, SHARP strongly recommends to take into consideration possible errors of diagnosis and failures in selecting strategies. Classification or taxonomies of human error modes and underlying psychological mechanisms constitute the most readily available help for the analyst according to SHARP. As direct tests of validity of predictions, the use of simulators and interviews with operators are suggested by SHARP.

One of the products of qualitative analysis is the detailed description of all defined (and not screened out) human actions. The approach to the description may and should be the same for both categories of errors. The question whether to formally separate both categories by developing different name schemes when
defining nomenclature of names of primary events has to be solved.

2.4 Modeling of human actions.

SHARP offers a comprehensive set of questions to aid the development of representations for each human interaction type. The following subset of questions are devoted directly to errors of commission:

- Are there different events within similar plant responses (e.g. alarm patterns) that require very different operator responses? (This affects the likelihood of responding to the wrong event.)
- Does the operator have enough instrumentation to have feedback on previous actions? (This affects the potential for recovery from a wrong action.)
- Are there steps in the procedure where the operator could make a mistake that could change the course of an accident?
- Can the operator's mental image of the plant cause one accident sequence to be linked to another?

The number of methods proposed for development of formal representation of individual human action is pretty high. Among them, mainly two methods were used within NPP Dukovany PSA Study with different aims. The human reliability analysis event trees proposed by THERP2 were found to be useful when modeling various variants of available interactions between human and hardware, all of them leading to fulfilling the given goal. The operator action trees were useful for analysis of various factors influencing probability of operator success. A variant of operator action trees methodology with the basic logic objects called decision trees3 was used within NPP Dukovany PSA-1 and S-PSA to model failures during information processing. This approach can be, from general point of view, directly applied to the solution of the problems with modeling errors of commission, nevertheless it is necessary to develop a specific set of decision trees.

Another analytical method mentioned and proposed by SHARP is confusion matrix. The method is used for systematic search for potential for misunderstanding the indications about current plant status and failure of diagnosis regarding specification of initiating event. This way, the potential for occurrence of errors of commission directly in or as a consequence of diagnosis phase of response to initiating event can be studied. The method was not used as a part of Dukovany PSA effort.

2.5 Integration of Human Actions into the PSA Model

In general, integration of human actions into the model brings an iterative kind of work with several versions of the PSA model. There is enough room within this step to take into account newly identified errors of commission and to include them into the model. The list of representations and descriptions of safety important human interventions identified so far can significantly help in searching for additional errors of commission, at least in two ways:

---

human actions identified so far including their mutual relations and dependencies force the analyst to discover extra potential for additional failures of plant staff

as a part of human actions description, the circumstances the given human actions are performed under are defined and analyzed in detail, this can lead to identification of specific (strong) error forcing context and, as a consequence, potential for new specific error of commission.

In the Dukovany S-PSA, the first part of work normally performed within this step was done already during the development of the first iteration of the model. After the development of the first set of human related primary events, all events were discussed in detail and the following changes were made in the model, for example:

- inclusion of new kind of initiating events
- changes in modeling of dependencies
- changes in fault tree logic.

A good example of integration of human element into the S-PSA model is the discussion about man-induced LOCAs and boron dilution problems and the decisions adopted leading to modifications in Dukovany S-PSA model. Here, the identified errors of commission strongly influence the structure of list of initiating events. It was found, for example, that the contribution of the case of normal (random) primary circuit piping breaks for real shutdown operation is almost negligible in comparison with loss of primary circuit coolant induced by failures of plant staff, which belong, to a big extent, to the errors of commission category.

2.6 Quantification of Human Actions

Both the methods evaluated and recommended in SHARP and some quite up-to-date methods were used for quantification of probabilities of failures of human actions. Among them, the methods ASEP4, THERP, HEART5 and decision tree method 6 did the largest part of work. Most of those methods have proven to possess good tools for quantification of errors of commission, as well.

The THERP methodology was used for quantification of all pre-accident actions, human failures contributing to initiating events and for a small part of quantification of probabilities of unsuccessful recoveries. Indeed, major part of quantification of human errors connected with man-induced LOCA scenarios was done this way, including errors of commission. There exist quite good tools for quantification of errors of commission in THERP, because almost a half of tables and equations forming together the quantification scheme in Chapter 20 of Swain’s manual are devoted to errors of commission.

The HEART methodology brings a very interesting list of factors influencing operator’s work, which is

---

structured in a pretty different way than performance shaping factors in THERP, many of them quantifying key elements of error forcing context leading to errors of commission occurrence. This way, HEART can help in quantification of some specific cases of errors of commission (as well as errors of omission), THERP has got problems with. The method is also broadly discussed in Chapter 8 of manual draft of new human reliability analysis methodology ATHEANA and is proposed as one approach suitable for quantification of probabilities of plant personnel performing unsafe actions.

The adjusted decision tree methodology was applied to analysis and quantification of failures during information processing as a part of analysis of type C actions, mainly errors of commission. In general, this method is very flexible and can be adjusted to be an efficient tool for analysis of a very broad spectrum of human errors. Even the variant of method used in Dukovany PSA, which was primarily developed for analysis of errors of omission, can bring some useful insights regarding errors of commission.

An example of detailed quantification of human related primary event connected with errors of commission is given in section 3.5.

3. Application of SHARP During Analysis of Man-Induced LOCA Phenomenon

The man-induced LOCA problems represent a specific issue, which is particularly important for shutdown operation, where the plant staff has got a number of opportunities to cause loss of primary circuit coolant. This issue was studied in detail as a part of HRA effort within NPP Dukovany S-PSA project. The SHARP method was used as a general framework for analysis.

3.1 Identification

In general, human errors starting the process finally leading to man-induced LOCA can be mostly seen as typical errors of commission, because the primary circuit integrity has to be broken by inadvertent action. Only in minor part of cases, the process is started by error of omission, i.e. when the real start of loss of coolant process (start of pump and opening of valve in discharge line) is part of planned operation and some valve was omitted to be closed or checked when leaking. To get realistic man-induced LOCA scenario with non-negligible consequences, the primary (initiating) error of commission has to be followed by one or a sequence of errors of omission (failures to check visually the status of equipment during regular walkthrough, failure to repair equipment correctly etc.).

The identification process applied to man-induced LOCA scenarios in NPP Dukovany S-PSA mostly followed the rules defined within SHARP. The issue of completeness was very important in there. The VVER 440/213 primary circuit piping and connecting safety and support systems include a very large number (several hundreds) of isolation valves, vent valves, drain valves, relief valves, and instrument root valves of various sizes. There are literally hundreds of combinations of misaligned valve configurations that could lead to draindown scenarios of different severity. All those combinations were, at least formally, taken into account during the identification phase. It was necessary, even within this starting point of application of SHARP, to define a set of informal, approximate, and fast screening rules to be able to make quick decisions
about neglecting most of alternatives. The more complicated, but expected to be neglected, variants were discussed with plant personnel with the aim to take into consideration their opinion. Finally, as proposed by SHARP, the database of plant specific safety important events SIS was searched through. Some non-trivial events with man-induced LOCA potential were found and this information was incorporated into that current list of man-induced LOCA scenarios. At the end of first step of SHARP procedure, the list of man-induced scenarios contained 53 elements representing various ways of loss of primary circuit coolant.

3.2 Screening.

There is special problem with screening when the subject of screening process are human related scenarios contributing to initiating event frequency (errors of commission as well as errors of omission). Normally, i.e. for type C actions, a preliminary version of PSA model is used for screening with highly conservative values of probabilities of human errors. However, for man-induced LOCAs, the expected final quantitative results of the whole analysis are only numerical values determining frequencies of several LOCA initiating events, as a consequence, the importance of many individual potential contributors to those several values can not be checked against the results of quantification of complete (although approximate and conservative version of ) PSA model.

Due to above mentioned reason, it was necessary to develop exact screening rules as a part of screening process. Barrier analysis was used as the principal technique for screening of the draindown scenarios. For a draindown event to occur, one or more safety barriers must be broken. The frequency of a draindown event is a function of the number and the kinds of safety barriers that fail.

Safety barriers are physical and administrative devices used to protect facilities and people from unexpected and undesirable actions, conditions or situations. Both categories of barriers, i.e. physical (electrical/electronic or mechanical valve interlocks, diversity, position indications etc.) or administrative (procedures, training, supervision/communications, equipment tagging etc.) were investigated during analysis.

There are many compensating factors, which enable operators to detect and recover from starting man-induced LOCA events. Although during the outages the role of the plant staff changes considerably during compared with full power operation and the operating circumstances become more difficult, these types of errors are normally identified fortuitously as a result of shift turnovers, routine system walkdowns or special inspections in most cases. An insufficient plant staff performance during this kind of activities can form error of omission contributor to man-induced LOCA scenario.

The following elements of plant operation, either hardware or administrative measures, have been defined to be barriers in Dukovany project:

- motor operated valve, which should be normally closed (solid barrier)
- manual valve, which should be normally closed (solid barrier)
- check valve (supposed to be solid barrier in most cases, questionable barrier in some cases)
- quick acting valve (solid barrier, part of emergency core cooling systems)
- blinded output (quite sufficient barrier, the existence of it leads to immediate screening of the given
scenario)

administrative measure ZRT, locked, blocked and tagged manual valve (solid barrier, three barriers in fact, but loss of individual barriers highly dependent, conservatively supposed to be one barrier only)

administrative measure ZRTA, locked, blocked and tagged motor operated valve disconnected from electric supply (solid barrier, four barriers in fact, but loss of individual barriers partly dependent, conservatively supposed to be one barrier only therefore)

- S-instruction, standard written form for transfer of equipment from operation into maintenance. The equipment with filled in S-order is formally considered to be unavailable. It is put in the list of blocked equipment, which is checked and agreed during every change of shift. The equipment under S-order should be protected and blocked against any manipulation (solid barrier, includes checking of status during change of shift)

valve position indication in control room (solid barrier in some cases, can be used during shutdown only provided that the corresponding signal train or its electric supply is not maintained)

signal water on floor XY (auxiliary criterion for screening, can reduce potential for man-induced LOCA features of accident scenario but, in some cases, can not totally prevent consequent damage of equipment below the room with the break)

(frequent) visual control (auxiliary criterion for screening, influenced the decision about screening of the given scenario in questionable cases)

continuous checking of JOV (sump of lost water) level and trends of JOV inputs (auxiliary criterion for screening, not used for basic decisions about scenario screening).

The final set of screening criteria took into consideration the expected frequency of occurrence, leak rates, and compensating factors (e.g. potential for recovery by the operators). Consideration also was given the Dukovany and Bohunice NPP service experience. The following screening rules were applied to the identified pathways:

- Physical location. Valves located at plant elevations above the primary loops were screened out unless credible siphoning effects via vent or relief valves were identified.

- Leakage not expected. For some identified paths, leakage is either impossible (blinded piping) or water flow in the relevant piping is hardly to be established.

- Leak rate. Two categories of leaks from point of view of scenario screening were defined: 1) small leaks up to 20mm of equivalent diameter 2) bigger leaks. For these two categories, different screening rules were developed based on number of safety barriers.

- Frequency of occurrence. In case of small leak category, more than one identified safety barrier was sufficient condition for screening of scenario. In case of bigger leak category, at least three solid barriers were necessary for screening. When only one barrier existed for small leakage or two barriers existed for larger leakage, an existence of additional positive factor was necessary for screening.

- Other specific factors. In some cases, there are additional factors decreasing the potential for loss of coolant occurrence, which are not supposed to be barriers, but whose existence can lead to screening of the given scenario, for example, not probable coincidence of two events (pump running and valve open). These factors influenced the screening process significantly in some
The screening phase of SHARP resulted in significant reduction of number of scenarios written in the man-induced LOCA list - from 53 to 16 scenarios grouped into 10 categories.

3.3 Qualitative Analysis

During identification and screening phase, every scenario contributing to man-induced LOCA category was analyzed as one integral representative of LOCA potential. Within qualitative analysis, every not screened out scenario was broken down into basic elements and potential failure mechanisms, including separation of error of omission and error of commission variants.

The first level of splitting the scenarios was separation of initiating and developing part of the scenarios. The initiating part represents direct cause of occurrence of mechanism leading to loss of coolant, what usually means mistaken opening of manual or motor operated valve (error of commission). The second part of scenario is normally connected with failure of various kind of check of equipment status (errors of omission). Both parts of scenario were further analyzed in detail.

Regarding initiating part of scenario, several basic mechanisms of errors of commission were identified. The most frequent two among them were:

- Misunderstanding in communication between the members of plant staff. There is correct decision to open some primary circuit valve reached by auxiliary operators, for example. The decision is transferred to the person manipulating equipment. The decision is misunderstood and some other valve is opened instead the right one.

- Misselection of valve. The (correct) decision about opening some primary circuit valve is successfully transferred to the person responsible for manipulation and is fully understood. For some reason, different valve is selected and manipulated.

The second part analyzed scenarios was represented by various kinds of failures of checks of equipment status. Usually, there are several possibilities of successful revealing of the break after the break was initiated, but before it can lead to irreversible consequences. If the break is very small, the process of loosing water is so slow under shutdown operating conditions that the whole scenario should be screened out in many cases. If the break was found to be more significant, several kinds of checks have to be analyzed as immediate visual check, regular walkthroughs made by every shift, signalization in control room (but with non-negligible potential not to be available due to maintenance in shutdown period) etc.

It can be interesting to analyze how the individual failure mechanisms are sensitive to the measures adopted against occurrence of them. From this point of view, miscommunication can be supposed to be pretty dangerous, because several barriers against opening the valve can be broken this way. If the person responsible for manipulation is instructed to manually open the valve, he can not be very surprised that the valve is, for example, tagged and locked. In case of misunderstanding of the direction, all standard administrative barriers can be broken. One of the conclusions made on the base of the analysis can be that, regarding potential for misunderstanding, there is additional factor which can be more important than
standard administrative measures. This factor is connected with general common status of the equipment during shutdown and can be described by following two rules:

- If there are several mutually interchangeable pieces of equipment, which can be found in different positions (operational modes) in shutdown period, there is relatively big potential for error of commission. As an example, primary circuit loops main isolation valves can be presented. During shutdown period of VVER reactors, one loop is operated and one loop is in reserve with main isolation valves closed, the remaining loops can be maintained with opened or closed main isolation valves. If the specification of loop is misunderstood during communication, different main isolation valve can be opened, even when it is tagged and locked.

- If all potentially interchangeable pieces of equipment of the given type are generally known to be in one position only during the whole shutdown period (closed and no reason to be manipulated, in many cases the manipulation even explicitly prohibited), the probability of mistaken manipulation is much lower, especially in case when some administrative measures against opening are adopted.

3.4 Representation.

For the logical structures integrating various alternatives belonging to the man-induced LOCA scenarios were not quite complex, it was not necessary to develop formal graphical representations for them in case of NPP Dukovany S-PSA. The basic simple probabilistic rules were used to derive probabilities of the man-induced LOCA scenarios from the individual elements. It should be noted that probability theory itself is quite good environment for analysis of this type and the cascade of equations used during the computations of probabilities or frequencies of the given scenario is really not bad representation of scenario logic (although not in graphical form). Another possibility, which was partly used during more complex computations and which helped to understand of the logic of the given scenario, were small standard fault trees. Of course, trees proposed by THERP could have been used.

3.5 Quantification

In Dukovany S-PSA, this step was performed before the step Integration, which normally follows the step Representation in SHARP. The reason was the specific kind of events analyzed, i.e. type B actions, and the necessity to integrate and transfer the frequencies of all elementary man-induced LOCA scenarios into the frequencies of LOCA categories occurring within the given set of shutdown POSes. To do that, it was necessary to quantify the elementary man-induced LOCA scenarios at first.

The methods THERP and HEART presented in the general part of this document were used for quantification of all 10 groups of 16 scenarios specified during screening phase of analysis and qualitatively analyzed in detail. In Table 1, the basic types of failures and corresponding values of probabilities taken from THERP for the purposes of man-induced LOCA analysis are described. This table can be used as a good example of the fact that not only errors of omission, but also errors of commission can be approximately quantified using generic data from THERP.
The table consists of four columns. In the first column, the codes are specified that have been used in further analysis for representation of the given alternative of failure (and the corresponding probability of failure). A short description of failure type can be found in the second column. The third column of the table contains probability value. Finally, the reference to the corresponding table in Chapter 20 of Swain’s manual is presented in the last column.

Table 1. Some generic values of probabilities of human failures taken from THERP

<table>
<thead>
<tr>
<th>Code</th>
<th>Definition</th>
<th>Probability</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL-1</td>
<td>failure to check valve (being in wrong status) using change or restoration list</td>
<td>1.0E-02</td>
<td>Ttab20-6</td>
</tr>
<tr>
<td>MIL-2</td>
<td>failure to receive oral instruction with one critical item</td>
<td>1.0E-03</td>
<td>Ttab20-8</td>
</tr>
<tr>
<td>MIL-3</td>
<td>selection of wrong control on a panel from an array of similar appearing controls identified only by labels</td>
<td>3.0E-03</td>
<td>Ttab20-12</td>
</tr>
<tr>
<td>MIL-4</td>
<td>selection of wrong control on a panel from an array of similar appearing controls arranged in well delineated functional groups</td>
<td>1.0E-03</td>
<td>Ttab 20-12</td>
</tr>
<tr>
<td>MIL-5</td>
<td>selection of wrong manual valve, which is clearly and unambiguously labeled and set apart from valves similar in size, shape, state and presence of tags</td>
<td>1.0E-03</td>
<td>Ttab 20-13</td>
</tr>
<tr>
<td>MIL-6</td>
<td>selection of wrong manual valve, which is unclearly or ambiguously labeled and set apart from valves similar in size, shape, state and presence of tags</td>
<td>5.0E-03</td>
<td>Ttab 20-13</td>
</tr>
<tr>
<td>MIL-7</td>
<td>probability of failure of human action with medium level of dependence on another human action with failure probability less than 1.0E-02 (provided that that action failed)</td>
<td>1.5E-01</td>
<td>Ttab 20-21</td>
</tr>
<tr>
<td>MIL-8</td>
<td>probability of failure of human action with high level of dependence on another human action with failure probability less than 1.0E-02 (provided that that action failed)</td>
<td>5.0E-01</td>
<td>Ttab 20-21</td>
</tr>
<tr>
<td>MIL-9</td>
<td>failure to check routine tasks, checker using written materials</td>
<td>1.0E-01</td>
<td>Ttab 20-22</td>
</tr>
<tr>
<td>MIL-10</td>
<td>failure to check routine tasks, checker not using written materials</td>
<td>2.0E-01</td>
<td>Ttab 20-22</td>
</tr>
<tr>
<td>MIL-11</td>
<td>failure to check position indicator (only)</td>
<td>1.0E-01</td>
<td>Ttab 20-22</td>
</tr>
<tr>
<td>MIL-12</td>
<td>failure to check status of equipment if that status affects one=s safety when performing his tasks</td>
<td>1.0E-03</td>
<td>Ttab 20-22</td>
</tr>
<tr>
<td>Code</td>
<td>Definition</td>
<td>Probability</td>
<td>Reference</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>MIL-13</td>
<td>probability of failure of human action with low level of dependence on another human action with failure probability less than 1.0E-02 (provided that that action failed)</td>
<td>5.0E-02</td>
<td>Ttab 20-21</td>
</tr>
<tr>
<td>MIL-14</td>
<td>selection of wrong manual valve, which is clearly and unambiguously labeled, but not set apart from valves similar in size, shape, state and presence of tags</td>
<td>3.0E-03</td>
<td>Ttab 20-13</td>
</tr>
<tr>
<td>MIL-15</td>
<td>probability of error of omission of one item of procedure without checkoff provisions</td>
<td>3.0E-03</td>
<td>Ttab 20-7</td>
</tr>
</tbody>
</table>

### 3.5.1 An Example of Quantification of Specific Man-Induced LOCA Scenario

The application of THERP and HEART on analysis of one specific man-induced LOCA scenario is showed in the rest of this section. It is man-induced LOCA scenario A3.1 (according to the classification adopted within Dukovany project). A short formal definition of the scenario is mistaken opening of main isolation valve located on connection of empty loop and full part of primary circuit when the integrity of the given loop is lost due to some kind of maintenance. The scenario is investigated in relation with three shutdown POSes representing 'realA shutdown, i.e. operation with natural circulation in one loop (sometimes two loops), one loop in reserve and four (three) loops empty.

A loss of coolant can be initiated in any shutdown POS this way. The equivalent diameter of the break depends on level of loss of integrity of the empty loop (any category of LOCA is possible to happen, in substance).

The main isolation valve connecting empty loop with full part of primary circuit should be disconnected from electric supply, blocked and tagged. In addition, the position of valve should be checked according to specific rules. Both ways of opening the valve are possible, in principle - either distant opening from control room or local manual manipulation. After mistakenly opening of the valve, there is high potential for revealing the break by visual checking of loop status, this potential depends on the location of loss of coolant from desintegrated loop and on amount of lost primary circuit water.

There are two basic variants of mistaken opening of main isolation valve:

- manual
- distant from control room.

The first variant can be represented by two sub-variants:

- 1a - error in communication, auxiliary operator does not understand correctly oral instruction and opens different main isolation valve than that, which has been planned (error of commission)
1b - failure in blocking and tagging of valve, the instruction is well understood, but mistake in selection before manipulation happens (error of commission).

Note. The other possible sub-variants were neglected. It was supposed that if the tagging and blocking of valve is done correctly and the auxiliary operator understand correctly the instruction, he does not open the blocked valve (does not made error in selection).

The variant 1a is quite interesting. If the instruction is not understood, the auxiliary operator can try to open the valve even in case it is blocked and tagged (he can suppose that the valve is blocked and tagged, because this is normal valve status before its opening during shutdown)!

In addition, the communication connected with specific checking using written S-order providing additional level of redundancy against opening the main isolation valve is intended to take place between the senior representative of operation department and senior representative of maintenance department so that it may not prevent misunderstanding in communication with other plant staff. It is important to take into account that there are six loops at VVER-440/213 reactor unit and four of them are normally empty during shutdown so that there is enough room for misunderstanding here.

The basic value of probability of not understanding instruction and opening wrong main isolation valve, as a consequence, is 1.0E-03 (MIL-2). During shutdown, several manipulations performed on different loops with potential for this type of mistake are performed, the number of such manipulations was estimated to be 5. On the other hand, even if such mistake happens, it may not cause LOCA, because the empty loop can be perfectly tight, the probability of empty loop not to be tight was conservatively estimated to be 0.5. In total, the annual frequency of causing some kind of LOCA during shutdown due to above defined alternative 1a can be estimated as

\[
1.0E-03 \times 5 \times 0.5 = 2.5E-03.
\]

The alternative 1b is much less probable, because three conditions have to be fulfilled at the same time:

- the valve is not blocked and tagged according to the procedure with all manipulations supposed to be absolutely dependent (error of omission, potentially also error of commission)
- the independent check of blocking and tagging of valve (related to S-instruction) is not correctly performed (error of omission)
- the auxiliary operator makes mistake in selection of valve (error of commission).

The probability of first two conditions was estimated to be 1.0E-02 (conservative estimate based on plant experience, MIL-1), the probability of selection failure can be transferred from THERP (MIL-5, MIL-6), low probability value is more realistic, because a very strong indisposition of local plant staff has to take place to make mistake in selection of main isolation valve. In total, the probability of alternative 1b as a whole is of order of 10^-7 and the alternative can be neglected in comparison with the alternative 1a.

The second variant of opening main isolation valve, i.e. distant opening from control room, can happen if two basic conditions are fulfilled:

- the valve is not disconnected from electric supply (probably error of omission)
- the CR operator makes mistake in selection of manipulator (error of commission).

The method HEART was used for quantification of mistake in disconnection of electric supply. The HEART category of action was specified as transfer of system (component) into new or original status using procedure..., the nominal probability of failure from this category is 3.0E-03 in HEART. There is independent control of electrical disconnection, a failure of it was quantified as 1.0E-01 (MIL-9). In total, the failure of disconnection of electric supply (persisting for a long time) was quantified by the value of 3.0E-04.

The operator in control room can make mistake due to wrong communication or due to wrong selection of valve control at panel. This possibilities can be quantified using values corresponding to codes MIL-2, MIL-3, MIL-4, i.e. 1.0-2.0E-03. The number of situations during shutdown with potential for this type of failure can be estimated as several.

In total, the annual frequency of the second variant may not exceed 1.0E-06 and should not exceed 1.0E-05. It means that also risk contribution of this variant can be neglected in comparison with the variant 1a.

The main result of so far performed analysis of Scenario 3.1 is that the variant 1a, i.e. failure in communication with local plant staff is the dominant contributor to the scenario 3.1. From point of view of continuation of accident scenario, loss of coolant can have two basic forms here

- loss of coolant through (maintained) main circulation pump
- loss of coolant through drainage piping.

In the first case, all kinds of loss of coolant (from point of view of intensity) are possible, a concrete equivalent diameter of the loss depends on how much is the pump repaired. The occurrence of LOCA's of all categories with the same conditional probability of 0.33 was expected. However, there is a very realistic possibility that loss of coolant will be identified immediately due to visual checking of empty loop status by plant staff, a probability of failure of this visual check depends on how much coolant is being lost and was subjectively estimated for the individual LOCA categories as:

- probability of 0.5 for very small LOCA
- probability of 0.3 for small LOCA
- probability of 0.1 for larger LOCA.

The total probabilities of individual variants are:

- very small LOCA: 2.5E-03 x 0.5 x 0.33 x 0.5 = 2.1E-04
- small LOCA: 2.5E-03 x 0.5 x 0.33 x 0.3 = 1.3E-04
- larger LOCA: 2.5E-03 x 0.5 x 0.33 x 0.1 = 4.1E-05.

In the second case, the amount of lost coolant is limited by the diameter of drainage piping, which corresponds to small LOCA. Here, no credit was given to visual detection of loss of coolant, because coolant flow goes directly into special sump through drainage line. The total probability of small LOCA is in this case:
2.5E-03 x 0.5 = 1.25E-03.

The final estimation of annual frequencies of LOCA caused by Scenario A3.1 can be made as sum of values for both variants, i.e.:

- very small LOCA: 2.1E-04
- small LOCA: 1.3E-04 + 1.25E-03 = 1.4E-03
- larger LOCA = 4.1E-05.

3.6 Integration

In the analysis of man-induced LOCAs performed within NPP Dukovany S-PSA project, the integration step of SHARP was represented by derivation of final values of annual frequencies for three man-induced LOCA categories potentially occurring during three shutdown POSES and by making decision whether the individual combinations of LOCA categories and POSES can be screened out on the base of frequency value (no combination was screened out).

The input into this step of SHARP were the frequencies of 16 man-induced LOCA scenarios identified, analyzed and quantified within the previous steps of SHARP method. During consequent analysis, it was necessary to group the scenarios according to the potential of occurrence within the individual POSES (some manipulations can occur at an arbitrary time point during the whole shutdown period, randomly in substance, whereas other ones are more probable in some specific POSES and the other are possible even only in one specific POS). After the grouping, the redistribution of frequencies in accordance with newly established groups was performed. The final output from the step was the following table.

<table>
<thead>
<tr>
<th></th>
<th>VERY SMALL LOCA</th>
<th>SMALL LOCA</th>
<th>LARGER LOCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS7</td>
<td>2.65E-03</td>
<td>6.85E-04</td>
<td>9.24E-06</td>
</tr>
<tr>
<td>POS8</td>
<td>6.8E-03</td>
<td>1.76E-03</td>
<td>2.38E-05</td>
</tr>
<tr>
<td>POS9</td>
<td>3.15E-03</td>
<td>8.15E-04</td>
<td>1.1E-05</td>
</tr>
</tbody>
</table>

This way, the primary goals of using SHARP method for analysis and quantification of man-induced LOCAs were fulfilled. Through analysis of the identified errors of commission as well as errors of omission, the potential for occurrence of man-induced LOCAs representing one typical case of type B human errors during shutdown operation was estimated and quantified.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASEP</td>
<td>Accident Sequence Evaluation Procedure</td>
</tr>
<tr>
<td>ATHEANA</td>
<td>A Technique for Human Event Analysis</td>
</tr>
<tr>
<td>DT</td>
<td>decision tree</td>
</tr>
<tr>
<td>EDU</td>
<td>Nuclear power plant Dukovany</td>
</tr>
<tr>
<td>HEART</td>
<td>Human Error and Reduction Technique</td>
</tr>
<tr>
<td>HEP</td>
<td>human error probability</td>
</tr>
<tr>
<td>HRA</td>
<td>human reliability analysis</td>
</tr>
<tr>
<td>IE</td>
<td>initiating event</td>
</tr>
<tr>
<td>JOV</td>
<td>sump of lost primary circuit water</td>
</tr>
<tr>
<td>LOCA</td>
<td>Loss of Coolant Accident)</td>
</tr>
<tr>
<td>NPP</td>
<td>nuclear power plant</td>
</tr>
<tr>
<td>NRI</td>
<td>Nuclear Research Institute</td>
</tr>
<tr>
<td>POS(x)</td>
<td>plant operating status (No.x)</td>
</tr>
<tr>
<td>PSF</td>
<td>Performance Shaping Factor</td>
</tr>
<tr>
<td>PSA</td>
<td>Probabilistic Safety Assessment</td>
</tr>
<tr>
<td>PSA-1</td>
<td>first level of probabilistic safety assessment</td>
</tr>
<tr>
<td>RHR</td>
<td>residual heat removal (system)</td>
</tr>
<tr>
<td>SHARP</td>
<td>Systematic Human Action Reliability Procedure</td>
</tr>
<tr>
<td>SIS</td>
<td>Dukovany plant database of safety important events</td>
</tr>
<tr>
<td>S-PSA</td>
<td>probabilistic safety assessment of operation on low power and during shutdown</td>
</tr>
<tr>
<td>THERP</td>
<td>Technique for Human Error Rate Prediction</td>
</tr>
<tr>
<td>VVER</td>
<td>water cooled and water moderated reactor</td>
</tr>
<tr>
<td>ZRT</td>
<td>administrative measure used at EDU to prevent misopening of manual valves</td>
</tr>
<tr>
<td>ZRTA</td>
<td>administrative measure used at EDU to prevent misopening of motor operated valves</td>
</tr>
</tbody>
</table>
Contribution from Finland: Framework for Analyzing Commission Errors

Pekka Pyy
VTT Automation, Finland

FACE, "A Framework for Analysis of Commission Errors," is currently under development by VTT Automation for STUK (The Finnish regulatory body). The idea of FACE is to:

1. Draw attention to different types of commission errors,
2. Form a system based model of commission error structure with selected examples
3. Develop an identification method for commission errors
4. Develop probabilistic modelling / quantification method of commission errors

In the following, a short description on FACE is given with some other activities in Finland.

1. Introduction

The objective of this paper is to present and develop a method that can be used to analyze wrong human actions. Often, these events are called human commission errors. Also another human error mechanisms leading to wrong system response are included in the scope. This is due to the fact that we should not forget them in safety studies.

Many probabilistic safety assessments (PSAs) include in their scope solely procedure based human actions or their unavailability - omissions. The need to complete PSAs with the analysis of errors of commission has been noticed world wide as notified by e.g. 1. Commission errors are important, since they may lead to many types of wrong plant response. As comparison, the effects of an omitted, delayed or deficient response are more straightforward to see. However, many kinds of deviations in human and organizational performance may lead to undesired system response, as shown in Figure 1. This is resource taking from the PSA point of view, since both the error effects and their physical consequences have to be analyzed.

---

2. Examples on commission errors and their analyses in Finland

2.1 Incidents with commission errors in Finland

During the past few years, Finland has experienced some events that could be classified as some kind of errors of commission. The most important ones have been:

- Reactor scram due to erroneous opening of switches - A reactor scram occurred at Olkiluoto 1 on 27 May 1997 which was caused by an operational error.
- 20 kV switch plant damage in consequence of a fire - on 6 May 1994 a.m., the 20 kV switch plant at the Loviisa plant site sustained damage in consequence of a short circuit by arcing and of a small fire that resulted. The event was attributed to human error in the writing of a coupling programme.
- Shut-down service water system reliability was impaired - at both Olkiluoto plant units, an error had been made when installing shut-down service water system filter pressure difference switches. Consequently, automatic back-flushing of the filters would not have started immediately on potential filter blockage.

More information on these events may be obtained from STUK, e.g. from Jouko.Mononen@stuk.fi.

2.2 Commission error analyses in Finland

As a part of Finnish PSAs, a number of analyses have been performed directly or indirectly related to commission errors.

In operations domain, an analysis of potential misdiagnoses has been carried out in 1980's for the Loviisa VVER-440 213 plant. The method used was the confusion matrix. The quantification of the matrix was based on the potential to the misdiagnosis (four probability classes based on indications, trends and alarm patterns), training familiarity of the disturbances (three classes) and the time to recover from misdiagnosis (eight classes). As a result, some steam side LOCAs, steam generator tube ruptures, LOCAs outside the containment and reactor coolant pump LOCAs were seen to have some confusion potential. The plant has taken actions to improve the situation.
In maintenance domain, a study to identify systematically dependent errors has carried out for the Olkiluoto ABB design BWR-75 reactor in 1980's, as well. The study was based on the experience of both maintenance and operations personnel of the plant. A specific form was used to collect information about potential dependent maintenance errors and their effects. The form included columns for component groups affected, the source task of the error, the frequency of the task, potential consequence, detection possibilities and their frequencies, CCF class, measures to be taken and remarks. Although the method was now way restricted to commission errors (CEs), many of the identified ones actually were CEs. The result was that approximately 20 cases were seen worthy to take into closer consideration in PSA study due to their risk. As examples, calibration errors of electronics and mixing two different grease types of valve drives (leading to a stiffening mixture) may be mentioned.

A large study of human errors in maintenance (Laakso et al., 1998) concludes that most human errors related to maintenance activities are actually commissions. A follow-up study, however, found that even though commissions are many, their consequence to equipment still may be only unavailability. Thus, about 70% of the single human maintenance related errors led to unavailability and the rest to wrong equipment functions/response.

3. What are commission errors?

There are many different definitions for commission errors in literature. The original definition comes from², who define the error of commission as somehow wrong human output i.e. selection error, error of sequence, time error (too early, too late) or qualitative error (too little, too much). For example, references³ ⁴ ⁵ ⁶ and ⁹ have thereafter completed the picture by making more detailed classifications of commission error subtypes. These classifications include add-on features such as premature actions versus alternate actions; intentional versus unintentional actions and global versus local misdiagnoses.

Talking about commission errors should be avoided, if no further definition follows, as stated e.g. by⁴. Instead, it is better to e.g. talk about human failure events (HFEs) leading to system/component function omissions and commissions, the latter called in the following commission opportunities (COs). This may be seen as a systems engineering oriented classification of the ‘commission errors’. The definition covers both wrong human actions and another human error mechanisms (e.g. omis-


sions of actions and normal human actions i.e. triggering events) leading to wrong system response. A wrong human action can result either in active or passive (unavailability) consequence. Active consequences are initiating events and other unanticipated system/component functions. Passive consequences may result e.g. in latent component unavailability.

The Finnish framework concentrates upon identifying opportunities to wrong system functions and quantifying them by using a probabilistic safety assessment (PSA) framework. In the following, the FACE framework is presented. The same framework can be used to study other types of human failure events and actions as well. It is important not to make any firm division between omission of functions and wrong functions as a result. However, here, special emphasis is put on wrong system / component functions as a consequence.

4. A framework for analysing commission errors (FACE)

As a part of the task 97-2, the Finnish regulatory body STUK has awarded VTT Automation a contract to develop a method for commission error analysis as a part of PSA studies. Chapter 4 describes the outline of this method.

The FACE framework consists of the following five phases: selection of human actions that need to be studied; identification of potential commission opportunities (COs) and (wrong system functions) initiating in them; screening commission opportunities (unimportant screened out); modeling the important commission opportunities for probability assessment and assessing the probability. The FACE structure is shown in Figure 2.

![Figure 2. An overview picture showing the main phases of the FACE.](image-url)
Since FACE aims at presenting a framework, some room for details is left. For example, in the identification phase, generic checkpoints and guidewords are given in reference ¹ instead of forcing the reader to use a normative approach. The different phases of FACE are discussed in the following chapters.

4.1 Selection of human actions that need to be studied

The interesting candidate human activities (commission opportunities) in the FACE are seen as events having a major potential to have effect on systems behavior/process safety. They may be selected based on: a) the plant history; b) quantitative PSA criteria or c) qualitative criteria.

The plant history may give an impression both on mechanisms leading to errors and on their consequences (COs). Plant PSA models with high screening values (e.g. 0.5), sensitivity analysis and e.g. risk increase & Fussel-Vesely importance measures may be good starting points for selection of CO candidates, given that the human reliability analysis was comprehensive and credible. If the previous human reliability analysis was carried out only for omission type of human action failure events, it is justified to expect some increase in the human error probability due to the inclusion of commission opportunities. Degrees of freedom of the human task, recovery potential, time windows and estimated consequences can be seen as criteria, if the risk is difficult to assess otherwise during the selection of candidate events.

4.2 Identification of potential COs

The FACE identification is based on systematic mapping of factors that affect 1) potential to human failure event and 2) the possibilities to recover from the failure event. Another starting point is the main context and add-on performance influencing factors (PICs). The main context consists of: a) initial plant state, b) responsible organization and c) position with regard to initiating event (if a credible PSA model exists). Combining the factor a-c and 1-2 leads to, after some merging, 12 basic cases for identification and modeling. Potential combinations are shown in Figure 3. An example of a combination is ‘operating acts after an initiating event during the power operation’, shown in Figure 4.

Figure 3. Different combinations of the organisation, time point in PSA model and plant operating mode used in commission opportunity (CO) identification.

Figure 4. An example of the identification charts (phase II in FACE) for operating acts after an initiating event during outages (screening goes under phase III of FACE)
Deficiencies with regard to the PICs may lead directly to a failure event or then they increase its probability. PICs have to be assessed both for 1) and 2). No human internal PICs are used due to observation difficulties. The major human external PICs credited in FACE are:

1. C₁, the guidance & history stable conditions only: training, instructions, experience, task familiarity, work orders, plant policy / past examples, etc.)
2. C₂, organisation of task I stable conditions: work planning & supervision, layout, access control, work practices, night/day etc. II dynamic conditions: manning/delegation, time windows)
3. C₃, team cooperation etc. (II dynamic conditions (only): communication / information transfer, expectations, decision making aspects)
4. C₄, information context (I stable conditions: information / man-machine interface system type, interlocks, independent inspections, tests, II dynamic conditions: process information; ergonomics)
5. C₅, other contextual factors (I stable conditions: initial state, system & process dependencies, similarities between objects etc. II dynamic conditions: degrees of freedom for human, environmental conditions, system complexity, faults and their effect, action dynamics, other stressing factors etc)

Stable conditions refer to factors that do not change during the assessed event, whereas the dynamic ones may change. These five PIC areas are used as checklists in the identification and as factors in the quantification, later on. Some different guide questions are related to the different combinations of the main context (1-2 and a-c). E.g. for the maintenance originated latent failure event the tests and independent check-ups are important. For a recovery of a misdiagnosis during an accident sequence, the immediate instrumentation and alarm system feedback are more important.

Furthermore, a commission opportunity can take place either in the identification/interpretation, decision making, in manual activities or in communication. Thus, the failure event types related to human performance may be:

A) Misdiagnosing in identification of the situation.
B) Carrying out unsuited action plans (decision or communication unsuited to environment, e.g. coordination errors).
C) Making a slip in a manual action or communication.

Apart from these types, in some cases normal human actions may trigger wrong system functions.

By providing users with simplified flow-charts and decision trees, the idea of FACE identification guidance is to draw attention to important areas and details. FACE also offers practical guidance for each of the human failure event types combined with the main context. The practical identification work has to go to a deeper detail level than presented, e.g. in Figure 4, in order to grasp the essence of the problems and to be able to suggest improvements. Identification of hazards is intellectual activity where guidance has to be put in practice by experienced, understanding and motivated persons. No formal method can compensate for the lack of human effort in the work.

---

4.3 Screening commission opportunities

The screening of important COs takes place in many phases in FACE. In the selection of candidates for COs, a preliminary screening takes place. During the identification phase, a set of plausible COs are chosen for probabilistic study. During the probabilistic modeling phase, the plant data and the contextual factors may show that the probability of the case is so low that there is no idea to put it in the PSA model. If a PSA model is available, it shall be used in each phase to check if further study is sensible. If no PSA model is available, the screening has to be based on other criteria.

The first question related to the screening is if a credible PSA model exists that could be used to support the screening. If the answer is no, the next topic is to check how plausible the recovery is (point 2 in main context). This means the goodness of feedback of critical information, time windows and the diversity & redundancy of check-up possibilities. If the recovery is not seen as utmost certain before consequences, it is required to go to the consequence evaluation. If the system is very tolerant to all kinds of potential human failure events, it is possible to screen them out. FACE gives more guidance for the screening in\textsuperscript{10}.

4.4 Probabilistic modeling

Many human reliability methods have failed because they have either been one-sided (e.g. either psychologically or probabilistically oriented) or too complex to be used in real HRA assessment situations. The FACE has set up the following principles for the probabilistic modeling of human reliability: sound mathematical calculus, transparency, allowance for different types of data, compatibility with identification phase, flexibility and use of contextual factors (PICs) where applicable.

The quantification stems from the two phase model of 1) human failure event birth and 2) recovery. There are three different basic cases in FACE, which are valid for power operation, shutdown and starting up /shutting down the installation):

A) both the failure event causation and recovery are approximately time independent e.g. latent maintenance related failures prior to initiating event,

B) the failure event causation is app. time independent but the recovery is time dependent e.g. human actions causing an initiating event and recovering from it, and

C) both the failure event causation and recovery are time dependent e.g. human failure in an action after an initiating event in an accident scenario.

Many PICs affect both processes human failure event birth and recovery. Apart from the C\textsubscript{1-3}, listed previously, time dynamics have to be taken into account in the cases B and C. As well, the detailed factors under the C\textsubscript{1} and C\textsubscript{2} are somewhat different in different main context combinations. All kinds of failures in the recovery phase are seen to lead to recovery failure (no specific commission type of effects are assumed for failed recovery).

The probability of an unrecovered human failure event \(p_{\text{u/f}}\) is calculated in formula (1):

\[
p_{\text{u/f}} = p_{\text{u}} * p_{\text{rec}} \quad (1)
\]

, where $P_{\text{lu}}$ & $P_{\text{re}}$ are human failure event and unsuccessful recovery probabilities, correspondingly.

In order to make the selection of modeling detail level flexible, three different quantification alternatives are under development in FACE. They are not way limited to the assessment of probability of commission errors. Rather, they are generic probabilistic modeling frameworks that may be applied to human reliability. The two main alternatives are:

1. Multiplicative PICs based quantification model
2. Multiple factor (PICs) logit quantification model

All these quantification methods make use of expert judgement, that has to be organized in a structured way to obtain credible results, as discussed e.g. by \(^{11}\) and \(^{12}\). The modeling complexity level increases from the first to the second one. Method number one may provide a quick way to get a coarse view on the order of magnitude and, thus, may be a tool for everyday PSA use. Method number 2 provides a better framework to study the relevancy and effect of various PICs to the probability. There are also thoughts about developing a Bayesian quantification model taking into account several different kinds of evidence.

The Bayesian one would require advanced stochastic tools to be used. Its advantage is the elegant use of different kinds of pieces of evidence such as historical, simulated and expert judgement data. Method number three is not discussed in this paper further.

4.4.1 Multiplicative quantification model

Multiplicative models have been used to update generic data to present plant conditions. The probability assessment is performed by using generic a priori ($P_{\text{gen}}$) probabilities and updating them with expert judgement data. The generic probabilities mean: a) per demand generic probabilities for human failure event causation in all conditions and for recovery in cases where an initiating event has not taken place or b) generic time-reliability data in the case that the recovery after an initiating event has taken place.

We may write a formula 2 for the calculation of a plant's specific estimate based on a generic a priori estimate by using the PICs mentioned earlier:

$$P_{\text{plantX, j}} = P_{\text{gen i, j}} \times \Pi C_i$$  \hspace{1cm} (2)

where $X$ = code of the event, $i = 1,2,3,4,5$, $C_i = \text{PIC i and } j = \text{fai, rec.}$

The first phase of applying the method is to define the a priori estimates. For different types (A-C) and their combinations, e.g. the following a priori point data may be used:

A) value $P_{\text{gen, fai}} = 0.01$ for human failures in pre IE actions\(^{13,14}\) and $P_{\text{gen, rec}} = 0.03$ for failing recovery\(^{15}\).


B) value $p_{\text{ext},B} = 0.01^{16,17}$ for human failures and the estimate for failing recovery e.g. based on Swain's or OAT time reliability correlation and modifying PICs factors (Ci).

C) Time dependent reliability (e.g. Swain's, OAT or other generic time reliability correlation with correcting Ci factors) for human failure events and for failing recovery.

The $t_{\text{gen}}$ that is used in the calculation of $p_{\text{gen}}$ in cases B (for recovery only) and for C is based on the total physical time available $t_{\text{tot}}$ (from success criteria); on time $t_{\text{del}}$ from the initiating event to the first critical alarm or other indication showing the need to act on a safety function and on time required for the actual manual actions $t_{\text{act}}$. The $t_{\text{gen}}$ may be easily calculated from the formula 3:

$$t_{\text{tot}} = t_{\text{gen}} + t_{\text{del}} + t_{\text{act}} \quad (3)$$

where $t_{\text{gen}}$ means time for identification and decision making.

The next phase in FACE is, defining PICs (C_i). This has taken place already as a part of identification but some revision may be required. The evidence on PICs influence come either e.g. from simulator training or, most often, from expert judgement reflecting the most important factors present. Thus, the next step is to select the expert team to give assessment of the levels of the C_i's for the formula (2). The factors C_i get e.g. values between [0.2 to 5]. Either use of some classes e.g. [0.2, 0.5, 1, 2, 5] or all the real values in that interval are possible. FACE gives guidance in defining the C_i's and their levels. The analysis flow by of the multiplicative model is shown in Figure 5.

---


Figure 5. Flow of quantification by using the multiplicative model.

The interpretation of factors $C_i$ is that they partly affect directly the success probability (e.g. availability of right tools) and partly they affect mental burden (stress).

Different expert judgements are combined e.g. directly or by considering them as independent multinomial samples. The latter leads to a Bayesian Dirichlet uncertainty distribution. Another way to assess uncertainties would be to ask the experts to express their uncertainty bounds with regard to the factors directly, and let the uncertainty then propagate in the model.

Multiplicative modeling approach is simple and a reduction in human failure event probability is obtained through improving contextual factors $C_i$. Thus, the approach is suitable for risk management and daily coarse HRA work. With the simplistic structure there is, however, a danger of hasty conclusions. Thus, use of the model has to be accompanied with a good qualitative analysis and documentation supporting the conclusions drawn.

4.4.2 Multiple factor (PICs) logit quantification model

Logistic regression (logit transformation) is a widely used technique to model a regression of a number of factors with known upper and lower bounds. In the probability applications, those limits are 0 and 1 leading to the formula (4). The underlying model of probability is binomial - certain factors have influence on the probability of outcome, the set of possible outcomes being dual.
The logistic regression on a random variable $p_{def}$ may be based on the equation 4:

$$p_{def} = \frac{e^{\sum_{i} w_i C_i + C_0}}{1 + e^{\sum_{i} w_i C_i + C_0}}$$

in which $C_0$ is in our case a constant, $C_1, \ldots, C_n$ are PIC factors that influence the probability and $w_1, \ldots, w_n$ are their weights.

As shown in Figure 6, the first phase for the multifactor logit quantification is to classify the case into the basic types A-C, as for the multiplicative model. The next phase is to define the PICs (mostly the $C_5$ stem from the identified important PICs) and the measures or indicators that describe them. As a regression model cannot regard time as a specific variable (as was for the multiplicative model), it has to be taken into account as e.g. variable $C_v$.

![Figure 6. Multiple factor (PICs) logit quantification model flow chart.](image)

After the PICs and their indicators have been defined, it is time calibrate the logit model. In the generic probability case, as in formula 4, they are 0 and 1. Next, plant or generic data should be collected to support quantification of PIC effect. This data may be used to aid expert judgement elicitation. If there are cases with known combination of variables (e.g. probabilities collected for some specific maintenance error or human action on simulator with separately defined PICs), they should be used as calibration data.

The next step is to select the expert team and design the elicitation of data to obtain a sufficient amount of data points for the regression model. If 5-6 variables are used, this normally requires more than 20 data points to ob-
tain a reasonable confidence for the parameters w and C. Generally, it is desirable to use more than one expert. The experts should preferably represent different disciplines in order to get more views about the topic.

The idea is to then elicit directly probabilities for certain combinations of PIC factors C with calibrated upper and lower bounds. For example, if class variables are used, e.g. C ∈ {1, 2, 3, 4, 5}, a typical question is to assess a probability for variable levels C₁=1, C₂=2, C₃=5, C₄=5, C₅=1 and so on. Direct probability judgement deserves expert training e.g. in probability concept, as discussed e.g. in 19. Combination of different assessment is planned e.g. to take place by averaging.

The calculation of the correlation parameters w and C takes place by using maximum likelihood principles. Then, significance testing is carried out to find out the relevance of the variables. The uncertainty in the parameters is obtained in an integrated way via fitting the parameters w and C. Most software packages also calculate directly the 90 % uncertainty interval.

The model is slightly more complicated than the multiplicative one. However, it allows for e.g. maximum likelihood fitting of the model parameters and statistical testing of the significance of the variables. The problems are the generic scarcity of observable data and finding objective measures for the independent variables. If such objective measures can be found, they may not be valid e.g. a high amount of instructions and alarms/indications is not good alone if their contents does not help the personnel.

5. Conclusions and remaining tasks

Generally, HRA methods should be generic rather than developed for one subset of events, such as ‘commission errors’ only. HRA has to fit in the generic systems analysis framework of PSA. This means that only important human actions are analyzed in a detailed way. Application of the methods should be multidisciplinary rather than put in practice by psychologists or reliability engineers only. This is due to the interdisciplinary feature of the problems studied.

So far, FACE has been created only on a generic level 20, although it partly goes to very detailed questions e.g. for identification. Applications are required to be able to better evaluate the strengths and weaknesses of the method. This part is planned to take place during the fall 1999 – winter 2000. Report one the application would, thus, be available in mid 2000.

---


1. **Introduction**

In France two PSAs have been completed in 1990: one by IPSN for a 900 MWe standardized PWR (PSA900) and the other by EDF for a 1300 MWe PWR (PSA1300).

In these studies a particular attention was paid to Human Reliability Assessment (HRA), especially due to the high contribution of human intervention in the overall results.

The approach which relies as far as possible on experience feedback allows to account for some errors of commission (EOC). The following chapters describe the general approach and examples of application to EOCs.

2. **General Approach**

2.1. **Introduction**

The approach used was common to PSA900 and PSA1300. It has been developed by EDF and discussed with IPSN.

This HRA method has been developed on the basis of earlier work, especially THERP methodology. However, substantial adaptation was required before this method could be applied to the French PSAs.

In particular, the greatest importance was attached to experience feedback, the only proper basis for realistic analysis. Experience feedback was essentially used to:

- identify potential errors
- quantify their probability by direct statistics when the situation studied corresponds to observed cases
- create models making it possible to extrapolate from experience to other situations

The main sources of information were real incidents, ad hoc interviews and investigations, and observations made by EDF during simulator tests. Simulator tests constituted a particularly rich source of information.

Human intervention explicitly allowed for in the PSAs can be divided into two main categories: pre-accident errors and intervention in accident situations.

Since EOCs belong to the second category, the method will be described only for this type of human intervention.
2.2 Human Intervention in Accident Situations

This category includes both intervention of the diagnostic and decision making type, and the taking of action.

In addition, the role of the operating team, the role of the safety engineer and the action of the emergency teams were distinguished and processed in a different manner, in order to represent the manner in which operation in an accident situation is organized, particularly the human redundancy provided by the safety engineer.

2.2.1. Operating Team Role

The activity of the operating team has been divided into two phases: diagnostic and operation.

The diagnostic phase includes detection of an incident, making the diagnostic and taking a decision (selection of a procedure or strategy). All these operations have been quantified using curves giving the probability of failure as a function of the time available to the operators to take the action.

These curves, which correspond to an easy, an average and a difficult situation, where prepared on the basis of simulator tests, supplemented by engineering judgement, making special use of the work of Swain.

Operation in accident situations can be represented by a list of key actions, whose success or failure modifies the accident sequence. In the event of failure of the diagnostic, it is generally considered that key actions are not performed. In the event of success of the diagnostic, the corresponding actions may fail (omission, mistakes or error of commission). For each important action, the failure probability is evaluated as follow:

\[ P = P_b \times K_j \times P_n \]

Where:
- \( P_b \) = the basic probability estimated at 6*10-2 (test on simulator)
- \( K_j \) = context factor equal to 1/3, 1 or 3 depending on whether the circumtances are favorable, average or unfavorable.
- \( P_n \) = probability of non-recovery, estimated using elements favorable to recovery (signal, explicit redundancy and time available).

It should be noted that these models are only used when there are no direct statistical values referring specifically to the situation analysed.

2.2.2. Safety Engineer Role

Safety engineer intervention was considered to represent recovery of degraded situations by application of specific procedures. It was assumed that the safety engineer would not play a role in the diagnostic and the actions taken by the operating team.

The probability of failure of the safety engineer is the sum of two terms:

- Probability of absence of the safety engineer from the control room (estimated by EDF using simulator tests and on-site investigation).
- Failure probability of the specific procedures, for which the values adopted were 0.05, 0.1 or 0.3 according to the procedure and to the time available.
2.2.3. Emergency Team

It was postulated that the local emergency team would be operational four hours after the start of the accident. Strategy errors beyond this deadline were not allowed for. However, allowance was made for non-recoverable execution errors.

3. Application to EOC

The EOCs introduced in PSA900 and PSA1300 were identified by help of experience feedback.

A first category of EOC was identified by a systematic analysis of the possible inappropriate termination of safety systems by the operators. This analysis was originated by the TMI accident. The example of the inappropriate termination of Safety Injection in case of small LOCA is described below.

Another category of EOC was identified during simulator experiments. This category is illustrated by the inadvertent isolation of SG relief valve in case of SGTR.

The examples below are drawn from PSA900, but the treatment in PSA1300 is similar.

3.1. Inappropriate Termination of Safety Injection

3.1.1. Identification

Considering the experience of TMI accident, a systematic analysis of the possible EOCs leading to the loss of a safety system was carried out. This analysis identified in particular the possibility for the operators to shut-off the safety injection (SI) system in case of small LOCA. If this EOC is not recovered in time, it leads to a core-melt.

3.1.2. Quantification

After a small LOCA the operators take the Emergency Operating Procedure (EOP) related to small LOCA. In this EOP the operator has to follow a diagram corresponding to the SI operation. In order to go to an inappropriate SI shut-off, the operators have to make at least two mistakes when reading the diagram. There are several favorable recovery factors: explicit redundancy between the operators and time available > 30 minutes. The safety engineer can also recover the situation, since the SI operation is also an action of his specific procedures.

Quantification was carried out following the general HRA method described above for the failure of execution:

- Probability of the first error = 6*10^{-2}
- Probability of the second error = 0.15 (medium dependency)
- Pnr = 0.1 (explicit redundancy and time > 30 minutes)
- Non-recovery by the safety engineer = 0.06 (60 minutes)

Result: EOC probability = 5.4 \times 10^{-5}

3.2. Inappropriate Isolation of Steam Generator (SG) Relief Valve

3.2.1. Identification

In case of SGTR a key action for the operators is to isolate the affected SG. For that purpose the EOP requires several actions (isolate the feedwater line, isolate the steam line, change the set-point of the relief
valve in order to avoid an opening of this valve...). An error can be to isolate the relief valve in place of changing the set point: in this case there is a risk of opening the safety valve which is not qualified for water discharge and can remain stuck open. The SG cannot be isolated and this can lead to a core melt sequence.

This EOC has been observed during simulator tests. The * error forcing context + was mainly due to a * series effect + : the EOP requires to close several valves and to change the set-point of the safety valve. The operators closed also the safety valve. It has to be noted that after the simulator tests the EOP was improved.

3.2.2. Quantification

Since this EOC has been really observed during simulator tests, the probability can be assessed by direct statistics.

The EOC probability is 0.2.

4. Conclusions

These examples illustrate the fact that some EOCs have been introduced in the French PSAs following two methods:

- A provisional approach based on the analysis of EOPs.
- An experimental approach based on simulator tests.

Although it was a first step towards a more realistic treatment of HRA, several limitations can be identified:

- The provisional approach is not validated by experience and the results are very uncertain
- The experimental approach gives more realistic results, but it can be used only for very frequent events, and moreover the root causes of the error are not modeled and the effect of a modification cannot be simply assessed.

These considerations underline the need for the development of new approaches. However, the interest of simulator tests is also a finding of these studies.
Contribution from France
MERMOS

Pierre Le Bot
Electricité de France, France

1. Description of the method used to analyze errors of commission

1a. Statement of purpose and scope

MERMOS is a Human Reliability Assessment Method. In French, MERMOS\(^1\) stands for "Méthode d'Evaluation de la Réalisations des Missions Opérateur pour la Sûreté ", which in English means "assessment method for the performance of safety operation." MERMOS is an improvement of EDF's previous HRA method and is designed to guide EDF's analysts in taking human factor aspects into account in the future PRA for units of the N4 series.

Scope:

- the PRA is generic for the four N4 units. The reference plant is Chooz B1.
- emergency operation during the four hours after the initiator (since it is assumed that the Emergency Crisis Team will then carry out emergency operation)
- the Man Machine Interface (MMI) is the computerized N4 Control Room
- Emergency Operating Procedures (EOPS) are computerized and they are designed with State-Based Approach type (what we call "generalized APE")

1.b. Underlying concepts

Human Factor Mission

Since HRA methods have to fit into the framework of PRA models, the interface between the two plays a critical role. For each initiator, a functional analysis will determine the "missions" that have to be performed to recover or mitigate the accident. Failures of one mission or several consecutive missions lead to unacceptable consequences. Among the missions, Human Factor missions (HF mission) refer to safety critical actions that the operating system, comprising the crew interacting with the procedures, the systems, the organization and the layout, has to initiate and carry out to handle the situation. This concept constitutes the interface between PRA and HRA.

HRA Purpose

The purpose of HRA is to assess the failure of HF mission. Finding how the failure can occur is a specific objective. Currently the expected operation is described first, and it is then assumed that failures occur since the crew deviates from this path. We think this biased method is not the right one: paths to failure have to be analyzed directly. The analysis should proceed from the failure backwards and not from the initiator forward using the prescribed path as a model.

\(^1\) Le Bot, C. Bieder, F. Cara & J.L. Bonnet: MERMOS, an EDF project to update Human Reliability Assessment methodologies, ESREL 98, vol 2 p. 767
Emergency operating system and SAD model

MERMOS considers that the performance of HF mission is the responsibility of a system we call Aemergency operations system (EOS). This system comprises the operating crew, EOPs and MMI (called KIC for the N4 control room) plus the formal organization and the workplace. The actions required to perform a HF mission are initiated in the control room by the operators, according to a predefined division of labor, using EOPs, prior knowledge, the information and the commands available on the interface.

The model of the EOS developed specifically for the purpose of MERMOS is named SAD, which stands for Strategy, Action, Diagnostic, for these are the three functions involved in the performance of HF missions. The three functions, which do not necessarily work in sequence, have to all be efficient to perform the mission. SAD allows to analyze the failure of a HF mission systematically through the dysfunctions of each of these EOS functions.

The computerized control room, because of the tight coupling it creates between operators, on screen EOPs, advanced MMI, makes the separation between operators and technical actions even more difficult and requires this broader, more systemic view of HF.

Human error

The failure of HF mission is explained in terms of the dysfunctions of the EOS, and not by human error. Cognitive failure mechanisms at an individual level alone are not sufficient to generate HF mission failure, but can instead be among the contextual features, together with other system components properties, that contribute to the HF mission failure. Instead of assuming that human error is a decisive element of failure per se, it is embedded within EOS as one of the determinants of ineffective performance.

CICAs and situation

The actual functioning of the system is modeled with the help of a new concept, named CICA (Important Characteristics of Emergency Operation). CICAs refer to particular ways of operating the plant adopted by the EOS in the course of the emergency situation. It takes into account organizational aspects such as task prioritization or distribution among people and systems. We know, in fact, from observation made in full-scope simulators that even with very detailed and precise procedures, operators still enjoy a certain degree of autonomy to organize the operations with respect to these procedures. Nevertheless, we also know that this autonomy is exercised within a stable, designed system, which defines effective guidelines and powerful constraints for action.

The CICAs have nothing to do with failure modes or error mechanisms or anything intrinsically negative. Basically, CICAs correspond to positive ways of operating the plant and capture EOS global functioning over time. In some contexts, however, CICAs may prove to be inadequate.

Because they are defined at a system level and are extremely contextual, CICAs are not necessarily conscious in the mind of the crew members. The situation as it is defined in the MERMOS method comprises the reasons leading the crew to operate in a certain way, as well as the reasons for which the operating choices are likely to lead to the failure of the HF mission. Features of situation come from what could happen before and during the mission, such as, for example minor equipment failures. Failures of the sensors necessary to deal with the HF mission are systematically addressed as potential elements of situations leading to the failure (analyst has to find out how - given that situation - CICAs that could lead to a mismatch with safety requirements can occur).
Example:

- The crew may rely on the computerized console to monitor certain parameters while focusing on other phenomena. This is a CICA.
- The crew may suspend a decision, waiting for the recovery of a system. This is also a CICA.
- An operator erroneously stops a pump. This is not a CICA, this is an individual error, considered by MER莫斯 as an event that builds a feature of a situation.
- The crew decides to start a pump. This not a CICA, this is an action, considered by MERMos as an event that may constitute a feature of a situation.

Recovery

Tests on simulator have shown that individual failures:

- occur whatever training the operator have or however sophisticated the interface design may be
- are of no consequences most of the time
- or are recovered very quickly, by the operator himself, with the help of computerized procedures, by the other members of the crew, or by corrective operation required by the state-based procedure since thermo-hydraulic parameters have changed.

No HF mission failure has been observed due to lack of redundancy. Therefore we think there is no special mechanism to refer to as an explanation of failure of HF mission. The mechanisms used by the emergency operation system that could lead to failure are the same as these that could lead to success (in other words, nothing abnormal in itself, but abnormality given the condition, ex. the rigidity can contribute to very adapted operations in some situation, and to less adapted operations in other situations).

They are described by the CICAs. A combination of CICAs can be stopped by a re-organization, generally as soon as the situation changes. For example, focusing on a parameter can be stopped as soon as the crew has to deal with a new problem.

Failure scenario

Many different paths lead to failure. A failure scenario is one of these paths. It shows how the failure can occur.

The aim of the MERmos qualitative analysis is to identify all possible scenarios leading to the HF mission failure. The dysfunctioning of the EOS is broken down into the dysfunctioning of each of the three functions Strategy, Action, Diagnosis, with respect to the role each plays in the execution of the HF Mission.

Each function can dysfunction according to several generic failure modes. The analyst is guided in the process of envisaging all possible failure scenarios.

A scenario is detailed enough to relate to real operational settings, but not too detailed so that the elements it refers to are likely enough and can therefore be quantified. A failure scenario can be explained by a combination of CICAs and a certain set of external circumstances, which in turn can be explained by features of a situation. A CICA is a type of EOS functioning emerging out of EOS features, some of
which refer to external circumstances, like the particular shape the process evolution takes). Each
individual situation feature is likely to be encountered either on simulator or on site. Thus, they can be
easily assessed, either by statistical calculation or by expert judgment.

Prescribed aspects versus required aspects

We think that the dysfunctioning of a system cannot be directly deduced from an analysis of its expected
functioning: to consider that it is dysfunctioning as soon as it deviates from the prescribed operation is a
bad shortcut. A specific reference has to be defined in order to characterize the dysfunctioning of a
system. This reference is the PRA point of view that defines required actions (or forbidden actions) in
certain circumstances. From this viewpoint, all the events are known from the initiator. For example, it
can be known in a given PRA sequence that an auxiliary system won’t be recovered, and therefore to
recover the system is not required, but from the prescribed procedure point of view, it is always necessary
to try to recover the system.

1c. Steps of the method

The method is divided into two modules in order to comply with EDF organization constraints. The first
one is dedicated to the identification and definition of the HF Missions modeled in PRA. The second one
is concerned with the analysis, both qualitative and quantitative, of HF Missions.

First Module: Identification and definition of the HF Missions

General process:

This task is carried out by PRA analysts, with help from HRA analysts if necessary. The starting point is
the initial event tree defined for an initiator. The first module of MERMOS provides HRA analysts with a
description of HF missions of the analyzed sequence. From a functional analysis of the state of the plant
after the initiator, the analyst describes the characteristics of each HF missions and their context in a
standard form. In practice, feedback from PRA shows us that functional analysis cannot be carried out by
itself. It is necessary to verify it and enrich it with elements from other information sources such as
Emergency Operating Procedures and Simulator tests feedback.

Let us give an example of how the method works, based on one initiator: a stuck-open PORV on the
pressurizer (when the plant is running at full power).

Functional analysis makes it possible to define how to mitigate the accident or recover the situation. The
analysis is carried out with respect to the Safety Functions. Safety-important systems required by the
situation are identified. In our example, as long as the primary pressure is high and there is a leak, water
injection is needed to preserve the reactor coolant inventory.

At this step, the HF mission could be defined in a positive, general way: start the safety-important
systems if needed and keep them functioning.

Let us now examine the branch of the event tree where Safety Injection pumps are automatically started
and are running well: the situation requires that they be kept operating for a sufficient time after the
initiator. Thermo-hydraulic studies show that during this time they must not be stopped for more than one
hour. It follows that one important HF mission is the safety injection pumps must not remain stopped for
more than one hour.

The identification of HF missions is then supplemented by complementary analyses of procedures and
simulator tests.
Second Module: Qualitative and Quantitative Analysis of each HF Mission

The emergency operation system in charge of the performance of the HF missions was determined in order to allow the analysis of the failure of a HF mission as a manifestation of the dysfunctioning at the system level. Since the system is modeled in a functional way, the dysfunctioning of the system can be analyzed at the level of each of the S.A.D. functions. The analysis thus proceeds function by function with each function potentially dysfunctioning according to (not both) modes. For each of them, the analysis consists in identifying and then quantifying all the failure scenarios that can lead to the failure of the HF mission. The analysis is divided up into five steps.

Step 1
The input data are the HF missions (defined through module 1) worded as macro-actions that are to be taken by the crew for a given PRA sequence within a time window. These actions are meant to maintain or restore required safety functions. Since the requirements are considered as the reference for the analysis proposed in the MERMOS method, the purpose of the first step is to identify the safety functions that are affected, the possible functional responses, the associated operation objectives, and to determine whether specific means are to be used. Each HF mission is at first analyzed separately, the integration into PRA event trees being performed once all the HF missions have been analyzed.

Example
- Safety function: maintaining the reactor coolant inventory
- HF mission: not switch off of the SI pumps for more than one hour
- Functional response: maintaining at least one SI pump in service
- Specified means: not switch off of the SI pumps before the primary temperature reaches a certain threshold
  restart the SI pumps if the vessel level reaches a certain threshold

Step 2
At this point, the safety requirement corresponding to the HF mission is too general to carry out any detailed analysis. Step 2 aims at breaking it down according to each of the SAD functions: what does this requirement mean from the respective points of view of the Strategy, Action and Diagnosis functions? The completion of these two first steps yields a detailed characterization of the HF mission in terms of what is required from a strictly safety and thus PRA viewpoint.

Example
Requirement from the point of view of the **Strategy**:
Give priority to maintaining the reactor coolant inventory

Requirement from the point of view of the **Action**:
No action / Restart of the SI pumps if needed

Requirement from the point of view of the **Diagnosis**:
> State: being aware that keeping the SI pumps switched on is necessary to maintain the water inventory and to comply with the saturation margin
> Situation: foreseeing the impact of switching off the SI pumps on the water inventory and on the saturation margin

79
Step 3

This is the most important step of the analysis. Its purpose is to imagine as many failure scenarios as possible by bridging the gap between theoretical concepts and real data. At this point in the analysis, failure scenarios can be predicted through a deductive approach. In addition, the analyst adopts an inductive approach starting from available site or simulator feedback data. Since the functioning of the EOS has been characterized through both the CICAs and the situation concepts, a framework exists to structure and use these data. In short, the CICAs refer to dynamic modes of organization within the EOS that are basically positive but may prove negative in a very specific situation. The situation includes features of the process, of the crew and of the procedures through time. The inductive approach consists in building failure scenarios on the basis of relevant situation features or CICAs observed on simulator or identified by experts, and then in enriching them with the associated missing elements (either additional situation features or CICAs or other). The identified failure scenario is then related to a failure mode of one of the S.A.D. functions. The qualitative analysis materializes in a table as shown through part of the qualitative analysis of the exemplified HF mission. (See Table 1.)

In order to help the analyst carry out this analysis, he is given a database including a complete qualitative analysis for each of the major kinds of HF mission modeled in PRA.²

Step 4

Quantification in the MERMOS method is based on the output of the qualitative analysis. No a priori assumption is made with regard to the respective weights of the various identified scenarios. A residual probability is used to cover the scenarios that couldn’t be imagined by the analyst. Should the occasion arise, dependencies between situation features or CICAs, or consecutive HF missions are taken into account in this step. The completion of quantification relies on the statistical data collected based on observations on simulator/site as well as on expert judgment. A specific method, named RETADE, has been developed for the purpose of MERMOS in order to collect and aggregate expert judgment.

Step 5

This final step consists in ensuring the consistence of the results and in integrating them into PRA event trees.

<table>
<thead>
<tr>
<th>Function</th>
<th>Failure mode</th>
<th>Safety requirement</th>
<th>Mode of non-compliance</th>
<th>Failure scenario</th>
<th>CICAs</th>
<th>Situation Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnosis</td>
<td>Wrong diagnosis</td>
<td>The HPSI is necessary to maintain the water inventory</td>
<td>The water inventory is seen as adequate</td>
<td>The crew doesn't start again the SI pumps after stopping them accidentally for the water inventory is seen as adequate.</td>
<td>Going through the procedure step by step</td>
<td>The RO stops accidentally the SI pumps (e.g., test error). Wrong information on the vessel level available to the RO. The supervisor and the SE have the same information as the RO.</td>
</tr>
<tr>
<td>Strategy</td>
<td>Wrong strategy</td>
<td>Priority to maintaining the water inventory</td>
<td>Priority to depressurizing</td>
<td>The crew wants to restrict the increase in pressure and the releases within the containment and decides to limit the flow leaking through the breach by switching off the SI pumps</td>
<td>Anticipation of a further operation objective Focus on the control of the containment</td>
<td>The crew thinks the water inventory is correct. Sharp increase in the pressure within the containment. SE not in the CR or follows the strategy of the crew. Supervisor follows the strategy of the crew.</td>
</tr>
</tbody>
</table>

Table 1. Example Application
2. Event or sequence analyzed

See example provided in Table 1.

3a. General findings

At this point in time, the application of the MERMOS method is used for N4 PRA.

We have worked with requirements rather than procedures as a normative reference, we have gone beyond a negative view of the operators, and, within our EOS analysis, we have accounted for collective and dynamic aspects of operations.

The formal breakdown of the qualitative analysis actually requires much expertise and a great deal of work. The HF mission database we are building will make available the results of the detailed work we are carrying out to HRA experts and become an organizational learning tool for analysts to have access to the expertise of other specialists, and to build their own analysis from slightly different sequences.

Moreover, the level of detail into which MERMOS goes makes it possible to point out critical aspects with respect to safety. Its findings can easily be related to specific features of the interface, of the procedures, or even of the crews. The outcome of the qualitative analysis may thus have repercussions on the plant operation in a broad sense.

Thanks to its level of detail as well as its structure, the MERMOS qualitative analysis constitutes a rich source of information that goes beyond the purpose of HRA.

About the data:

It appears that actual events and tests on simulator provide analysts with very few examples of HF mission failure. Thus a cognitive model is necessary to extrapolate from observation to prediction of failure. CICAs and situation features, including individual errors, are important elements of our model that could be observed on simulator, and then quantified. These elements must be completed with expert judgments. The level of breakdown of MERMOS makes it possible to use combinations of significant elements with high probability (0.01 to 1), that are more easily assessed by experts.

3b Findings about errors of commission

Since MERMOS doesn't use a taxonomy of Human Errors to identify, analyze and quantify HF mission failure, distinction between commission errors and other types of human errors is not relevant in our method. Only individual minor errors that we can assess by tests on simulator need to be taken into account. The problem of errors of commission (EOCs) is shifted to the identification and the description of the Human Factor mission. But instead of a problem about Human Behavior understanding, it becomes a question about PRA event tree definition and functional analysis of the plant.

This may be the explanation of EOC. At the system level, EOCs appear as orientations that the EOS takes diverging with respect to required actions.
Additional References


Contribution from Germany:
CAHR Method

Oliver Straeter
Gesellschaft fuer Anlagen- und Reaktorsicherheit (GRS), Germany

1. Introduction

In September 25, 1997 the PWG5 Task 97-2 decided on a meeting in Paris to exchange methodological insights into research of the member countries on human errors of commission. Three general goals were identified:

1) to develop insights on errors of commission;

2) to apply methods for the quantitative and non-quantitative analysis of errors of commission; and

3) to identify data needs.

It was agreed that during the first phase of Task 97-2 those countries participating in the task would select an analysis method, of their own choice and provide written descriptions of either complete analysis methods or preliminary / initial methods that are able to be applied on the analyses of operational events or cases.

This paper describes an initial method that was developed at GRS in the framework of a Ph.D. study together with the Institute of Ergonomics of the Technical University of Munich (Prof. Dr. Heiner Bubb). The method is currently under further development.

The information contained in this paper is a synopsis of different publications since 1993 on this method and its development (Sträter 1993\(^1\) to 1999). A more detailed treatment of the aspects presented here is provided in a paper that is being published in “Reliability Engineering and System Safety” in 1998 together with Prof. Dr. Heiner Bubb. Many of the basic ideas within this paper are also based on the previous works in PWG5 concerning critical operator actions and data issues and also on the recent publication of the EARTH-group (Mosneron-Dupin et al., 1998)\(^2\).

This contribution describes the method on the level of the Ph.D.-study. Currently, the method for analysis and its results concerning error mechanism, cognitive aspects and organizational insights are

---


adapted by GRS in order to achieve an improved method for evaluation of events regarding HF-issues and PSA (Probabilistic Safety Assessment). It is also currently further elaborated in achieving more insights into the quantification part of the method and a better analysis and assessment of cognitive and organizational aspects. This paper will reflect the basic ideas of the method on the level of the Ph.D. study and some ongoing work.

1a. A Statement of the Purpose and Scope of the Method Used in the Analysis

In this paper, the CAHR-method is introduced. CAHR means “Connectionism Assessment of Human Reliability”. The term “connectionism” was coined by modeling human cognition on the basis of artificial intelligence models. Connectionism is a term of artificial intelligence describing methods that represent complex interrelations of various parameters (known for pattern recognition, expert-systems, modeling of cognition). By using the connectionism idea, the CAHR-method attempts to consider that human performance is rather affected by the interrelation of multiple conditions and factors (of internal as well as of external nature) than by singular factors that may be treated isolated (cf. Rasmussen, 1986). By this, it enables to represent and evaluate dependencies and context on the qualitative side and suggests to consider HEP always as driven by human abilities and the difficulty of situation.

The method consists of several steps: (1) a structured framework for data collection, (2) a method for qualitative analysis of the collected data, and (3) a method for Human Reliability Assessment. Basic ideas of the method are:

- Operational experience about human failures and human performance is an indicator for human reliability in accidents (that are usually assessed in PSA). This holds for cognitive errors as well as for others (like organizational aspects, skill- and rule-based errors)

- Human failures and human performance are usually a result of multiple factors and mechanisms and are affected by an interrelated set of several internal and external factors that have an effect on human reliability by their interrelations (i.e. context).

- Simple error models are not realistic, because human performance is depending on multiple relationships between PSFs and errors and context. Dependencies between failures, PSFs and situational characteristics have to be considered in HRA (Human Reliability Assessment). In CAHR this is considered by the connectionism approach for evaluation.

- Human failures are to be treated guilt-free in order to enable understanding and analyzing them. Human failures always have to be seen in relationship to the successful performances of humans in technical systems.

1b. A Summary of the Steps Taken or the Procedure Used for Conducting the Analysis

In this section, the method will be presented which was found as one possible solution to identify errors of commissions as well as the factors that are influencing them. It supports root cause analysis in the evaluation of events and the description of human failures with respect to HRA purposes (i.e.,

---

qualitative analysis of error prone situations and quantitative assessment) as well as evaluation of a set of collected events. It consists of two basic steps:

- Structured framework for event evaluation and data collection
- Evaluation of collected events for generating extensional statements

1b.1 Structured Framework for Event Evaluation and Data Collection

The basic idea of the approach for event evaluation and data collection is a detailed analysis of the information flows that were important in an event (for detailed description of the whole method see Sträter, 19974; descriptions in Sträter, 1993-1998). Figure 1 provides a general overview about the event analysis procedure.

![Diagram of event analysis procedure](image)

Figure 1: Overview about the event analysis procedure of CAHR.

The approach presented in the following is a bottom up approach. The method first performs an event analysis consisting of the following steps:

- Event decomposition

---

• Detailed analysis of human failures
• Analysis of cognitive demands
• Description of improvement measures

1b.1.1 Event Decomposition and Organizational Aspects

In the first step, it is necessary to decompose the event into the relevant occurrences that are of importance to understand the event. For this purpose, a sequence diagram of the involved MMS-units is used as outlined in Figure 2.

![Event Decomposition Diagram]

Figure 2: Event decomposition into different MMS-units.

In the event decomposition, a complex event is broken down into different error and recovery situations. For the detailed analysis of human failures a generic framework called MMS (Man-Machine System) is used to describe the human interactions and failures (omission or commission), important conditions of the working environment, and PSFs.

Within the figure, three major parameters are used for decomposition that may also be used to assess dependencies: (1) The place where the action took place, (2) the involved persons and (3) the situation of the action given by different action types. While the first two points are directly given by locations and involved persons, the last point is based on a classification of human actions by IAEA-
However, an investigation of 165 events showed that the IAEA-classification has to be extended by further action types.

For classifying the situations, the following types of human interactions are distinguished:

- **Type A0**: This type is characterized by human interactions, where personnel have performed its work as planned. Therefore, in these actions there was no error in the action itself but the action was a necessary condition for an error that occurred at the same time or later in the event sequence (e.g. the "error-free" part of two interfering maintenance actions).
- **Type A**: All actions before the initiating event leading to latent failures (as in IAEA, 1995)\(^6\).
- **Type Ba**: This type describes actions performed as intended but resulting in an initiating event due to previous errors of Type A actions (i.e. the come-out of a latent failure).
- **Type B**: Initiating event actions as defined in IAEA (1995)\(^7\).
- **Type Cr**: Recovery actions similar defined to IAEA (1995)\(^8\).
- **Type Cd**: Actions deteriorating the situation (similarly defined as in IAEA, 1995)\(^9\).

Note, that there is no distinction of Type C actions performed with or without procedures. As discussed in Sträter (1994)\(^10\), deterioration of a situation may occur with using procedures (planned) as well as without (unplanned).

### 1b.1.2 Analysis of the MMS-Units

For each defined MMS-unit, a detailed analysis has to be performed. The framework for detailed analysis is based on the MMS (Man Machine System) approach (see Bubb & Schmidtke, 1993)\(^11\). The reason for subdividing working situations into MMSs is that it could have been shown that the ergonomic approach of MMS is able to provide information for all common HRA-methods (for detail see Sträter, 1997\(^12\) or Sträter & Bubb 1998). Figure 3 is showing the generic MMS that was used for detailed analysis.

---


A MMS can be described in the following way: A task has to be evaluated by an operator. The operator processes the task with respect to the actual system state (feedback loop). By performing an action via the control elements he changes the system behavior. The system change is then displayed and reported to the operator. The whole MMS is embedded in a specific situation and environment. For instance, the situation is related to shift or revision plans or time and duration. The environment represents classical ergonomic aspects such as noise, illumination etc. In most situations the operator also interacts with other persons in the plant during an event. This Human-Human Interaction is realized by the two components 'task-order' and 'task dispatch'. Task dispatch means all activities that the person has to do to inform others about his work (e.g. report the task transaction to the supervisor or document his transaction with a check mark in a test-protocol). The 'task-order' means all oral and written orders for the operator to perform his task (e.g. procedures or orders of management). In the analysis of events, it was found that it is important to distinguish 'task' and 'task-order'. The term 'task' describes what the operator physically has to do on various levels of detail (e.g., by a hierarchical task description). The term 'task-order' describes the way how the task was introduced (e.g., by administrative order, by oral instruction of the supervisor). Additionally to the well-known structure of the MMS, the introduced term 'task-order' enables together with the term 'task dispatch' to depict the important aspect of communication within working systems.

The system outcome of a MMS defines whether an erroneous occurrence took place (e.g., valve xy not open, steam outlet too high). This error is a result of one or multiple weak points within the MMS. To find these weak-points, in a first step information about each aspect of the MMS should be collected for each occurrence:

Situation: Under which situational conditions took the occurrence place? When has the action happened and how long did it last?

Environment: Where has the event happened?

Task: What has the operator to do physically in the plant by considering the actual conditions?
Person: Which persons were involved and what were their necessary cognitive activities?

Action: What has been done?

Feedback: What are the information sources for checking plant parameters?

Task-order: How was the operator informed about his task (prescribed in procedures, oral order by supervisor, implicit order by management, ...)?

Task-Dispatch: What had the person to do to inform others about his work?

System: What part of the system has been manipulated?

These questions that a user is asked for to describe the MMS stages are mostly identical with the questions presented by IAEA-499 (1987)\textsuperscript{13}. Additional information about the system state and consequences of an event are added. To extend the MMS approach to an error modelling approach, it is necessary to assign the weak-points and to describe the influences causing the weakness of the different stages of the MMS. These influences are known as PSFs and are indicated by the dotted arrays in Figure 4. Internal PSFs can be found in the human related arrays and external PSFs in the other arrays. Note that organizational and communicational PSFs are belonging to the information-flow to and from the Human (task and task-order, task-dispatch).

Figure 4: Possible weak point in the MMS and related PSFs.

As already mentioned during the discussion of Figure 2 and Figure 3, these links are used to describe the interaction between different MMSs and, by this, complex working systems. As outlined in

Figure 5, this procedure consequently also supports the analysts in systematically collecting information about the sequence (dynamics) of an event and the relationships between the MMSs. Complex working systems can be built by using several MMS. Interactions between Persons are represented and the complexity and the dynamics of an event are represented (e.g. Influence of Maintenance on Production).

Figure 5: Building complex working systems by using several MMS.

Summarizing, in the MMS an error is defined as a consequence of any deficiency (weak-point) in a stage or in an information transmission part of the MMS. To analyze an event and to find the important information about errors and influencing factors, the following questions must be asked for each aspect within the MMS:

1. What was the object of interest, e.g. "valve"?
2. What was the performed action, e.g. "open"?
3. What was the error, e.g. "omitting" or "too much"?
4. What was the influencing factor, e.g. "bad labeling"?

By these questions the factual aspects of each MMS-aspect may be described (the object, the action, the errors, and the influencing factors). A fifth factual aspect called 'element' was added in order to be able to describe the event in more detail and to make comments on the previous columns. This distinction is of importance because each step means a deeper insight into reasons for the error within the observation. According to epistemology, in Sträter (1997)\textsuperscript{14} these steps were consequently called

\textsuperscript{14} "Op. cit., 4, Sträter (1997)".
phenomenological view (assignment of an error, step 3), causal view (relationship of step 1 and 2 to step 3) and actional view (step 4).

Answering all these questions (description of all factual aspects for every stage of every MMS that were identified within an event) leads to information about the context of an event. Context is defined here at least as the task-order and tasks, the information from the system to perform the tasks (feedback), and the characteristics of the situation (e.g., time constraints) or of the technical system (e.g., dynamics) as well as the interrelationship of various MMSs (the operators, the management or organizational staff). All these aspects together build the error situation or error context. In total, one finds plenty of specific questions that may be of relevance to describe the context. The derived answers concerning the MMS-aspects and the description-aspects may be compiled in a table as outlined in Table 1.

<table>
<thead>
<tr>
<th>Factual aspects:</th>
<th>Object</th>
<th>Action</th>
<th>Error</th>
<th>PSF</th>
<th>Elements</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMS aspects:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Situation</td>
<td>reactor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>pump</td>
<td>actuate</td>
<td>omitted</td>
<td></td>
<td>pump xyz</td>
<td></td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>+ time-pressure</td>
<td>+ too high</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>? task-precision</td>
<td>? low</td>
</tr>
<tr>
<td>Person</td>
<td>reactor</td>
<td>Asso-</td>
<td>wrong</td>
<td></td>
<td>location</td>
<td>Description of the</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>operator</td>
<td>ciate</td>
<td></td>
<td></td>
<td>mixed up with function</td>
<td>cognitive activities and</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>processing</td>
<td>the cognitive error and</td>
</tr>
<tr>
<td>Action</td>
<td>pump</td>
<td></td>
<td></td>
<td></td>
<td>pump xzy</td>
<td>performing the cognition</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>actuated</td>
<td>Description of the error of commission and the</td>
</tr>
<tr>
<td>Feedback</td>
<td>indicator</td>
<td>Recogn-</td>
<td>omitted</td>
<td></td>
<td>location</td>
<td>PSFs on performing the action</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>nize</td>
<td></td>
<td></td>
<td>inappropriate</td>
<td></td>
</tr>
<tr>
<td>Task order</td>
<td>procedure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>for pump xyz</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>Follow</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task dispatch</td>
<td>supervisor</td>
<td>Inform</td>
<td>too late</td>
<td></td>
<td></td>
<td>about action</td>
</tr>
<tr>
<td>System</td>
<td>cooling system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>primary cooling</td>
</tr>
<tr>
<td>&quot;&quot;</td>
<td>&quot;&quot;</td>
<td>start up</td>
<td>omitted</td>
<td></td>
<td></td>
<td>due to low flow</td>
</tr>
<tr>
<td>pump xyz</td>
<td>switch off</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The table is filled from left to right. Every empty field in the table represents an unknown possible contributor to the event; consequently the table has to be filled as completely as possible to describe an event. However, if information is not available, the field remains empty. If a taxonomy is used to fill the framework the acquired data become highly reliable. But, the taxonomy should not be standardized too much and should also be open and flexible for incorporating new information to assure validity. In this way one can describe an event by assigning errors (in the sense of weaknesses) and PSFs to any stage of the MMS. A collection of PSFs that were found in the application of the method is presented in chapter 2.

Within the table, the left columns 'object' and 'action' describe what has been done and the column 'error' whether this was wrong. Consequently, what would have been right is only implicitly coded and may be inferred from a lacking action-error relation. The advantage of such a procedure is that event analysis is structured from observable information (objects) to the more interpretative information (PSFs) which is in turn based on and selected by previous information about the event. This also makes event-analysis efficient: the answers are structured in a way that specific information (object and action) is needed to generate answers about errors and PSFs. Furthermore only if an error could have been specified, it is permitted to award one or more PSFs as possible causes for this error. This is obvious because identifying a PSF without having identified an error is contradictory. Furthermore it is guaranteed that the relationships of objects, actions, errors and PSFs are documented.

In the application program (chapter 1b.2), the table itself is filled up interactively with a knowledge-based-system that provides lists of the most probable terms (e.g. most probable PSFs for omission errors). At this point it should be mentioned that the evaluation-program needs two essentials features to allow this procedure: (1) dealing with incomplete information and (2) learning by additional information observed in new events. Both are described later on in chapter 1b.2. Some properties of such an analysis structure are:

- By this procedure, the method combines advantages of open methods (high flexibility, open for new facts that are not considered in the method yet) and closed methods (high reliability, statistical treatment).

- For the description of an event, one has to look at all elements and information flows in the MMS in order to find weak-points (i.e. errors in the working environment). For specifying these errors, one can start with observable (or factual) information (i.e. objects and actions). This leads to a more accurate error analysis because the objects to describe an event can be verified in the plant.

- "Hard" information about every detail of an event often is lacking. As demonstrated for the PSF 'time-pressure' in Table 1, every term used within the table may be marked with a certainty indicator (no indicator for certain information, + for uncertain, ? for hypotheses). Thereby, real information, assumptions and interpretations may be distinguished in order to represent the degree of insight and trust in the own analysis of the event. In an evaluation, information about the certainty is essential to depict the validity of prediction and improvements (cf. Mosneron-
Dupin et al, 1998). Also different (to some extend alternative) explanations may be included in the analysis scheme by this (e.g. task precision or time pressure).

- The element column is useful to specify the information of previous columns (e.g. specifying which pump was omitted) or to specify whether an PSF had a high or low negative effect. It provides more detailed information than the generic ones of the first columns and is also useful to make comments on the previous columns.

1b.1.3 Analysis of Cognitive Aspects

Cognitive issues of the operator are related to the MMS-component 'person'. This component is dealing with the description of the cognitive processes, cognitive errors and internal PSFs (motivations, expectations, perceived consequences, goals, etc.). The problem of dealing with cognitive aspects is not that much the lack of knowledge about internal or cognitive PSFs (they are well elaborated in psychological literature and may be found in numerous taxonomies of ergonomics; some are summarized in Mosneron-Dupin et al, 1998). Moreover, in the initial step of analysis it is important to find the relevant cognitive mechanisms and PSFs within event analysis. For this, the method requires a 'red line' from the objective information (Which person was involved?) via the cognitive activity (What was his cognitive activity during the event?) to the cognitive error (Was the activity right?) in order to finally constitute an internal PSF (e.g. motivation, fixation). This traceability is even more important than for the other MMS-aspects because cognitive aspects are latent and hidden properties. Traceability may be assured by a similar procedure than already suggested for the other aspects of the MMS (but with different content):

1. Object: Specify the involved person within the event
2. Action: Specify the cognitive activity of the person
3. Error: Specify whether a cognitive error took place and which type of cognitive error it was
4. PSF: Specify the internal PSFs

This 'red line' starts with the objective (external) available information about the operator who was involved within the occurrence of the event. After having identified the operator, his cognitive world has to be investigated. In most of the HRA methods, cognition is equaled to 'looking at the cognitive processes'. They are usually subdivided into certain stages (e.g. perception, identification, evaluation, action) or certain phases (skill-, rule-, knowledge-based). However, such a view on cognitive processing is limited in a sense that it cannot explain why a certain stage or phase failed.

Hence, it may be concluded that it is not sufficient to describe the cognition of the operator only by looking at the way how information is processed. This is the reason for not subdividing the human part of the MMS in more detailed processing stages as sometimes suggested by other authors. What has to be considered additionally to the processing is immediately obvious if one considers cognitive


models, like the one of Rasmussen (1986)\(^{17}\), completely. Additionally to the well known behavioral phases, Rasmussen (as an example for many other authors in cognitive science) also distinguishes topographic search and symptomatic search. Topographic search is information driven and symptomatic search is hypotheses or goal driven. By these additional distinctions, Rasmussen's model is able to explain different diagnostic strategies and errors during diagnosis (Sträter, 1991)\(^{18}\). In consequence, in the CAHR-method the following basic aspects of cognition were distinguished:

- Information that the operator considered, where information may either stem from memory or the sensory system
- Goals that the operator had, where the term 'goal' is closely related to expectations, intentions, motivations and attitudes
- Processing of goals and information, ranging from conscious to unconscious

Note that this distinction is different to the subdivision of classical information processing approaches, as used in THERP for instance. They are focusing on the way of processing and insufficiently consider the role of goals and information.

Based on these considerations, the red line starts with assigning cognitive activities. To perform this step, the system ergonomic approach of Bubb (see Bubb, 1992\(^{19}\) or Sträter, 1995\(^{20}\)) was found as an approach that fits the basic aspects of cognition. It distinguishes between different aspects of a situation that are of importance for the cognitive activity of the operator. The approach is outlined in Table 2.

The classification of cognitive activities is based on all of the above described cognitive aspects (aspects written in italic are more demanding). Though describing the meaning of a system ergonomic description in a single word is difficult, catchwords describing the cognitive activity are derived from the classification and introduced with '→' in the table. They are related to the factual aspect 'action' of the MMS-aspect 'person'. In the system ergonomic approach it is assumed that every cognitive activity requires at least one aspect of each type (orthogonal classification): For instance, a cognitive activity may be either dynamic or static but independently thereof either simultaneous or sequential as well.

The reason for choosing the system ergonomic approach for classifying cognitive demands was: (1) The approach does not depend on the experience level of the operator, but on the general abilities that an operator has to use for coping with a given situation. This is different to, for instance, the skill-

\(^{17}\) "Op. cit., 3, Rasmussen (1986)".


rule-, knowledge-based-approach and others such as the GEMS-model of Reason (1990)\textsuperscript{21}. Hence, this method focuses on the operator's cognitive stress (the context related demands of the situation the operator has to cope with) and not on the cognitive strain like other models (the cognitive skills the operators might use to cope with the situation). (2) Information about the cognitive strain of an operator is difficult to acquire from plant experience, only person-related acquisition methods - such as interviews for instance - are able to acquire cognitive strain (Eberleh et al., 1989)\textsuperscript{22}. (3) It was possible to show in the investigation performed in Sträßer (1997)\textsuperscript{23} that this classification of information processing errors according to the cognitive strain is suitable for classifying cognitively demanding situations: It was found that situations with cognitive strain may be predicted by analyzing the cognitive stress. The same cognitive habits and their modifying PSFs were found.

Based on the description of the cognitive activities as an important link between the 'objective world' and the 'internal (cognitive) world' and hence a necessary pre-condition, cognitive errors may be assigned to the activities (e.g. tracking omitted) and cognitive PSFs may be assigned. Main reasons for cognitive errors that may be distinguished are:

- Information considered inadequately
- Inadequate reduction of goals
- Inadequate processing of goals or information

By considering these aspects of goals, information and processing, errors may be explained like ignoring information during circumvention of safety-rules or delaying effects due to rethinking about well trained procedures instead of applying them immediately. Because these cognitive aspects are able to explain cognitive errors, they may be used to fill up the PSF-column of the MMS-aspect 'person' rather than the action-column.

\footnotesize


\textsuperscript{23} "Op. cit., 4, Sträßer (1997)".
Table 2: System-ergonomic classification for describing cognitive activities in human information processing.

<table>
<thead>
<tr>
<th>Type of Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content of Task</td>
<td>dynamic: the task is changing over time and depends on time frame (e.g., tracking-task); more than two information units → track</td>
</tr>
<tr>
<td></td>
<td>static: the task is independent of the time; only one information unit → operate</td>
</tr>
<tr>
<td>Type of Operation</td>
<td>simultaneously: a simultaneous operation of several controls is required; parallel processing required → coordinate</td>
</tr>
<tr>
<td></td>
<td>sequential: the control has to be performed in a defined sequence; serial processing required → follow</td>
</tr>
<tr>
<td>Dimensions</td>
<td>multi-dimensional: the technical system is characterized by more than one parameter that has to be brought into relation to another; more than two goals → imagine</td>
</tr>
<tr>
<td></td>
<td>one-dimensional: the technical system is characterized by one parameter; one goal → expect</td>
</tr>
<tr>
<td>Design of Task</td>
<td>monitorive: the human being is monitoring the process by collecting information and deciding about the process state; 1:1 relation between information and goal → observe</td>
</tr>
<tr>
<td></td>
<td>active: the human being is actively involved in process control by collecting and combining information and process interacting; 1:1 relation between information and goal, top down processing → perform</td>
</tr>
<tr>
<td>Type of Presentation</td>
<td>compensatory-task: the system provides only information for the human being how large the difference of task and actual state is; 1:N relation between information and goal → identify</td>
</tr>
<tr>
<td></td>
<td>pursuit-task: the system provides information which systems are affecting the difference of task and actual state; 1:1 relation between information and goal, bottom up processing → recognize</td>
</tr>
<tr>
<td>Compatibility</td>
<td>primary: compatibility of the mental model of a person with external information (e.g. learned, stereotype behavior); compatibility of goals and information → associate</td>
</tr>
<tr>
<td></td>
<td>external: compatibility of different external information (e.g. displays and controls); compatibility of different information → match</td>
</tr>
<tr>
<td>Secondary Compatibility</td>
<td>compatibility of external movements with learned meanings (e.g. up means higher level); compatibility of goals → transfer</td>
</tr>
<tr>
<td>Feedback</td>
<td>Information presented to the Operator by the system in an appropriate time; information → perceive</td>
</tr>
</tbody>
</table>
1b.1.4 Description of Improvement Measures

In the final stage of every event analysis method it is important to mention the backfitted improvement measures in order to be able to evaluate their gain for the future. For this purpose, the undertaken improvement measures were coded in the method similar to the description of the MMSs and added to the event description (Table 3):

Table 3: Example for coding improvement measures within the event-analysis scheme.

<table>
<thead>
<tr>
<th>Factual aspects:</th>
<th>Object</th>
<th>Action</th>
<th>Error</th>
<th>PSF</th>
<th>Elements</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMS aspects:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improvement</td>
<td>pump</td>
<td>display</td>
<td></td>
<td></td>
<td>pump xyz</td>
<td>After the event occurred, the pump was rearranged on the control board</td>
</tr>
<tr>
<td>&quot;</td>
<td>&quot;</td>
<td>Rearrange</td>
<td></td>
<td></td>
<td>place</td>
<td></td>
</tr>
</tbody>
</table>

1b.2 Evaluation of Collected Events for Generating Extensional Statements

The event analysis method is leading to a description of an event in the form of simple sentences like "valve was omitted to be opened due to bad labeling". These sentences are the basis for information about the situation (the context) within each event. Several of these simple sentences are describing a MMS and several MMSs describe the whole event.

1b.2.1 Evaluation of Event Descriptions

The data structure of the event description is extensive and complex and has to be analyzed according to the intended outcomes of the analysis for HRA. The detailed information about an event that is obtained by application of the method is only useful if the data may be evaluated with a somewhat extended meaning for a question of interest. For this purpose, the evaluation method has to identify events that contain similar error prone situations, similar error opportunities, similar PSFs or other qualitative information about the man-machine interface, the organization, or the operators. The evaluation model has to provide answers for various qualitative and quantitative analyses in HRA or retrospective analysis (plant improvements), such as the following ones:

1. For HRA and plant improvements, information is needed about relations of different PSFs, errors and objects in the plant. To evaluate qualitative and quantitative predictions about these relationships, the gathered information has to be analyzed with respect to the semantic relations that are observed within the collected information; e.g.: which PSFs may be observed by errors of omission in the control-room? Also, frequencies of occurrence of PSFs, errors or any of their relations have to be calculated; e.g.: how many errors of omission happened in the control-room and how often were accompanied PSFs observed?
2. The data must be available on different levels of detail in order to support different steps of MMSA (Man-Machine System Analysis) or different HRA-methods such as the detailed THERP or the holistic HCR.

3. The relationship of errors and PSFs to the improvements realized should be analyzed in order to investigate the effectiveness of the improvements; e.g.: how useful is the improvement of procedures in situations with time pressure?

4. The error chain should be analyzed according to safety-relevant aspects, e.g. involved safety systems or broken safety barriers; e.g. which PSFs do affect administrative precautions like check lists or personnel redundancy and how high is this potential by e.g. checking control rods?

To assure that these analytical questions can be answered, it was necessary to develop an advanced evaluation model that is able to transfer the detailed information of the description table into the needed form. The general features that are of importance for HRA will be outlined.

- The Evaluation Model

Because of the high level of detail of the event description and the high complexity of the desired output of evaluation, it was necessary to create an advanced algorithm for analysis of the collected data. Basis for this algorithm was a connectionism approach. The term connectionism includes a family of advanced data processing models starting with neural nets on one side and ending with probabilistic models for semantic processing on the other (Rumelhart & McClelland, 198624; Pearl, 198825). The connectionism network is representing the collected data from the events as nodes and relations within a network. It represents the relationships and dependencies between objects, actions, errors and PSFs, i.e. the dependencies within the context of an error. Figure 6 provides a general overview about the event evaluation procedure. Further details about the data processing algorithm are given in Sträßer (1997)26.

---


Figure 6: Overview about the event evaluation procedure of CAHR.

- Characteristics of the model

By describing many events, a strongly connected semantic network of the descriptors which were used in all events represents the total collected information. This net consists of nodes (representing descriptors for certain PSFs for instance) and connections between different nodes (e.g. relations between the different PSFs). In a connectionism approach, both (nodes and connections) possess weights and an activity function is used to generate statements for any combination of descriptors. Is it also possible to combine various descriptors to one class that is representing a specific level of abstraction (e.g. all errors occurred in the first 10 minutes or all digital displays).

The characteristics of the model can be described by the ability to learn, by the ability to generate similarities between events, and by the ability to organize itself. These characteristics are important to enable an open and bottom-up approach and to generate the information that is needed for HRA Analysis. Normal databases with fixed acquirement and evaluation structure are not able to exhibit this behavior.

Ability to learning

- Weights of relations between descriptors (e.g. two PSFs) that frequently occurred together in various events are increased. Other connections that are not used will weaken in relation to the updated ones. With this behavior the net is able to learn. The network is optimized with respect to the observed information. Often observed descriptors or links of descriptors represent the experience of the net.

Not observed descriptors will isolate themselves from the rest of the net by relative weakening of their links. Beside evaluation of quantitative information (e.g. frequencies of relations between
PSFs), this experience of the net may be used to support event description and may also lead to a consistent event description: the net may provide suggestions for those PSFs that are found to be the most probable ones in similar former events.

**Similarity-Matching**

To look at different levels of detail (e.g. in a HRA screening sequence) it is necessary to determine the similarities of different events at different levels of abstraction. This can be done by looking at the different layers of the network (e.g. level of abstract terms like 'display' or level of detailed terms like 'analog meter xyz'). Thus, similarities of different tasks, different personnel or any other stage of the MMS can be determined.

**Self Organization**

Two ways are possible to build up a data structure: The information can be acquired and then classified (classification methods), or an analytical structure can be used to describe an actual event (analysis methods). With respect to acquisition of plant experience, the first approach is problematic mainly due to two reasons. First, the description demands and possible descriptors are not predictable. Second, the scheme only allows a generation of qualitative and quantitative data from the collected plant that is restricted to the taxonomy that was chosen but does not enable a generation of novelties and nuances observed within an event experience. As discussed, a bottom up approach was used here for these reasons. Such an approach has to be able to consistently integrate new information into the present one. The presented approach does this by inserting new terms in the present hierarchy of terms by their use and position within (1) the MMS-aspects and (2) the factual aspects. This behavior may be called self-organization.

**1b.2.2 Data-Base Application for HRA**

As pointed out before, the method for recording of plant experience employs a hybrid solution between open analysis and structured analysis form (i.e. a formation technique, see e.g. Bonato, 1989)\(^ {27} \). Formation techniques perform best if applied as a computer program. For these reasons, the program for recording, evaluating and assessing plant disturbances with respect to human errors was implemented as a database program named CAHR (Connectionism Assessment of Human Reliability); see also brief description in Sträter (1996a)\(^ {28} \). It is based on the database MS-Access under MS-Windows. Within the program, an occurred event can be analyzed interactively. Two different functions are offered to the user:

1. Case and cause description of an event that has occurred in a plant.

---


2. Quantitative and qualitative evaluation of the human reliability information aggregated in the system.

The structure of the whole system is shown in the block diagram in Figure 7.

Figure 7: Block diagram of the database program.

In the description part, an occurred event may be qualified by filling the analysis table (as Table 1) with a set of descriptors. This set of descriptors was derived from various taxonomies used in literature but was designed as an open set. By selecting descriptors from a list or inserting new ones, the user can describe the facts, the errors and different reasons (PSFs) for failure. The user is supported in describing an occurred event and in finding the relevant errors and influencing factors by a knowledge-based evaluation: The system provides possible answers, which are the most probable ones to explain the initially entered information about an observed event. This interactive analysis is structured by the stages of the MMS and the factual aspects (objects, actions, errors, root causes / PSFs and elements). As an example, the program lists 'task-preparation', 'task-complexity' or 'task-precision' as possible PSFs belonging to the MMS-stage 'task'. These descriptors can be detailed again by further description of elements. By answering all questions concerning the event, all
information necessary for later analysis is collected. In this way tasks and actions, errors, particular circumstances and possible reasons for the failure of an action in an event can be named.

Due to the complexity of the event descriptions, in the evaluation part of the method the relationships of the descriptors are compiled as links between nodes of a connectionism net. By describing many cases, a database with an intensely linked structure of weighted links is generated. As discussed above, the links can be evaluated in different ways: (1) Across the strength of the links a quantitative analysis is possible to supply HRA with the needed quantitative data. (2) The structure of the network can be used to make qualitative predictions (e.g. screening of error-potentials or analyzing PSFs to find plant improvements).

1b.2.3 Discussion

The evaluation method is able to analyze the complex and highly variable event descriptors in a quantitative and qualitative way. This can be used to estimate influences of PSFs in a given situation or to find plant improvements without giving up specific and detailed information that enables understanding and tractability of the specific event. Additionally, similarities of different plants, tasks or data of different personnel (e.g. supervisor, operator, maintenance technician) can be determined. The features of the connectionism approach are summarized in Table 4.

Table 4: Features of the integrated approach.

---

**Acquisition - description part**
- flexible scheme to collect data
- consistent collection of data with structure formation technique
- able to learn from experience
- optimizes the classification scheme by frequencies of use
- able to deal with incomplete and inconsistent descriptions
- considers dependencies between failures, PSFs and situational characteristics

**Evaluation - analysis part**
- similarities between events are analyzed
- relevant factors for error prone situations and the importance of their combinations can be requested
- provides information for HRA and plant improvements
- dependencies between tasks errors and PSFs can be evaluated

**Application**
- open solution for wide range of use
- integrates events (different plants, tasks or different personnel)
- failures not defined as human failures but as failures in a working system (MMSs); hence guilt-free understanding of errors

---
1c. A Description of the Underlying Concepts of the Analysis Method Used (that is, Reference to Human Sciences, if Relevant):

The last chapter briefly described the event evaluation method. Now, the method should be reflected against information demands of HRA and retrospective analysis.

1c.1 The Ergonomic Perspective

The MMS provides typical information needed for ergonomic analysis of the working environment as the following example about the serious impact of latent PSFs shows: Typical ergonomic factors are reliability of equipment, the system dynamics and the degree of automation of the technical system. They are related to the system-component of the MMS. The way how the system behavior is presented to the operator (feedback) may have an impact on his image (or mental model) of the system. Hence, reliability, dynamics and degree of automation are system related PSFs for operators’ performance that have an impact if the information is not or inappropriately presented to the operator or if the operator cannot manipulate these system behaviors appropriately.

1c.2 The Cognitive Perspective

Using the MMS as a generic error model provides useful information for various cognitive error models such as the ones of Norman (1981)\textsuperscript{29}, Rouse and Rouse (1983)\textsuperscript{30}, Rasmussen (1986)\textsuperscript{31}, Hacker (1986)\textsuperscript{32}, Swain and Guttmann (1983)\textsuperscript{33} or Reason (1990)\textsuperscript{34}. This is obvious since the MMS includes the operators’ information processing as well as the context in which this takes place. On the other hand, using the MMS avoids a typical problem of cognitive error models, namely that they are implicitly assigning a liability to the operators since they reduce every occurred failure to an error within the operator. They only implicitly consider interactions of man and machine or the interface by assuming an impact of external PSFs on certain stages of cognitive processing. This kind of error modeling represents errors of the working system always in relation to cognitive stages and hence as PSFs for cognitive errors. Thereby, errors due to the context in which cognition took place and errors in cognition itself are mixed up.

Purely cognitive or human-focused error models do not only have the problem of lacking representation of the context of cognition but also the problem of blaming the operator because he is always set into the center of analysis and in the center of possible causes for the error. Thereby,


\textsuperscript{31} "Op. cit., 3, Rasmussen (1986)".


\textsuperscript{34} "Op. cit., 21, Reason (1990)".
distrust and perturbation and finally reduction of the quality of collected information may be produced.

Because human-focused error models reduce possible causes to humans, those models are also inadequate to collect the needed information for HRA or for finding plant improvements because both need information about the working environment of the operator. External PSFs that may lead to plant improvements cannot (or only indirectly) be represented.

In contrast to human-focused models, the presented MMS model describes a human error (1) within its context of the event flow and (2) within the whole man machine system. This offers the advantage to describe a failure not only as a human problem. Plant operating failures will not only be defined as deficiencies of the operator that blame him indirectly for every failure. This feature of the MMS-model is particularly important with respect to IAEA (1995)\textsuperscript{35}.

On the other hand, the method presented here also enables analysis of cognitive processing but it respects that human errors are occurring within the context of the MMS, as Figure 3 shows. Referring to the picture, the following aspects of cognitive interest may be pointed out:

- In order to be able to understand errors in the cognitive process of the operators, it is not sufficient to describe how he processed information (e.g. divided into perception, decision and action). Moreover, the underlying goals and the information that were used in the information processing have to be considered to explain errors such as circumvention of safety rules.

- The actual system state is usually not directly observable (especially in a control room, but also during local maintenance operations). An operator usually judges a system state by its symptoms (e.g. provided by displays). The operator has to compare the symptoms with his knowledge of the system to initialize an action. It's a well-known fact that this feedback loop is essential for the operator to build a mental model of the situation (e.g. Schmidt, 1988)\textsuperscript{36}.

- In most situations the operator has to report the task transaction to the supervisor or has to document his transaction in a test protocol. This communication aspect is crucial for any working situation where more than one person is involved in the event. Communication means always an additional task for the operators that may interfere with the primary task of performing actions on the plant.

- It is important to distinguish the task and task-order. The 'task-order' is given by some administrative orders (e.g. procedures) and describes how the operator was informed about doing something. The 'task' describes what the operator has to do physically in the plant by considering the actual conditions. This distinction also represents the difference between what the designer intends the operator to do (task-order) and what the operator sees to be important.

\textsuperscript{35} "Op. cit., 6, IAEA (1995)".

in a situation (task) such as constrains and conditions under which the operator has to realize a task-order (e.g. two procedures conflicting with each other). Differences between task-order and task are cues for the operators that a decision has to be taken, Hence, this distinction is an important aspect in understanding the decision process.

By these features, the operators' role in the plant should also be understood in an extended way: The approach considers that the operator is not only a weak link in the system that is making errors but is also able to compensate errors within the working system. This positive and active role of the operator is often ignored (or not explicitly mentioned) in most approaches of event evaluation. Most of the times event evaluation is equalized with "looking at human errors". Thereby, the problems of the operators are not considered seriously. Considering the positive role by the MMS is also decisive if an assessment of operators' performance is needed or the potential for recoveries is to be understood (i.e. finding factors that affect whether recoveries are successful or not).

1c.3 The Organizational Perspective

The complete analysis finally leads to a large table (as partly described in Table 1) including all MMSs and improvements (vertical direction) as well as all tasks, errors and PSFs (horizontal direction). This in fact is nothing else than a way to describe an event in a structured language. Hence, the dynamic and context of an error as well as the complexity of the error-situation are represented together with the recovery situation in the table. This property is usually only ascribed to free text descriptions of events. The event as a whole represents also the information needed for analyzing the organizational factors that have played a role. The information flow between the MMS (cf. Figure 1) for instance is able to represent the impact of maintenance errors performed some time ago (e.g. latent failure of a closed valve) on the active error an operator made during operation (e.g. assuming that valve is open).

Additionally to the event sequence, the following parts of the description model are focusing on possible organizational PSFs: The 'task' (especially how well the task is prepared), the 'task-order' (e.g. the implicit order given by management to avoid shut down although this was not ordered explicitly), the 'task dispatch' (e.g. lack of communicating the task transaction may be a result of personal reluctance to provide to someone else information he needs in order to keep his own might or to blame the other). These components are minimum requirements to depict organizational behavior since every organization is characterized by the communication between the persons belonging to the organization, see Schuler (1995)37.

Another aspect of the organizational perspective (but as well of the ergonomic one) is the one of interrelations between PSFs. They infer more global influences such as: if task-preparation and ergonomic design are bad, this leads to the conclusion that the management has yet not drawn enough attention to adequate design and preparation of this task. They also show mechanisms of how safety barriers may fail (e.g. a procedure was not followed due to personnel conviction to have the situation under control or simply due to time-stress). By including the organizational perspective in this implicit way as a coherency of multiple PSFs (and not by explicitly naming the global management factors directly) also a 'red-line' for analysis of organizational and management factors can be drawn.

from the objective observable errors via PSFs to the more abstract field of organizational impact (the interrelation of PSFs). Hence, these factors that are usually difficult to be fixed (and that are not favored by the management itself) can systematically be included into event analysis and later assessment.

1c.4 The Perspective of Safety Impacts on Technical Systems

From the engineering point of view and for analysis regarding safety impacts of human errors, it is essential to describe the technical system that was affected by the human failure. INTENT (Gertman et al., 1992) also distinguishes decision-based errors with respect to the safety relevance of the technical system that is affected. Also, the gain of improvements sometimes has to be related to the safety relevance of the observed error. This perspective is related to the 'system-component within' the MMS. Beside the above discussed human-aspects (ergonomics, organizational, personnel), now the status of the plant is put in focus. Here, it is described which technical system was erroneous due to human interaction such as over-pressure of tank, or failure of high pressure injection. Within the analysis table, these aspects are placed in the object and action columns of the MMS-aspect 'system'. Their relationships to the HF-information are established by the analysis table.

---

1c.5 Use of the Framework for HRA

The scheme introduced in the last section provides data for various HRA-purposes, especially concerning (see Sträter & Bubb, 1999 for details)\textsuperscript{39}.

- The information requirements of the different current used HRA-methods like the HCR model (Hannaman & Spurgin, 1984)\textsuperscript{40}, the SLIM approach (Embrey et al., 1984)\textsuperscript{41}, the THERP method (Swain & Guttmann, 1983)\textsuperscript{42}, and the ASEP method (Swain, 1987)\textsuperscript{43}. For summary of the requirements see IAEA (1995)\textsuperscript{44}.

- The different PSA-types like Type A (pre-initiators), B (initiators) and C (post-initiators) (see Hirschberg, 1990)\textsuperscript{45}.

- Swain and Guttmann (1983)\textsuperscript{46} had set up 10 steps for MMSA. As discussed in Sträter (1994)\textsuperscript{47}, these steps can be arranged as a subset of the HRA process described in IAEA (1995)\textsuperscript{48}. The Data for MMSA like qualitative data and quantitative data as well as general and abstract vs detailed data may be derived from the framework.


\textsuperscript{44} "Op. cit., 6, IAEA (1995), p. 5"


2. Describe in Detail the Event or Sequence Analyzed

The procedure presented here is based on evaluation of observed plant events. To make predictions with the approach, occurred events have to be evaluated. This chapter provides an overview about some results of using the CAHR-approach.

2a. Inductive Qualitative View: Analysis of Events

The method was used for qualitative and quantitative evaluation of 165 events of boiling water reactors in German nuclear power plants. After having collected different events, the collected data may be evaluated for different purposes of HRA (i.e., qualitative analysis of error likely situations and quantitative assessment). An overview is given in chapter 3. The major results of this application are

- the comparison of the derived data with the data provided in the THERP-Tables as well as in the French simulator experiments,
- major PSFs, their interrelations and their importance for cognitive errors, and
- data that could be derived concerning cognitive errors and organizational influences.

Some major results of this test-application will be described in the following.

2b. Inductive Quantitative View: Comparison with the THERP Data Tables

Concerning HRA-assessment, the data base application is able to find context related similarities of different events (i.e. common error prone situations) and to calculate frequencies of occurrence for these situations. With this model, probabilities of occurrence were calculated for situations that are similar to situations underlying the data items of the THERP handbook tables. As the comparison with the THERP data shows, these probabilities of occurrence may be interpreted as estimates for HEPs.

A comparison with quantitative predictions of HEP-Items of THERP was performed as follows: First, queries were set up for error types that are similar to 79 items of the THERP-Method. Then relative frequencies of errors that were observed in the events were determined by the data base application. These relative frequencies are not directly able to estimate probabilities but they represent the difficulty operators may have in a certain situation. In psychological measurement, Rasch (1980)\(^49\) assumes a simple functional relationship between difficulty and probability. Consequently, probabilities were estimated from these relative frequencies by a psychological measurement method according to Rasch (see Sträter & Bubb 1999 for detail)\(^50\). Figure 8 provides an overview about the quantification process of CAHR.


Figure 8: Overview about the quantification process of CAHR.

- **Estimating Probabilities**

By no means one might conclude that the frequencies of errors observed within events may be used as estimates for HEPs directly because plant experience has a principal problem of estimating HEPs: plant experience is on principal not able to provide a sophisticated information to calculate a HEP=n/N. The reason for this is that every event reporting to someone is always defined by a certain message-threshold that was exceeded (no matter by whom, how, or on which level of detail the event is reported). Surely the message-threshold is lower within the plant compared with the message-threshold for reporting to the regulator but the principal problem does not disappear: it is impossible to derive the number of demands N from the number of events and to some extent also the number of errors n may be higher than the ones that were reported. Hence, the information collected from plant experience may only be taken to support calibration. For estimating HEPs, a different approach is needed that is able to work with this incomplete data.

To find such an approach, one has to think about what the frequencies of observed events mean from the HRA point of view. First of all, they describe how often a specified situation of type i has been observed beyond a certain level of threshold (where the threshold depends on the organization that requests the information like plant management or authority, for instance). This frequency includes two parts: (1) n_i, the frequency of errors that the operators made in situations of type i and (2) o_i, the frequency of situations of type i where the operators made no errors (e.g., they recovered an event successfully). Since HRA is concerning the amount of errors in a given situation of type i, the following proportion may be built, where m_i is the number of the totally observed situations of type i:
\[ \frac{n_i}{m_i} = \frac{n_i}{n_i + o_i} \]  \hspace{1cm} (1)

Of course, this relative number still does not represent a HEP but in psychological terms this number means: if the relative number of errors is high, it seems to be a difficult situation for the operator; if the number is low, the situation seems to be easier. Hence, plant experience is able to represent the difficulty that operators have with some error prone situations. In psychological measurement, Rasch (1980)\(^{51}\) assumes a simple functional relationship between difficulty and probability. Consequently, a psychological measurement model according to Rasch was used to generate estimates for probabilities of occurrence. Each relative frequency of occurrence was taken as a rating for the difficulty that the operators perform the situation correctly and probabilities were gained from this measure of difficulty. For each frequency of occurrence the probability of occurrence was calculated according to a normalized probabilistic model after Rasch (1980)\(^{52}\) according to the following equation (see Strätler 1996b\(^{53}\), 1997).

\[ P\text{Failure of Type } i = \frac{\left(\frac{n_i - \mu}{s_n}\right)}{1 + e^x} \]  \hspace{1cm} (2)

and \( n_i = \frac{m \times n_i}{m_i} \)

where:

- \( n_i \): Expected number of events with failure of type \( i \)
- \( n_i \): Observed number of events with failure of type \( i \)
- \( m_i \): Observed number of events with type \( i \)-situations
- \( m \): Total number of observed events in the data base
- \( \mu \): Average number of observed events (=m/2)
- \( s_n \): Expected deviation (empirically estimated: 12.5)

The Rasch model performs a calibration by considering situational conditions (D) and cognitive abilities (X). It attempts to consider that plant experience is always incomplete information for generating a HEP=\( \frac{n}{N} \) due to the event-threshold. The event threshold may lead to

---


• an over-estimation of probability if relationship of recorded errors type i to recorded events of type i is used to generate a HEP (because the set of data is incomplete)

• an under-estimation of probability if relationship of recorded errors type i to all events of type i is used to generate a HEP (because errors may occur also below the event threshold)

The Rasch model considers the proportion of errors in events and uses this proportion to correct the observed relative number. It is making a hypothesis about how the proportion will continue below the event-threshold.

Table 5 illustrates, how the comparison of predictions of THERP with the observed errors was performed.

Table 5: Database Queries for Quantitative Predictions from the Investigation

a) Database Queries

<table>
<thead>
<tr>
<th>THERP-Item 20-6 (3)</th>
<th>Corresponding Database-Query... for</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Use operating procedures under normal conditions&quot;</td>
<td>TaskOrder.Object=Procedure AND Situation.Object=Type A OR Situation.Object=Type B OR Situation.Object=Type Ba</td>
<td>(mi+ni ) Query searches for all events where a procedure in pre-initiator and initiator situations was used</td>
</tr>
<tr>
<td></td>
<td>TaskOrder.Object=Procedure AND Situation.Object=Type A OR Situation.Object=Type B OR Situation.Object=Type Ba AND Task.Error=(any error) OR Action.Error=(any error)</td>
<td>(ni) Query searches for all events where an error occurred by using a procedure in pre-initiator and initiator situations</td>
</tr>
</tbody>
</table>

HEP = 0.01
EF= 3
Frequeny: 19 errors in 151 similar events

b) Quantitative Predictions

<table>
<thead>
<tr>
<th>Steps</th>
<th>Calculations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Frequencies of the error within the observed events</td>
<td>n(Failures)=19 &lt;br&gt; n(Successes+Failures)=151</td>
</tr>
<tr>
<td>• Relative frequencies represent the difficulty of the situation</td>
<td>n'=n(Failures) / n(Successes+Failures) <em>165 &lt;br&gt; = 0.13</em>165</td>
</tr>
<tr>
<td>• Estimation of probabilities from difficulty measure by Rasch model calibrated with THERP-data</td>
<td>P=7.11E-03 &lt;br&gt; EF=6.7, based on (Bayes)</td>
</tr>
</tbody>
</table>
Probabilities of occurrence were calculated for 79 situations that are similar to corresponding items of the THERP handbook. As an example, the THERP-Item 20-01(1) was realized as the query "All errors of omission and errors of commission that were made within the 1st minute of a recovery-situation". To determine the relative number, all events were determined where a time for diagnosis was mentioned (i.e., events where no diagnosis time was mentioned have to be left aside to make a statement about time-reliability). Another example is: All events where an omission occurred by using a procedure (THERP-Item 20-07). To determine the relative number in this case, only those events were considered where a procedure was used.

In this way, the data obtained by event evaluation have been compared with the human reliability data provided in the THERP data tables and in the French PSA studies (EPS 900, 1990)\textsuperscript{54}. Similarities and differences of the data are described in the following and discussed in detail in Strätter (1997)\textsuperscript{55}.

Figure 9 shows the HEPs of the handbook compared with the probabilities estimated from the events. As the figure shows, the data derived from the events fits well to the data of the THERP handbook. The correlation is about r=0.88 for the raw data and about r=0.81 for the logarithm of the raw data. Most of the calculated probabilities (75\%) are inside the uncertainty bounds of the items given in THERP. Uncertainties in the calculated probabilities are mainly the result of lacking information in the event descriptions, but there were also found some deviations with importance for adjusting HEPs, especially concerning the handling of procedures in maintenance compared with normal procedures.


\textsuperscript{55} "Op. cit., Strätter (1997)".
HEP-Values of the THERP Handbook

Figure 9: Comparison of the THERP handbook data and the data derived from 165 events.

The presented approach of quantification is different to a 'classical' laplasian definition of HEPs and is more related to psychological findings about the principal problem of quantification of human performance (cf. Adams, 1982\textsuperscript{56}; Heslinga & Arnold, 1993\textsuperscript{57}) and a good overview about this problem in Fischer (1974)\textsuperscript{58}. Because of the importance of quantification in HRA and this psychological reasonable approach on assessing human reliability, a detailed discussion of these findings and implications in necessary and currently prepared.

2c Deductive Qualitative View: Some Qualitative Results

2c.1 Observed PSFs

In the event description PSFs were mentioned not in every case. However, it was able to identify major root causes (in total 30 PSF) in qualitative terms as well as interrelations of PSFs (i.e. multiple


115
PSFs of ergonomic, organizational or personal nature mentioned as important for an error). These interrelations cover the fact that human errors are usually influenced by multiple PSFs.

The PSFs may be summarized as follows (number of observations is mentioned in brackets, multiple PSFs may have occurred in one event):

Task:
- Task preparation: lack in planning, organization or preparation of task (13)
- Task precision: lack of precision of a task (7)
- Task complexity: task was too complex in the given situation (6)
- Time pressure: time pressure caused trouble in performing the task (6)
- Task simplicity: task is originally simple and small deviations in the given situation were not considered (3)

Task-Order:
- Completeness of procedures: procedures don’t contain all necessary information (24)
- Presence of procedures: procedures do not exist for the given situation (7)
- Design of procedures: procedures are ergonomically bad designed (4)
- Precision of procedures: procedures don’t provide precise preconditions or parameters for action (3)
- Content of procedures: procedures contain wrong information (1)

Person:
- Goal reduction: person simplified the task and reduced the goal to be accomplished (11)
- Information: person ignored information provided by the system (8)
- Processing: person performed task without attention although it was required (7)

Action:
- Usability of control: control-systems are bad to handle for operators (12)
- Positioning: control-systems are difficult to be brought into a certain position (e.g. open, close, 50% open) (7)
- Quality assurance: quality assurance is the only way to check functioning of equipment but was not used (7)
- Equivocation of equipment: equipment is not designed such that it can be used without mixing up (e.g. two plugs with different functions are fitting in the same socket) (6)
- Usability of equipment: equipment (some movable part) is bad to handle for operators (4)
• Monotony: action is monotone and typical vigilance effects occur (indolence, search for change) (4)

Feedback:
• Arrangement of equipment: equipment (e.g. displays) is not arranged according to the task to perform (6)
• Marking: semantic meaning of system states linked with a certain value of a process parameter is not marked (6)
• Labeling: display is not or badly labeled (5)
• Display precision: display does not show the process parameter precisely enough (4)
• Reliability: display is unreliable and hence operators' belief in it is low, or it is not expected that it might display wrong information (2)
• Display range: display is not capable of displaying the current value of a process parameter (1)

System:
• Construction: a system (like diesel, conduit) is badly constructed so that it is obstructive for operators (8)
• Coupled equipment: electrical equipment that is supposed to be redundant had impact on each other or is coupled (6)
• Technical layout: layout of technical system is beyond necessary condition (e.g. cable too thin) (4)
• Redundancy: several redundancies are affected (e.g. unavailability of several redundancies due to maintenance work or other common causes) (4)
• External event: an unforeseen external event caused technical failure (1)

The most frequently observed factors are concerning procedures and process feedback. The completeness of procedures is a salient factor for failures. Nevertheless, single PSFs do not exhibit that strong effect that is often ascribed to them. As discussed above, the interrelations of PSFs give more insights into the error mechanisms especially if cognitive errors and organizational impacts are to be analyzed. The concept of cognitive dissonance was found appropriate to understand how these cognitive aspects interact to produce cognitive errors. A detailed treatment of the interrelations provides a deeper understanding of cognitive error mechanisms and organizational aspects (see Sträter, 1997).59

2c.2 Interrelations of PSFs

In Sträter (1997)\textsuperscript{60} the interrelations of influencing factors (PSFs - Performance Shaping Factors) were analyzed to get information about the role of cognitive processes for understanding human errors. A NMDS (Non-Metrical Multi-Dimensional Scaling) was found as an appropriate method for this investigation. Figure 10 shows the result of a NMDS of the interrelations of the PSFs. PSFs influencing cognitive processes are bordered by the thick line. A NMDS is in principal comparable with a factor analysis. According to the figure, four general areas were found for explanation of human errors: task perception vs. task performance on the one hand and usual tasks vs. unexpected tasks on the other hand. These areas may be condensed to two factors that are responsible for human errors: (1) cognitive processes (from task perception to task performance) and (2) situational conditions (from usual tasks to unusual tasks).

![Graph showing interrelations of human performance and cognitive errors.](image)

Figure 10: Interrelations of influences on Human performance and their importance for cognitive errors (from Sträter, 1997)\textsuperscript{61}.

The figure shows a vertically oriented cloud of PSFs that were observed together with cognitive errors. The shape of this cloud indicates that cognitive errors occur in the transition from usual tasks to unusual tasks: They occur, if the situation is not clearly/obviously erroneous or if the situation is not clearly/obviously a usual one. Cognitive errors do not occur in situations that are clearly/obviously complex or usual. Therefore, it may be concluded that cognitive errors happen if

\textsuperscript{60} "Op. cit., 4, Sträter (1997)".

\textsuperscript{61} "Op. cit., 4, Sträter (1997)".
the established heuristics of operators do not work as planned but were used in the expectation that they will work.

Table 6: Relation of Cognitive dissonance and Situational complexity

<table>
<thead>
<tr>
<th>Principal error types (x), samples for typical PSFs (x) and cognitive behavior (z)</th>
<th>Cognitive dissonance</th>
<th>no dissonance (Operator does not care about situation)</th>
<th>dissonance (Operator cares about situation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Situational complexity</td>
<td>apparently simple</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cognitive dissonance</td>
<td>X Omission (e.g., no action)</td>
<td>X omission (e.g., no action) or commissions (e.g., wrong action)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Y marking, labelling</td>
<td>Y reliability and equivocation of equipment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Z fixation</td>
<td>Z frequency oriented reasoning</td>
<td></td>
</tr>
<tr>
<td>Obviously complex</td>
<td>X quantitative commissions (e.g., too much/less)</td>
<td>X delay (e.g., too late)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Y precision and design of procedures</td>
<td>Y arrangement of equipment, reliability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Z eagerness to act</td>
<td>Z reluctance to act</td>
<td></td>
</tr>
</tbody>
</table>

By this simple and basic mechanism, many types of human errors may be explained: Why do operators circumvent orders? Why do they nothing, even if the system clearly needs control? Why do they make control actions even if the system does not require them? Answers to these questions may be provided by the way how the above mentioned factors do interact within a certain error situation. This relation is outlined in Table 6. Note, that the term ‘situation’ is to be understood from the cognitive point of view and is different from the one used in PSA context. From the cognitive point of view it is describing the cognitive coping process, an operator uses to cope with a certain PSA-situation. Consequently one PSA-situation may lead to several cognitive situations.

The reader who is familiar with cognitive models may notice that this classification of cognitive processes describes very basic processes. These processes are based on the specific knowledge of operators about a given situation.

Such a view on cognition is going beyond the descriptive models as proposed by Sternberg or Rasmussen for instance. Such descriptive models assume that cognitive error mechanisms are to be classified according to certain stages (like perception, decision, action; Sternberg, 1969) or certain phases (like skill-, rule-, knowledge-based; Rasmussen, 1986\footnote{Op. cit., 3, Rasmussen (1986)} of cognition. In contrast to such assumptions, the observation shows that there cannot be assumed a certain relationship between stages (or phases), errors and influencing factors. In order to understand these basic cognitive mechanisms, it was observed that the analysis of interrelations of PSFs is more important. The observation suggests that the basic mechanisms are to a great extend independent from the phases or

\[ \text{119} \]
stages where they come into play. Due to this, problems of classification of cognitive processes in descriptive models are arising.

Descriptive models currently used in HRA are frequently not explaining effects that were observed as responsible for cognitive errors in this investigation and are well known in psychological literature. Examples for these are:

- Attention may be distributed and focused
- Memory span is limited; contents of memory are interfering according to certain mechanisms
- Emotions, motivations and attitudes impact cognitive processes
- External and internal cues impact the cognitive processes
- Cues and goals interrelate within a cognitive act
- Sluggishness of decisions and the hysteresis of attitudes during a current track of diagnosis are to be explained and predicted
- Heuristics (learned patterns), like proposed by Tversky & Kahneman (1974), play a leading role in explaining cognitive human recognition and behavior
- Behavior is based on the given information within a situation, the goals an operator has, and the neural links for processing (representing the experience of the operator)

3. Describe the Findings from the Analyses

The CAHR-method shortly presented in this paper is a preliminary approach to evaluate plant experience for Human Reliability Assessment in Probabilistic Safety Assessments. Of course, further developments are necessary and are currently performed at GRS.

3a. Findings Regarding the Method Used, Especially Theoretical Insights, Practical Lessons Learned, and Data Input and Output

The presented method may be a starting point to improve Human Reliability data collection systematically. It may provide various human reliability data (e.g., for supporting the system analysts in the definition of important initiating events). By a wider application and by further event evaluations it would also provide a growing knowledge about human error mechanisms. Though applied here for human factor related events, it may also be a reasonable procedure to analyze other data as well as (e.g. simulator experiments). Due to the chosen approach of the structure formation technique instead of a fixed classification, the suggested procedure may also enable data collection in a wide range of safety relevant industries (e.g., for aviation or conventional power or chemical plants). By such a procedure, the assessment process becomes a living procedure that is increasing its knowledge with a growing collection of events.

Typical application fields for the presented approach are the currently discussed assessment problems of HRA such as assessment of cognitive errors or organizational impacts especially during low-power and shut-down modes. Here, the presented approach may be used for validation and
comparison of data used in other new approaches (e.g. INTENT, Gertman et al, 1992\textsuperscript{64}; ATHEANA, NUREG-1624, 1998; CREAM, Hollnagel, 1998\textsuperscript{65}) or for complementing these approaches. How the method may be used for analysis and assessment of errors of commission may be illustrated by its application as outlined in chapter 3b.

Also, some disadvantages were observed that currently inhibit a wider use of the method. These are mainly:

- An improvement of the usability of the database is necessary, especially concerning the interactive analysis of events
- The information source has to be improved by detailed analysis and discussions about the events
- A general accepted compromise between open and closed classification should be found
- A concise description of the procedure and a glossary should be developed
- The used calibration / regression with the Rasch-model is mathematical reasonable but currently not validated.
- Further events should be analyzed in order to achieve validation
- CAHR is currently no HRA method in the PRA sense, because a systematic search scheme is lacking. It is more providing a framework for analysis of events and a tool for providing data for qualitative and quantitative predictions.

Table 7 summarizes the prospectives of the approach and the advantages and disadvantages of the method observed so far.

\textsuperscript{64} "Op. cit., 38, Gertman (1992)".

Table 7: Prospective of the CAHR -approach.

<table>
<thead>
<tr>
<th>Advantages of the methodological qualitative approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Context, Situation and Cognition: Method provides an operational definition of context: By using the MMS it considers ergonomic, cognitive, organizational and technical aspects</td>
</tr>
<tr>
<td>• Multiple parameter approach: Dependencies between actions, errors and PSFs are represented by using a connectionism network</td>
</tr>
</tbody>
</table>

Advantages of the methodological approach for quantification

| • minimal-square approach considers all reference-values for calibration |
| • reduced variability because not only one or two anchor values are used (other calibration methods may have high variation if using other anchors) |
| • single parameter (s_y) is adjusting calibration to THERP-values |
| • possibility to replicate the way how data were derived (even down to an event) |
| • possibility to meet scientific criteria of traceability |

Disadvantages of current application

| • quality of the underlying event descriptions not high |
| • inter-rater reliability for event evaluation not measured |
| • inter-rater reliability for data-base queries for THERP-Items not measured |
| • currently no validation of calibration with the Rasch-model (is planned) |

Current status of work

| • evaluation of additional 55 events of PWR as a comparison study performed in 1999 (Sträter & Reer, 1999)66 |
| • further mathematical insights into the quantification with the Rasch-model performed in 1999 (Reer et al., 1999)67 |
| • comparison with expert judgments of German utilities |

3b. Findings Regarding Errors of Commission, Especially Contributors to These Errors and Consequences of These Errors in the Event or Accident Sequence Analyzed

The method as it is currently developed was used for the analysis of 165 events from German plants and was initially applied for assessment of human interactions in Accident Management (AM, Sträter, 1996) and Low Power and Shut Down states (LP&SD, Sträter & Zander, 1998)68. The application of the method in these studies may illustrate, how it may be used for assessment of errors of commission, because the general procedure is identical.

---


3b.1 Assessment of Human Interactions in Accident Management

The CAHR-method has been used at first for assessment of human interactions in Accident Management during the scenario "reinforced flush of control-rods" (Sträter, 1996).

- Procedure and Effort

The assessment process in CAHR is different compared with THERP or HCR. In CAHR the most important situational characteristics have to be investigated and assessed. Compared with other methods, the quantification process of CAHR has principal differences:

- Dependencies are included in the observed error frequencies and have not to be considered as single error contribution like in THERP for instance. They need not to be modeled explicitly. The connectionism approach takes implicitly care about the dependencies.

- A failure of the whole action may be caused by communication or other failures. The defined query to the data-base regulates whether these are included in the observed error frequencies.

- The assessment-unit is the situation or error context. The situation is assessed and neither the single tasks (like in decompositional methods) nor the whole sequence of the scenario (like in holistic models). Hence, it is not as detailed as THERP where every sub-task has to be assessed but more detailed as HCR.

- Task-elements that have to be separated in THERP may be treated together (e.g., omission due to wrong procedure or communication error may be treated in one data-base query).

- Errors to be assessed are modeled only once (e.g. communication errors are covered by one assessment and don't have to be assessed every time for that sub-task where they might have an impact on).

These advantages may be used for a more straightforward assessment as it is performed by THERP and a more sophisticated assessment as it is possible to perform with HCR. This leads also to some simplifications concerning the whole process of HRA. As the following example shows, this simplification is not accompanied by a reduction of evidence concerning quantification, PSFs or possible improvements (as it is the case in HCR), because CAHR is based on real events.

- Quantification

For each of the identified action-steps, one situational query to the data bank of the collected plant experience was defined and frequencies of errors in similar situations were determined. The query may specify (1) the system component that is involved, (2) the action that has to be performed, (3) the error, and (4) identified PSFs. Each query may be proceeded on any level of detail on which an analytic statement is needed (i.e. general queries for screening vs. specific queries for detailed assessment). Table 8 summarizes the observed frequencies according to the considered action-steps of the operators' model.
Each frequency of occurrence may be taken as a rating for the difficulty that the operators have to perform the situation correctly. To gain probabilities from this difficulty-measure, Rasch (1980)\textsuperscript{69} suggested to assume a simple functional relation between difficulty and probability. Hence, for each frequency of occurrence the probabilities of occurrence were calculated according to a normalized probabilistic model after Rasch by formula (2), see chapter 2. Following this formula, the HEPs according to Table 8 are calculated for the different steps of the action sequence.

The model also assumes a simple calculation of dependencies as shown in Table 8: If one intends to assume dependencies between different action steps, he simply has to add the frequencies of occurrence of those steps that are depending on each other before estimating the probability for the steps as a whole. Hence, assuming dependencies between all diagnosis activities, one has to add all frequencies of the diagnosis steps first. After that, formula 2 is used for estimating the probability for diagnosis (column marked 'Dependency of either Diagnosis or Action'). Assuming dependencies between all action steps one has to add all frequencies of the entire sequence before calculating the dependency (column marked 'Complete Dependence'). Therefore, depending on the degree of dependency that is assumed by the analyst for the sequence, three different HEPs may be estimated for the entire emergency procedure:

\[
\begin{align*}
\text{HEP}_{\text{independent}} &= 0.03 \\
\text{HEP}_{\text{middle}} &= 0.11 \\
\text{HEP}_{\text{dependent}} &= 0.26
\end{align*}
\]

\textsuperscript{69} "Op. cit., 49, Rasch (1980)."
Table 8: Detailed calculation of the reliability of the operators' actions in the AM sequence.

Assessment of the AM-scenario "Reinforced flush of control-rods"

<table>
<thead>
<tr>
<th>Action Step</th>
<th>Independence</th>
<th>Diagnosis or Action</th>
<th>Complete Dependence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>EF</td>
<td>n(Step)</td>
</tr>
<tr>
<td>Diagnosis Part</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Recognition</td>
<td>1</td>
<td>4,81</td>
<td>1</td>
</tr>
<tr>
<td>2. Attempts on feet-water</td>
<td>2</td>
<td>5,43</td>
<td>2</td>
</tr>
<tr>
<td>3. Failure of high injection</td>
<td>4</td>
<td>7,77</td>
<td>4</td>
</tr>
<tr>
<td>4. Communication</td>
<td>6</td>
<td>1,00</td>
<td>6</td>
</tr>
<tr>
<td>5. After SCRAM</td>
<td>6</td>
<td>1,34</td>
<td>6</td>
</tr>
<tr>
<td>6. Waiting for RS</td>
<td>3</td>
<td>5,00</td>
<td>3</td>
</tr>
<tr>
<td>7. Check of automatic of RS</td>
<td>6</td>
<td>1,00</td>
<td>6</td>
</tr>
<tr>
<td>8. Changing level meter</td>
<td>4</td>
<td>1,00</td>
<td>4</td>
</tr>
<tr>
<td>9. Attempts on auxiliary feed-water</td>
<td>5</td>
<td>7,28</td>
<td>5</td>
</tr>
<tr>
<td>10. Decision to wait for RS</td>
<td>11</td>
<td>1,05</td>
<td>11</td>
</tr>
<tr>
<td>11. Attempts on de-pressurize</td>
<td>2</td>
<td>5,43</td>
<td>2</td>
</tr>
<tr>
<td>12. Decision to use AM procedure</td>
<td>4</td>
<td>4,72</td>
<td>4</td>
</tr>
<tr>
<td>13. Alarming</td>
<td>2</td>
<td>4,50</td>
<td>2</td>
</tr>
<tr>
<td>Action Part</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Violation of Procedure</td>
<td>3</td>
<td>1,00</td>
<td>3</td>
</tr>
<tr>
<td>15. Performing the AM-action</td>
<td>11</td>
<td>5,43</td>
<td>11</td>
</tr>
<tr>
<td>Sum</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EF</td>
<td>70</td>
<td>6,31</td>
<td></td>
</tr>
<tr>
<td>n(Independent)</td>
<td></td>
<td></td>
<td>3,05E-02</td>
</tr>
<tr>
<td>n(middle)</td>
<td></td>
<td></td>
<td>1,92E-01</td>
</tr>
<tr>
<td>n(dependent)</td>
<td></td>
<td></td>
<td>4,82E-03</td>
</tr>
</tbody>
</table>

The detailed unavailability of human actions calculated by CAHR are shown in Figure 11 (for simplification $m_i$ was set to $m$ in this calculation; this leads to optimistic values).

Figure 11: Predictions of CAHR for the 15 action-steps within the AM-sequence.

- Measures for improvement

Beside quantification, for every action step the PSFs may be determined by the database algorithm. For that purpose, the database algorithm looks for all events in the collected plant experience where

125
circumstances were observed that are similar to those of the action steps of the AM-scenario. Using this feature of the database leads to the most important contributing PSF and to the most effective measures for improvement. Figure 12 is showing the PSFs that were a result of the database query for all action steps of the AM-scenario. See chapter 2 for detailed discussion of the PSFs.

Compared with the extensive THERP procedure, similar PSFs are identified for the reliability of the entire sequence. These are diagnosis-based decisions of the operator and quality of the emergency procedures. Furthermore the CAHR method has identified additional PSFs: The most important ones are task-preparation and knowledge of the operator. These measures were not obtained by THERP but were discussed with the plant staff as important contributing factors. Summarizing, the advantage of the CAHR procedure is that measures for improvement are more detailed and realistic: PSFs may be gained directly by considering the knowledge about PSFs that is contained within the database of similar events being observed in the past.

![PSF frequencies](image)

- Figure 12: Predicted PSF and frequencies of observations in events that are comparable to the AM-scenario.

- Comparison with THERP and HCR

Figure 13 is comparing the results of quantification of all HRA-methods that were used in BWR-study for assessing the above described scenario.

As the figure indicates, the HEPs obtained by CAHR provide a broader view to the entire sequence enabling to see the impact of dependencies. Nevertheless, assuming at least some or complete dependency, CAHR is providing nearly the same results as THERP or HCR. THERP and CAHR also agree quiet well on the impact of the diagnosis and action part. Note, that the assessment of all methods is based on the same model of operators' behavior mentioned above.
As the short overview about CAHR shows, it is able to give estimates similar to those of THERP or HCR and is leading to a more detailed view on PSFs. This opportunity makes HRA easier and hence more suitable for assessment of AM scenarios, because in AM assessment each path of an event-tree has its specific situational aspects (e.g., time constrains) that has to be calculated for their own (path dependent assessment). Concluding, it seems to be an appropriate procedure to provide estimates for qualitative and quantitative assessment. The underlying reason for this advantage is that CAHR proceeds situation related and neither exclusively error related like THERP nor exclusively time related like HCR. Nevertheless, CAHR may consider both approaches as one possibility to assess a situation. Other accesses are cognitive demands, organizational tasks or errors under certain PSFs for instance.

![Graph showing comparison of quantitative predictions of different HRA-methods.]

Figure 13: Comparison of quantitative predictions of different HRA-methods.

3b.2 Application on Assessment of Human Interactions in Low Power and Shut Down States

- Background

Funded by the Federal Ministry of Education, Science, Research and Technology (BMBF), Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) has been performing a probabilistic analysis for a boiling water reactor (BWR) during low-power and shut-down (LP&SD) states. The reference plant is Gundremmingen NPP with a twin unit of 1344-MW electrical power each. Strüter and Zander (1998)\(^7\) are discussing some problems that were observed within the study, especially concerning human reliability assessment and data issues. The CAHR method was tested to approach some of the limitations in modeling human reliability in order to achieve a more realistic assessment of risk in shutdown states.

---

\(^7\) "Op. cit., 68, Strüter and Zander (1998)".
Actual methods for evaluating human errors are mainly designed for dealing with rule-based actions. These methods are considering PSFs (Performance Shaping Factors) like stress factors, completeness of procedures and training, and time available for performing a required task as parameters for assessment. Common known approaches are THERP (Swain & Guttmann, 1983)\textsuperscript{71}, ASEF (Swain, 1987)\textsuperscript{72} and HCR (Hanaman & Spurgin, 1984a)\textsuperscript{73}. For assessing human reliability in full power operation, these methods are broadly accepted.

In shutdown states, additional circumstances have to be considered by which appropriate assessment of human interactions with such methods becomes difficult. Important tasks and their circumstances are different compared to full power operation. Usually, a lot more time is available for avoiding hazardous states during shutdown periods. In contrast to this, the application of current assessment methods for human interactions is limited to time windows of about one hour of mission time for success. Moreover, for some of the sequences, precise procedures are not prepared for supporting the decision making process of shift personnel. Thus, knowledge based behavior plays a larger role. Such additional circumstances have effects on the modeling of the whole event sequence as well as on the assessment of certain human interactions.

- Some of the Observed Difficulties in Assessment

Administrative aspects: One difficulty in assessment is the organizational impact on human performance: Compared to full power operation, the role of administrative barriers like communication between personnel is increasing and therefore, communication is a more decisive aspect of human reliability during LP&SD states, especially if the way of communication is not prescribed in detail like in unusual maintenance tasks (in the LP&SD-study it was found that the activities for exchanging an internal recirculation pump shaft may be an example for that). INTENT (Gertman et al., 1992)\textsuperscript{74} was tested as one approach to consider these communication aspects. However, INTENT is a so-called holistic approach that does not allow a detailed comparison of various communication paths (Reer et al., 1996). Typical effects on the reliability of communication are not considered in this approach. Examples for these effects are group-structure (in-group vs. out-group effects), reluctance against unknown groups or persons, or the coherency between trust and acquaintance (see for details e.g. Schuler, 1995)\textsuperscript{75}. Consequently, a fault-tree based approach was used in this study to compare various administrative solutions for the maintenance task. Such an approach was also found as more useful to model the above mentioned effects during communication. Data were taken from the CAHR-approach (Sträter, 1996; 1997a)\textsuperscript{76} and

\textsuperscript{71} "Op. cit., 33, Swain & Guttmann (1983)"

\textsuperscript{72} "Op. cit. 43, Swain (1987)"

\textsuperscript{73} "Op. cit. 40, Hannaman & Spurgin (1984a)"

\textsuperscript{74} "Op. cit. 38, Gertman (1992)"

\textsuperscript{75} "Op. cit. 37, Schuler (1995)"

\textsuperscript{76} "Op. cit. 4, Sträter (1997)"
alternatively from the THERP-tables. By using this modeling approach of different communication paths, an optimal administrative solution for the maintenance task was identified.

Types of actions: Other observed disadvantages of applying ASEP on LP&SD states concern the similar treatment of actions with different nature: placing a fuel-element in a certain position, re-configuring electrically unavailable equipment in the plant, or starting a pump from the control room is assessed by ASEP in the same way. Additionally, methods like THERP may provide some distinctive data for some type of tasks. However, the principal problem of current HRA-methods is still present: They were designed for assessment in full power operation. An example for this effect is:

An action well known from operational experience like positioning fuel elements in the spent fuel pool has to be assessed by ASEP with at least P=2E-2. In plant experience, irregularities are observed in far less than these 1 per 50 fuel-elements.

An assessment with the CAHR approach was tested here. Its preliminary application and comparison to the other methods used is summarized in Table 9. As a further development of the CAHR-method, error factors were calculated in this study by using a Basian calculation of the 5% and 95% percentile of the difficulty measure (i.e. the observed relative frequency).

Table 9: Assessments with the CAHR approach in comparison to results of other methods used in the LP&SD-study.

<table>
<thead>
<tr>
<th>Assessment aspect</th>
<th>Method</th>
<th>THERP</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative aspects:</td>
<td>CAHR</td>
<td>THERP</td>
<td></td>
</tr>
<tr>
<td>• Communication (direct, oral, face to face)</td>
<td>P=1.62E-03 EF=6.7</td>
<td>P=1.00E-03 EF=3</td>
<td>THERP only applicable with additional assumptions concerning nature of error (i.e. median of Table 20-8 Item 1 reflects errors due to misunderstanding by direct communication).</td>
</tr>
<tr>
<td>• Communication (indirect, oral, by telephone)</td>
<td>P=2.74E-03 EF=2.5</td>
<td>P=3.00E-03 EF=3</td>
<td>THERP only applicable with additional assumptions concerning nature of error (i.e. upper bound of Table 20-8 Item 1 reflects errors due to misunderstanding by indirect communication).</td>
</tr>
<tr>
<td>Types of actions:</td>
<td>CAHR</td>
<td>ASEP</td>
<td></td>
</tr>
<tr>
<td>• positioning of a fuel element under abnormal circumstances</td>
<td>P=1.92E-03 EF=6.6</td>
<td>P=4.81E-03 EF=13.5</td>
<td>ASEP only applicable with additional assumptions concerning error and recovery and by using a fault tree approach.</td>
</tr>
<tr>
<td>• availability of a certain tool outside CR</td>
<td>P=3.27E-03 EF=6.5</td>
<td>P=4.81E-03 EF=9.7</td>
<td>ASEP only applicable with additional assumptions concerning error and recovery and by using a fault tree approach.</td>
</tr>
</tbody>
</table>

129
3b.3 Application of the Method for Assessment of Errors of Commissions

Currently, the same procedure is used to make estimates about errors of commissions. For this purpose, a comparison with the errors of intention provided in the INTENT-method was performed (Sträter, 1998a)\textsuperscript{77}. Further on, the errors of commissions observed during the Davis-Besse event were assessed with CAHR during a common work of PSI (Paul Scherrer Institute) and GRS. The assessment procedure is the same as described above. The interested reader is referred to Reer et al. (1999)\textsuperscript{78} or Sträter et al. (1999).

4. Provide Definitions of Terms and Parameters Used in Responses to the Questions Listed above

Until now, there is no document available that provides definitions of terms and parameters used in CAHR. The major work is documented in Sträter (1997)\textsuperscript{79}, see also Sträter & Bubb (1999)\textsuperscript{80}. Parameters and definitions are included in the database program that is mentioned in chapter 1 and is available in German language.

Acknowledgments

The author would like to thank Prof. Dr. Heiner Bubb (Institute of Ergonomics, Technical University of Munich, Germany), Prof. Dr. Bernhard Zimolong (Ruhr-University Bochum, Germany), and Dr. Bernhard Reer (Paul Scherrer Institute, Switzerland) for the interesting and fruitful discussions about the ideas and approaches presented in this paper.


\textsuperscript{78} "Op. cit., 67, Reer, Sträter (1999)".

\textsuperscript{79} "Op. cit., 4, Sträter (1997)".

Contribution from Hungary
Human Reliability Analysis - Errors of Commission

Attila Bareith
VEIKI Institute for Electric Power Research, Hungary

Background

In the past and ongoing probabilistic safety assessment (PSA) studies for the Paks NPP of Hungary, human reliability assessment (HRA) was based on a range of methods and data sources. Within these studies use was made of the following methods:
- THERP³ and ASEP HRA² with modifications) for pre-initiator errors within full power PSA
- HCR¹, HCR_ORE¹, SLIM² and a decision tree approach⁶ to construct crew reliability models applied to post-initiator operator errors within both full power as well as low power and shutdown PSAs

The above-mentioned first generation HRA methods were, in most cases, applied with modifications to allow for an evaluation of cognitive nature of human errors and to better reflect data (field data or simulator data) that were made available or generated for the purpose of HRA.

A recurrent problem of the PSA/HRA efforts for Paks has been the difficulty to adequately represent the context dependent nature of human activity/reliability in terms of specifics of scenario/situation and other human or machine related influences (performance shaping factors). Another important shortcoming has been the oversimplistic modeling of human cognition as given in most first generation HRA methods. Simulator experiments and expert opinion were used to make up for these deficiencies, at least to some extent⁷. Also, an analysis of shutdown operational records has helped the extension of PSA/HRA to low power and shutdown plant operational states.

---

So far no specific attempt has been made within the PSA studies for Paks to particularly address human "errors of commission" in the sense defined in either\(^8\) or\(^9\). It is noted, however, that a lot of the human system interactions analyzed in the PSAs for the Paks NPP cover or overlap with the definition of commission. It is mainly because commission corresponds to numerous different types of actions as described in\(^{10}\). Although the omission-commission categorization gives a seemingly simple "taxonomy", in practice it can be difficult, sometimes arbitrary, to label a complex human-system interaction or even a specific action/error as error of commission. In a safety analysis one would not just look for errors of commission but try to at least understand and model
- the situation in which humans are required to operate including the demand placed on them
- the conditions representing the situation and their likely effect on human performance
- the anticipated critical failure modes of the human-machine system including errors made by humans.

Parallel with this understanding a quantitative assessment should provide probabilistic estimates for the critical failures of the human-machine system.

Although past and current HRA developments and applications for Paks have not been particularly centered around errors of commission, some of the ongoing safety analyses can be used as demonstration of case studies that include commission type errors. Probably the most important of these analyses is the identification and probabilistic modeling of scenarios that lead to an inadvertent dilution of the primary coolant and, as a result, endanger core integrity by causing a reactivity transient through lowering the boron concentration. The study covers all the allowable plant operational states including full power, low power as well as shutdown operation. Consequently, the analysis is not limited to operator actions, but it also deals with maintenance and other-operations during an outage. With reference to the usual categorization of human actions in a PSA, this analysis deals with all types of interactions, i.e. pre-initiator, initiator and post-initiator actions/errors that may be important from the point of view of development of a dilution accident.

The study is not aimed at developing a stand-alone method for error analysis. However, the insights are expected to support efforts in that direction.

The overall approach followed was an integrated system and human reliability analysis. It means that safety significant human-system interactions were identified during a process that included a detailed evaluation of both system and human related causes, of potential dilution scenarios without rigid separation of HRA from the rest of the analysis. The analysis process is further outlined under question 1c below.

The quantification of safety significant actions was based mainly on expert judgment with support from an analysis of relevant operating experience. Quantification was aimed at estimating human error probabilities or human error rates as well as producing estimates of core melt frequency or probability.

1b. A description of the underlying concepts of the analysis method used (that is, reference to human sciences, if relevant):

\(^8\) "Op. cit., 1, Swain, A. D., Guttamann, August 1983".
In general the needs of the HRA are quite simply to have a model which correctly answers questions about the errors that the operators (and other plant personnel) make, accurately and easily. Humans are quite complex and therefore the need cannot be satisfied simply. Up to now, PSAs have been more concerned with addressing equipment related issues and failed to more closely address the human problem. However, there is growing requirement to more properly address this area in PSAs. One of the requirements for a suitable description of humans in the context of the PSA is that it should be based on human behavior concepts.

The model should be built upon how persons behave under accident and operational conditions. Persons are affected by the way that information is presented to them, helped by appropriately designed procedures, perform better when challenged, when the time for response is not too long or too short, etc. These are the factors which should be considered in the construction of a suitable HRA method.

During the process of analyzing dilution scenarios an attempt was made to incorporate some important behavior concepts. What was considered important in the first place was the idea that the human response is very much affected by the situation or context under which the action is taking place. There are two sets of contextual conditions. These are the effects of the accident scenario and the other is the plant condition, including management effects. For example, the area of the human-machine interface (MMI) affected by the accident scenario has a direct effect on the operator and is a local effect. The influence of management decisions, for example in the case of maintenance, the allocation of funds sets the level of manpower used for maintenance and is a global effect.

Some of the other human behavior concepts are split-up between cognitive and manual tasks, errors of omission and commission, influence of different environments on operator reliability, effect of time under certain circumstances, i.e. failure to take an action in a timely manner, etc. If the analyst considers the split-up between cognitive and manual activity, the additional effect of a manual operation on the overall human error probability (HEP) is not large. The choice is not a limitation of the method. In dealing with errors of omission and commission, here one is dealing with a PSA concept rather than a human error concept.

1c. A summary of the steps taken or the procedure used for conducting the analysis:

The main objectives of the PSA based review of boron dilution faults are to (1) define the contribution of the dilution phenomenon to the overall core damage risk, and (2) identify the dominant dilution scenarios. In order to ensure that the final results are originated from a complete list of potential initiators/scenarios, a procedure has been developed and followed for the systematic identification of initiators, their screening and selection of dominant dilution scenarios. The procedure is outlined in Figure 1. It consists of three main phases as follows:

- preparatory work
- identification of all potential initiators
- screening and evaluation of dominant scenarios.

During the preparatory phase of the PSA based review of boron dilution faults the dilution phenomenon has been described in general and some preliminary analyses have been carried out in order to gain information about the phenomenon itself as well as about the dilution related operational experience. The following sub-tasks were performed within this phase of the study:

133
Figure 1 - Procedure for Analyzing Dilution Scenarios
• identification of the ultimate sources of water with lower boron concentration than that of the primary circuit, from which water can potentially be delivered (through transitions between the systems) to the primary circuit and the core

• identification of generic mechanisms by which water of low boron concentration can be transferred from one system to another and finally into the primary circuit

• analysis of operational experience concerning dilution faults

• estimation of critical volumes and/or concentrations of water that can lead to an undesirable state of the core if added into the primary circuit

The second phase of the study has been aimed at the identification of the complete list of initiators which would result in the dilution of the primary circuit. The complete list was intended to include all possible external and inherent initiators as well. The following were the important sub-tasks within this phase:

• identification of systems connected directly or indirectly to the sources and/or that can be affected by the generic mechanisms defined earlier,

• description and evaluation of system interconnections from the point of view of the possibility of transferring water from one system to another,

• building up chains of transitions systematically from systems to systems starting from a source and ending with the primary circuit, and (as a result) identifying all the potential external initiators,

• systematic identification of inherent initiators that have the potential to occur during normal operation, supplementing the list of external initiators with the list of these inherent ones,

• identification of dilution scenarios that are consequences of other initiating events by a literature overview, supplementing the above list with these initiating events.

Having identified the complete list of the potential initiators a screening process had to be performed in order to (1) exclude unimportant initiators/scenarios, and (2) be able to fulfill the main objectives of the PSA based review of boron dilution faults. The following sub-tasks were performed within this phase of the study:

• screening out initiators with volumes and/or concentrations below the critical value,

• identification of recovery possibilities,

• evaluation of the probability of occurrence of each of the dilution scenarios associated with screened-in initiators by taking into account possible recoveries, and screening out scenarios with low probability of occurrence.

As a result of the above procedure (1) the contribution of the dilution scenarios to the overall core damage risk has been calculated, and (2) a list of dominant dilution scenarios has been produced.
2. Describe in detail the event or sequence analyzed:

The purpose of the study was to assess boron dilution faults which could occur at the Paks NPP. Two main types of the dilution processes have to be distinguished, namely homogeneous and inhomogeneous dilution.

Homogeneous dilution is characterized by the slow decrease of the boron concentration that is uniform in the whole primary circuit or at least in a certain sector of it. Mixing of the added water of low boron concentration and the primary coolant is significant. Since the process is slow, there is a certain time interval during which the dilution process can be detected and appropriate actions can be taken. In general, detection is possible by the following signals:

- unexpected insertion of the control rods, which is caused by the reactor power limiter that tries to balance increased reactor power (during power operation - annunciator signal),
- decrease of the boron concentration by the continuous measurement connected to the charging lines of the make-up water system (during those plant operational states when make-up water system is in operation - unannunciator signal),
- high count rate by the neutron measurement (during shutdown states - unannunciator, but indicated by an audible warning signal, i.e. increased beep rate).

Inhomogeneous dilution is characterized by the fact that mixing of the added water of low boron concentration is not significant; so the change (decrease) in the boron concentration is not uniform for the whole primary circuit; it is rather local. Layering can occur between the water added and the primary coolant, or a slug of diluted water can be generated. In both cases the locally boron weak water may enter the reactor core causing local reactivity increase, and so local damage to the fuel. The dilution process is rather quick, it is not detectable after it has been started, thus no recovery action is possible. However, the potential for such a dilution process can be detected prior to introducing the water of low boron concentration into the primary circuit based on e.g. changes in tank levels, etc.

The start of the dilution of the primary coolant is referred as initiator even if it is a result of multiple errors. An initiator followed by the failure of mitigating systems or any possible recovery action leading at the end to core damage is called a dilution scenario. As discussed above, if the process is a quick inhomogeneous dilution there is no way of recovery after the dilution has been started.

All potential initiators have been accounted for, be they from mechanical failure of equipment, inadvertent system operation, deficiencies in operating procedures, errors by the operators or the build up of slugs of low-borate water within the reactor cooling system during normal operation or following an initiating event. It means the analysis covered a number of events/scenarios considered potentially important with respect to a dilution accident. As an example, some of the potential dilution scenarios will be shortly described in the following chapters.

3. Describe the findings from the analyses, including

3a. Findings regarding the method used, especially theoretical insights, practical lessons learned (e.g., software requirements, expertise requirements, resource requirements), and data input and output:

From among the methods used during the analysis of inadvertent dilution those are thought to be of interest that were applied to model and quantify: (1) initiator type errors and (2) post-initiator human responses.
Erroneous actions, consequence of which is the occurrence of an initiator are commission type errors that entail the operator (or maintainer) undertaking actions that are not required. That is, errors in which the human in the system performs an action, that is not appropriate at the time the action is taken. Various methods have been looked at to examine this problem. A review of open literature has shown that existing methods take their starting point as a task that is required, and then determine the possibility of an error. It means most methods provide a means for examining known tasks that could lead to commission errors, but cannot be applied “in reverse” that is, to show what tasks could result in errors of commission. The most viable way ahead was to derive a method for screening the large number of dilution initiators postulated using methods available for examining violations of rules. (Thousands of potential scenarios were found that required a way of screening.) This was because, in the case of the dilution scenarios, the protection against the commission errors postulated largely, consists of administrative controls, for example rules, procedures and supervision. The two methods used were an HFRG\textsuperscript{11} guide and elements of another (but similar) approach suggested in\textsuperscript{12}.

The result was that each error was considered in terms of the “incentives” that could encourage a violation and the “barriers” that could discourage a violation, and thus prevent the postulated tasks taking place. The approach to an initial quantification for screening purposes, was to evaluate (score) incentives and barriers and consequently increase or decrease a conservative screening probability of 1.0 based on the sum of the scores. The basic assumption of the quantification is that if an incentive is estimated to affect the likelihood of the error strongly, then the error probability increases by an order of magnitude and it affects only in an intermediate degree then by half an order of magnitude. Similarly, if there is a strong barrier, then the error probability decreases by an order of magnitude while in the case of a barrier of an intermediate degree it decreases by half an order of magnitude. In the case of weak or no effect of either an incentive or a barrier the error probability remains unchanged. In order to avoid being too optimistic or too pessimistic the same number of incentives and barriers should be defined in such a way that they cover all areas having the potential to affect the error likelihood and that their weight was the same in general.

After performing an initial screening the screened-in errors of commission needed a refined estimation. The APJ (Absolute Probability Judgment)\textsuperscript{13} method was found to be a technique that could be used for the evaluation since it relies on “expert judgment”, and this is felt to be the most appropriate means of generating “data” for uncommon events. APJ has several different approaches from which the Nominal Group Technique method has been chosen as the one requiring the least time, but allowing discussion between experts. The method consists, briefly, of the following steps:

- Assemble an expert group (those with a detailed knowledge of the plant, the equipment and work conditions relating to the task described in the scenarios)
- Brief participants on what is required of them (to generate human error probabilities) and on the tasks to be considered
- Ask each participant to independently record a human error probability for one of the tasks
- Facilitator examines the judgments to determine whether they agree
- Facilitator encourages discussion of the estimates, in particular any widely varying figures - usually additional factors emerge from this debate
- Ask for each participant, again, to independently derive an estimate
- Check agreement and continue until the results converge sufficiently.

During the APJ sessions organized for the estimation of dilution faults an attempt was made to avoid the following problems with the APJ technique:

\textsuperscript{11} HFRG guide “Improving Compliance with Safety Procedures” published in the UK Health and Safety Executive.
\textsuperscript{12} Nigel Holloway: “SURVIVE” a Safety Analysis Method for a Survey of Rule Violation Incentives and Effects.
• Discussion can be dominated by a strong personality within the expert group (in which case the facilitator must ensure that all of the group are allowed to contribute).

It is thought that none of the experts taking part in the APJ session dominated the discussion. Each of them contributed to the discussion to a reasonable degree.

• Participants may fear disciplinary action if they criticize their company or management. None of the participants of the APJ session feared any disciplinary actions, since the actions of interest were not subject to any criticism of the plant.

• The estimates may never converge (in which case the facilitator can remove “outliers” and calculate the average on what is left).

During the estimation process a reasonable agreement could be reached in each of those cases when the difference between the individual estimates was not larger than one order of magnitude. Thus, it can be stated that the estimates converged and there was no need for removing any of them.

• It may not be possible to identify a sufficient number of “experts”, i.e. those who have sufficient knowledge of the tasks, and, especially when considering low probability events, those with direct or indirect experience of the events postulated.

The expert group that took part in the APJ estimation procedure consisted of 5 experts.

During the process of analyzing dilution faults those post-initiator operator responses were evaluated that need to be taken after an inadvertent dilution occurs. Using the commission-omission terminology this means omission of actions to terminate the dilution process. Of course such an error may well be a result of a sub-level commission error if, say, the operator closes valve B rather than valve A to stop diluting the primary circuit. What is important from the point of view of post-initiator responses following an inadvertent dilution is the consequence of an inappropriate action. Therefore those factors were in the focus of the analysis that could make the operator fail to terminate the dilution process. For the analysis of post-initiator (operator) errors a so-called decision tree approach was used. A decision tree shows the dominant influences on crew reliability, the impact of these influences (in terms of their relative importance with respect to human error likelihood), their dependencies together with the probability values assigned to each pathway in tree. Figure 2 is a simple decision tree to show the main elements of the tree: the headings, the branches, the tree construction and the pathway dependent HEP figures. The HEP value for a given action is determined depending on the characteristics of the situation (the context in which an error may occur) in terms of the effects of performance influences.
Separate decision tree models were developed and applied to the quantitative assessment of required operator responses during accidents at full power and low power operational states respectively.

As to the full power operation use was made of the HRA model developed by using support from the results of 192 simulator experiments performed at the full scale training simulator of NPP Paks between 1992 and 1995. These experiments were aimed at collecting and analyzing operator response data for the purpose of HRA. All the 24 main control room crews working at the four units of Paks were observed during responses to 8 simulated transients with multiple equipment failures. The following dominant performance influences were found from the simulator observations:

- difficulty of scenario (task complexity)
- crew knowledge of situation
- quality of man-machine interface

---

- time available for operator response
- required degree of crew integration during diagnosis and response
- quality and availability of procedures.

A decision tree based representation of crew reliability was used to integrate the findings from the simulator studies with expert judgment and generic human reliability data. The approach to quantifying post-initiator actions during full power operation of the Paks plant is depicted in Figure 3. Calibration of HEP values was primarily based on structured expert judgment with the use of four simulator instructors, two PSA analysts and a psychologist. This approach as well as the results of the full power PSA\textsuperscript{15} were found to be useful during the analysis of dilution scenarios too.

Figure 3 - Quantification of post-initiator actions - plant operation at full power
At low power and shutdown the conditions of post-initiator actions can be very much different from the full power accidents, which required extensions to the existing decision tree model for full power conditions. Some examples of such differences are as follows:

- In shutdown modes some accidents develop very slowly. Due to this there is a long time available to response to the situation. The time available may exceed even 10 hours. The effects of slow accident progression have not been addressed in the full power PSA.
- In general, the emergency operating procedures are not very well developed for low power modes.
- In most of the shutdown modes there are several parallel and sometimes concurrent activities going on (normal shutdown work in main control room, various types of maintenance, system alignments and re-alignments, functional tests, etc.), which may well affect the ability of operators and other plant staff to respond to an accident.
- Due to excessive maintenance, safety related systems are taken out of service. As a result, there can be less indications of an accident in the main control room, and/or local actions may be needed (especially recovery of power supply to equipment) as part of an emergency action.

The extended decision tree development process tried to take into account the specifics of plant operation in low power and shutdown modes and to integrate inputs from various sources: data from event reports, simulator data (if applicable) and expert opinion. The most important steps in the process were as follows:

- Draw up a list of the potential performance influences.
- Rank influences in order of importance and select the most important ones.
- Select the number of branches per performance influence and draw logic tree.
- Estimate the weighting factors for each performance influence.
- Determine the anchor values for HEP and calculate HEP distribution.
- Check and modify HEP distribution, if necessary.

When modeling and quantifying post-initiator errors in the low power and shutdown states use was made of the following:

- the model applied to the full power case
- an understanding of crew operation based on an analysis of plant operating procedures and walkdowns performed during an outage of unit 2 of Paks
- interviews with plant operators
- an analysis of over 100 safety related events occurred during outages of the four units of Paks.

After identifying dominant performance influences weighting factors were assigned to them to describe their importance with respect to the likelihood of an error. In addition, dependence between certain performance influences was taken into account by changing weighting factor values according to the combinations of performance influences. Choosing anchor HEP figures from expert opinion the weighting factor values were used to shape the distribution of HEP figures along the pathways in the decision tree. The calibration of HEPs assumes that multiple factors have multiple effects on human error likelihood. The rules for estimating HEP values from anchor HEP’s and weighting factors are described in\(^\text{16}\) and\(^\text{17}\).


The distribution of HEP values in the decision tree for low power and shutdown operation was checked by a comparative analysis of the low power and full power decision tree models. A number of situations were identified that could be evaluated by both models. After that the calculations were performed, and the results were compared. Where discrepancies were found changes were made in the numerical estimates using non-linear optimization.

3b. Findings regarding errors of commission, especially contributors to these errors and consequences of these errors in the event or accident sequence analyzed:

Generic mechanisms of dilution

With respect to the initiators of an inadvertent dilution process five generic mechanisms have been identified by expert judgment by which water of low boron concentration can be added into the primary circuit (and the core). Some of these mechanisms can develop as a result of inappropriate human actions (including errors of commission), others are equipment failures. For the sake of completeness all the five mechanisms are listed below:

- normal path
  There are cases when the water of low boron concentration is introduced into the primary circuit by a normal operational route (e.g. boron removal throughout the campaign).

- erroneous alignment of systems
  This is an error made during the alignment of the systems causing an inadvertent injection of water with low boron concentration into the primary circuit.

- damage (loss of integrity) of a system boundary separating primary coolant from the system with water of low boron concentration
  Such kind of damage can take place in heat exchangers with primary coolant on one side of the heat exchanger and water with low boron concentration on the other. Of course, this mechanism leads to a boron dilution problem only if the pressure of the latter is higher than that of the primary coolant.

- maintenance errors
  These errors can take place mainly after rinsing pieces of equipment (pipes, tanks, filters, etc.) containing usually primary coolant with pure condensate during refueling outages. Pure condensate may inadvertently remain in the equipment and enter the core during start-up of the reactor.

- occurrence of an initiator that can cause inherent dilution of the primary coolant
  An example of such a mechanism may be an initiator that causes evaporation of the primary coolant at one place and condensation of the steam poor in boron at another.

Insights from relevant event reports

An examination of operational events at Paks revealed 13 events that could be of interest from the point of view of the dilution phenomenon. None of the events led directly to the dilution of the primary coolant, they had only the potential to dilute it. The majority of the events (9 events) were recorded during normal power operation and some of them took place during the shutdown plant operational states. In most of the cases events were concerned only with “simple” dilution of the safety related boron concentration tanks to a degree which was not at all dangerous to the core. In several cases high concentration boron tanks (like e.g. high pressure safety injection tanks) were diluted with water of lower, but still sufficiently high boron concentration. There appears to be one event that had some real danger to the core. A valve had been left open following a normal dilution in
a water purification system so that pure condensate could enter the make-up water system inadvertently. The event report was not sufficiently detailed to be able to identify the causes of this event.

Dilution due to commission type errors

Using expert opinion and some insights from event reports it was determined that errors of commission can result from three underlying causes:

- As a result of an error of omission (for example, in the case where an operator is required to open valve A, if that valve is next to a similar valve, valve B, he may open B instead. Thus, he has omitted to open A and has opened B. Opening B is the error of commission).
- As a result of a “cognitive error” in which the operator forms an incorrect diagnosis of a problem, and produces a solution which entails performing an action that is not required nor appropriate at that time. This is sometimes known as a ‘diagnostic’ error.
- As a result of a “violation”, in which the operator is motivated to break a known rule and may thus begin a task that is not required nor appropriate.

Recoveries from a dilution scenario

The means available for mitigating the consequences of an initiator and possible recovery actions were examined. Based on this examination scenarios leading to core damage were developed from each of the initiators. As concerns initiators occurring during power operation a functional event tree was developed to model automatic (mitigating) plant responses as well as required operator actions. Details of this event tree are out of the scope of the current discussion. When the reactor is shut down the only way of mitigating a dilution initiator is a recovery action performed by the operator. Recovery refers to the actions that are performed either after the dilution process has been started to stop the process or before that to recover dangerous (from the point of view of potential for the dilution) state (e.g. erroneous alignment) of the systems. There are initiators when no recovery is possible due to the quick local dilution.

Results

After the initial screening analysis 21 dilution scenarios were selected for refined quantification. The initiator type human errors included in these scenarios were numerically estimated by the use of the APJ method as referred above. The 21 scenarios involved 11 different operator errors: 9 of them were errors of commission and 2 errors of omission. The expert group evaluated these actions one by one. A description of each action has been prepared prior to the session including the circumstances (plant operational state, procedures and regulations concerning the action in question) of the action. However, it should be emphasized that this was not the only source of information used for the estimation. Each expert (mainly experts from the operation) had a chance to add his own knowledge about the task/situation. Making any estimates during these discussions was tried to be avoided. Debrief discussions were continued until everyone felt that the situation or action to be evaluated was fully understood. Each expert made his own estimate by the use of the APJ estimation scale. Having individual estimates they were compared and the outliers were further discussed. After that it was asked whether anyone would like to modify his estimate. Modifications were made in a number of cases. Following this procedure a reasonable agreement could be reached so that the difference between the individual estimates was not larger than one order of magnitude. Geometrical average of the estimates was used to produce a final estimate of HEP.
As to the quantified risk figure the core damage probability resulting from the dominant dilution initiators in one year is 2.0E-6. A limited number of scenarios dominate this value. Two of them are briefly summarized below each containing a commission type human error.

**Scenario No 1**

Dilution occurs through the interconnections of the following systems:

- TK  Pure condensate system
- TC  Water purification system No. 2
- TK  Make-up water system
- YA  Primary circuit

Pure condensate lines are connected erroneously to one of the filters of the water purification system No. 2, thus pure condensate gets into the discharge line TC22 of the TC pumps. After the borating of the primary circuit has been completed “soft” decontamination of the primary coolant starts. The systems are aligned so that the primary coolant is removed through the make-up water lines, transferred to the TC system, forced through the filters by TC pumps, returned to the suction line of the make-up water pumps and then returned back to the primary circuit by the operational make-up water pump. The pressure difference between the pure condensate and the TC systems allows the pure condensate to be added to the primary coolant being purified. Due to the flow rate the dilution process is homogeneous. Detection of the dilution process is possible (1) by the level increase of the deaerator (annunciated alarm) due to the overall increase of the coolant mass and (2) by the continuous boron concentration measurement (unannunciated signal). Taking into account the relevant deterministic criteria the time window for a recovery action to be successful is over 10 hours. The possible recovery action is closing the valves of the pure condensate system being erroneously open.

The probability of an erroneous alignment of the pure condensate system to the TC system was initially assessed to be 3.0E-2 and then it was modified during the APJ session to 4.5E-4. All the additional routes are aligned intentionally, so the probability of those transitions is 1.0. The probability of omitting the recovery action was assessed to be 1.8E-3 taking into account the performance influences characterizing the required human interaction (very long available time, insufficient training, high workload, good MMI, poor procedures). Thus, the core damage probability resulting from the given scenario is 8.1E-7.

**Scenario No 2**

Dilution occurs through the interconnections of the following systems:

- TK  Pure condensate system
- TC  Water purification system No. 4
- TK  Make-up water system
- YA  Primary circuit

The isolation of the pure condensate system from the water purification system No. 4 in shutdown modes is ensured by two valves that are normally closed. Due to an erroneous opening of these values during a plant operational state when the reactor coolant pumps (RCPs) are running pure condensate can be injected into the line of the filters of the TD system. This line is normally isolated from the make-up water system by two other valves. If these valves are also open inadvertently pure condensate enters the deaerator, and then it is delivered to the primary circuit by the operational make-up water pump. Due to the flow rate the dilution process is homogeneous. Detection of the dilution process is possible (1) by the level increase of the deaerator (annunciated alarm) due to the
overall increase of the coolant mass and (2) by the continuous boron concentration measurement (unannunciated signal). Taking into account the relevant deterministic criteria the time window for a recovery action to be successful is well over 10 hours. The possible recovery action is the isolation of the pure condensate system from the TD system.

The composite probability of opening two sets of valves erroneously (two virtually independent errors) was initially assessed to be 9E-4 that was modified by the APJ session to 7.1E-5. The additional route is aligned intentionally, so the probability of that transition is 1.0. The probability of omitting the recovery action was assessed to be 1.8E-3 taking into account the performance influences characterizing the required human interaction (very long available time, insufficient training, high workload, good MMI, poor procedures). Thus, the core damage probability resulting from the given scenario is 1.3E-7.

4. Provide definitions of terms and parameters used in responses to the questions listed above.
No attempt was made during the analysis describes in this section to develop a list of definitions of terms and parameters specific for the study. In effect, most of the terms used are explained in the discussions above on the various analysis tasks.

5. Provide thoughts on the relevance of the analyses method and findings to PSA:
The analysis was carried out with the objective of extending the existing level 1 PSA analyses for NPP Paks with risk of core damage due to the consequence of inadvertent dilution faults both at full power as well as in low power and shutdown states. An additional objective is to develop recommendations for safety improvements if there are plant vulnerabilities to the dilution process. Since the analysis is part of a PSA study, the results are of direct use in the plant specific PSA for Paks. In addition to quantified risk figures, qualitative findings from the HRA are currently being reviewed. Following this review the results will be incorporated into the existing PSA study for Paks and the necessity of safety improvement measures will be evaluated.

Although the analysis was not intended to develop a new HRA method, a lot of the findings are seen useful for the purpose of future HRA development efforts. Probably one of the most important findings from the analysis is that in certain plant operational states at low power and shutdown the likelihood of a plant transient due to inappropriate human actions may not be negligible. A number of causes have been identified that can lead to an initiator type error either by plant operators or maintainers. These errors, if coupled with latent errors made during maintenance, can be an important contributor to risk. Therefore a more detailed analysis of both pre-initiator and initiator errors during an outage is planned, and the results will be fed back to the low power and shutdown PSA for Paks.
Contribution from Japan

Mamoru Fukuda
Institute of Nuclear Safety/Nuclear Power Engineering Corporation (INS/NUPEC)
Japan

1. Describe the method used to analyze errors of commission, including
1a. A statement of the purpose and scope of the method used in the analysis:

Background

Safety Information Research Center (SIRC) of NUPEC has been filing accident and incident reports, which Japanese utilities report to Ministry of International Trade and Industries (MITI) according to laws or voluntarily; in order to make database. IHF has been developing methodologies of systematically analyzing these events from the viewpoint of human factor. Using these methodologies, IHF has been analyzing these events to make human error event database. These contents were reported to PWG1 Task 7 in September 1997. Events due to human error have been analyzed and evaluated systematically from the view points of error causes, human error mechanisms and error modes, where about 73% of human errors occurring in Japanese nuclear power plants is categorized into error of commission (EOC). These EOC events mainly occurred during periodic test and maintenance. However, there is no EOC event during accident/incident nor leading to initiating event, which is worthy of 'case study'. On the other hand, current level 1 PSA conducted at INS/NUPEC does not explicitly cope with EOC.

However, accident analysis reports of foreign countries (Accident Sequence Precursor analysis) have pointed out the significant contribution of EOC during accidents and incidents to care damage frequencies (CDF), which implies the importance of the introduction of EOC into level 1 PSA. The PWG-5 task group meeting held on September 25, 1997 required each member country to give its own methodologies of identifying EOC and error forcing contexts (EFC) and evaluating EOC influences on plant safety, and to supply its own operating experiences which will be used in 'case study' for EOC methodologies.

Therefore INS/NUPEC has just started literature survey of EOC in level 1 PSA (NUREG/CR-6093\(^1\), 6265\(^2\), 6350\(^3\), Borssele PSA and NUREG-1624\(^4\)). Using this literature survey, INS/NUPEC made a trial application of ATHEANA for our level 1 PSA of a Japanese 1,100 MWe-class four loop PWR


\(^3\) NUREG/CR-6350, "A Technique for Human Error Analysis (ATHEANA)", May 1996.

plant to raise our understanding of EOC in a level 1 PSA. In parallel IHF/NUPEC has started preliminary study for methodology development of EOC using the human characteristics experiments. This report presents the current status, as of March 1998, of the above studies in NUPEC.

In the fiscal year of 1998 NUPEC has made re-evaluation of the trial application of ATHEANA based on NUREG-1624 (Draft)\textsuperscript{5}, where we have experienced screening process of both HFE and EFC, and quantification process of CDF. These are not included in this paper but the insights from the re-evaluation are reflected in Table 2.1 ‘Summary Description of Methods’ in Chapter 2 and Table 3.1 ‘Findings Concerning Operator Performance and EOCs’ in Chapter 3.

**Trial application of ATHEANA to a level 1 PSA**

(1) Methodology of analyzing EOC

ATHENA developed in USA (NUREG/CR-6350\textsuperscript{6} and NUREG-1624\textsuperscript{7})

(2) Purpose of the method used in the analysis:

The objectives of the trail application are as follows:
(a) to understand the ATHEANA methodology itself
(b) to understand the importance of introducing EOC into level 1 PSA
(c) to point out the items which should be made clear in the Japanese specific circumstances
(d) to contribute to making the future approach of EOC study in NUPEC

(3) Scope of the method used in the analysis:

The scope of the trial application is as follows:
(a) The level 1 PSA for Japanese 1,100 MWe class four loop PWR conducted in INS/NUPEC
(b) The application is limited to human failure events (HFEs) in SGTR event.
(c) The application is in conformity with ATHEANA written in NUREG/CR-6350\textsuperscript{8} and the results are reviewed from the viewpoint of the description of NUREG-1624\textsuperscript{9}.
(d) The application is made to obtain the knowledge of the contribution of EOC to core damage frequency estimated in the current level 1 PSA.

**1b. A description of the underlying concepts of the analysis method used (that is, reference to human sciences, if relevant):**

\textsuperscript{5} “Op. cit., 4, NUREG-1624”.


\textsuperscript{7} “Op. cit., 4, NUREG-1624”.


\textsuperscript{9} “Op. cit., 4, NUREG-1624”.
The application was conducted in conformity with ATHEANA written in NUREG/CR-6350\textsuperscript{10}; NUREG-1624\textsuperscript{11} was not used because it had not yet been published when the application had been conducted. ATHEANA was developed in US NRC, of which details are described in NUREG-1624\textsuperscript{12}. In ATHEANA, HFE during accidents, unsafe actions (UA) which induce HFE and error forcing contexts (EFC) which induce UA, are systematically specified and the probability of HFE is also quantified systematically.

1c. A summary of the steps taken or the procedure used for conducting the analysis:

The trial application was made in conformity with the description of NUREG/CR-6350\textsuperscript{13} to the level 1 PSA conducted in INS/NUPEC. The trial application was conducted by PSA specialists who were engaged in the level 1 PSA, mainly using emergency operating manuals at SGTR, in the following procedure:

(1) PSA initiator priority for examining

SGTR events are a-priori screened for application of ATHEANA because there are so many operator actions at this accident where there should exist a lot of potential for EOC.

(2) Identification of HFE

HFEs are identified in every function of ‘RCS de-pressurization by PORV (power operated relief valve)’ and ‘Feed and bleed operation’ on the premise that HFEs should be considered in every safety function or event heading of event tree.

(3) Specification of UAs

UAs are specified for the above-identified HFEs based on engineering judgment considering actually happened human failure events in the world.

(4) Specification of EFC for UA

EFCs are specified for the above-specified UAs based on the emergency operating manuals at SGTR according to the instructions of NUREG/CR-6350\textsuperscript{14}.

(5) Quantification of probability of HFE

Probabilities of HFEs are quantified in conformity with NUREG/CR-6350\textsuperscript{15}.

\textsuperscript{10}“Op. cit., 3, NUREG/CR-6350”.
\textsuperscript{11}“Op. cit., 4, NUREG-1624”.
\textsuperscript{12}“Op. cit., 4, NUREG-1624”.
\textsuperscript{13}“Op. cit., 3, NUREG/CR-6350”.
\textsuperscript{14}“Op. cit., 3, NUREG/CR-6350”.
\textsuperscript{15}“Op. cit., 3, NUREG/CR-6350”.
(6) Consideration

The results are considered in light of the contribution of EOC to CDF in level PSA, comparison with instruction of NUREG-1624\textsuperscript{16}, needs for Japanese specific data and future work in this field at NUPEC.

2. Describe in detail the event or sequence analyzed.

(1) Identification of HFEs

SGTR events were selected to apply ATHENA for because SGTR has many operator actions that seem to have fruitful potential for EOC. Namely, SGTR events compel operators to make failed SG isolation, RCS cooling through secondary side, RCS de-pressurization PORV, early connection to RHR and Feed and bleed operation after SG isolation failure. Accident sequences of SGTR were analyzed in level 1 PSA in terms of event tree (Fig. 1). HFEs were identified for the functions of ‘RCS de-pressurization by PORV’ and ‘Feed and bleed operation after SG isolation failure’ as follows:

(a) HFE\#1: failure of ‘RCS de-pressurization by PORV’ due to inappropriate termination of HPI pump leading to HPI system failure
(b) HFE\#2: failure of ‘Feed and bleed operation after SG isolation failure’ due to inappropriate closure of PORV

(2) Specification of UAs

UAs were identified for the above-identified HFEs considering actual human failure events and emergency operating manuals at SGTR as follows:

(a) UA/HFE\#1: Operators suspend HPI pumps operation before the plant satisfies the suspension conditions for HPI pumps in order to connect to RHR operating conditions.
(b) UA/HFE\#2: Operators close PORVs before the plant satisfies the suspension conditions for the feed and bleed operation.

(3) Specification of EFC

EFCs were identified for the above-identified UAs considering the suspension conditions of HPI pumps operation in the operating manuals at SGTR as follows:

(a) EFC/UA/HFE\#1:
   EFC1: 1/2 failure of RCS pressure gauges (PC1; plant condition 1)
   EFC2: 1/2 failure of RCS water level gauges (PC2)
   EFC3: lack of mental clarity (PSF1)
   where the suspension conditions for HPI pumps in order to connect to RHR operating conditions are:
   - RCS pressure gets stable or increase after the termination of RCS de-pressurization
   - PORV RCS water level is recovered above zero level
   - RCS sub-cooling is above some level

\textsuperscript{16}“Op. cit., 4, NUREG-1624”.
Fig. 1 SGTR Event Tree Considering HFE\#1 and HFE\#2
(4) Quantification of HFE

HFES were quantified using component failure data used in the level 1 PSA as follows:

(a) HFE#1 = (1/2 failure of RCS pressure gauges)*(1/2 failure of RCS water gauges)*(lack of mental clarity)
   = 2*(1/2*(1.1E-6/h+7.9E-7/h)*8760h)*2*(1/2*(1.4E-6/h+1.1E-6/h)*8760h) * 1/6
   = (1.7E-2)*(2.2E-2)*(0.16)=6.0E-5

(b) HFE#2 = (1/3 failure of SG water gauges)*(lack of mental clarity)
   = 3*(1/2*(1.4E-6/h+1.1E-6/h)*8760h) * (1/6)
   = (3.3E-2)*(0.16)=5.3E-3

where both failure of function and deterioration of function are taken into account as pressure gauge and water level gauge failures.

(5) Quantification of core damage frequencies

Core damage frequencies were estimated for the above HFES, where SGTR initiating event frequency is 5.4E-3/ry, SG isolation failure is 1.9E-3, unavailability of auxiliary feed-water system (AFWS) is 2.0E-5:

(a) CDF for HFE#1=(SGTR frequency)*(isolation failure of failed SG)*(probability of HFE#1)=(5.4E-3)*(1.9E-3)*(6.0E-5)=6.2E-10/ry

(b) CDF for HFE#2=(SGTR frequency)*(unavailability of AFWS)*(probability of HFE#2)=(5.4E-3)*(2.9E-5)*(5.3E-3)=8.3E-10/ry

3a. Findings regarding the method used, especially theoretical insights, practical lessons learned (e.g., software requirements, expertise requirements, resource requirements), and data input and output:

From these analyses the following findings were obtained:

(1) Further experience of the screening process of HFES is needed to confirm the possibility of introduction of ATHEANA to level 1 PSA.

(2) ATHEANA guideline (NUREG-1624\textsuperscript{17} draft) does not always seem to state explicitly the way of identifying and quantifying mental factors as EFC. In order to understand how to identify mental factors as EFC in ATHEANA, it is important to make event analysis (retrospective analysis), which involves EOC, with ATHEANA.

(3) Usage of simulator experiment should be pursued to identify probabilities of unsafe actions and recovery actions occurring in the context of EFCs based on the Japanese specific

\textsuperscript{17} “Op. cit., 4, NUREG-1624”.

152
3b. Findings regarding errors of commission, especially contributors to these errors and consequences of these errors in the event or accident sequence analyzed:

From these analyses the following findings were obtained:

(1) CDF due to both HFE#1 and HFE#2 is 1.5E-9/ry, while total CDF in SGTR is 1.6E-7/ry in current level 1 PSA. Therefore CDF due to both HFEs accounts to about 1% that of SGTR. Conceivable reasons that CDF due to EOC is estimated to be smaller than we have imagined are as follows;
(a) Evaluated HFEs are relevant to alternative safety functions in level 1 PSA, which means these HFEs alone do not directly lead to core damage.
(b) Only one UA was specified for each HFE unlike NUREG-162418 where plural UAs are systematically specified for one HFE.

(2) HFEs should be carefully identified taking into account the structure of event trees such as the following.
(a) Almost all safety functions have redundancies and diversities in the event tree structures in level 1 PSA. This means single HFE hardly leads to core damage directly. For example, in level 1 PSA, even if HPI function fails due to some troubles at SGTR, the plant does not result in core damage under the condition that both isolation of failed SG and AFWS are succeeded.
(b) Similarly even if HPI function fails at small LOCA, operators can avoid core damage if operators open main steam valves to accomplish the forced secondary cooling and use low pressure injection system. However, these operations correspond to some recovery actions after EOC.
(c) The attention should be also paid in that operators, who failed the preceding actions, could have different PSFs

(3) Initiator of SGTR, which was selected for the trial application of ATHEANA, was screened out in the demonstration application of NUREG-162419 mainly because HFEs in SGTR have comparatively large allowable time for core damage.

(4) In the trial application, one HFE which gives rise to HPI failure due to EOC was selected by PSA specialists based on engineering judgment. However, plural HFEs should be systematically chosen in accordance with implementation guideline in NUREG-162420. For example not only inappropriate closure of PORV but also inappropriate termination of HPI pump could be identified for ‘Feed and bleed operation’. Another example is that only inappropriate termination of HPI pump was identified to be HFE for HPI failure due to EOC.


153
However, in NUREG-1624\textsuperscript{21} inappropriate isolation/alignment, output/resources inappropriate diversion, output/resources inappropriate depletion and inappropriate removal from armed/standby status are identified for HPI failure, in addition to inappropriate termination of HPI pump. The same can be said for the identification of UAs. Only 'operators stop pump' was identified to be UA for HPI failure. However, in NUREG-1624\textsuperscript{22} various UAs are identified for 'operators stop pump'.

(5) In the trial application EFCs were identified based on the description of emergency operating manual by PSA specialists, where PSF (performance shaping factor) was neglected. Therefore, EFCs should be systematically clarified in accordance with NUREG-1624\textsuperscript{23}, taking into account both PC (plant condition) and PSF. However, we recognize there are a lot of grounds for investigation in the identification of EFC for UA such as follows:
- scenario dependency of EFCs
- weighting of EFCs among them
Operators’ opinion at-site and simulator experiments are very important.

(6) The probabilities of HFEs were quantified using component failure data used in the level 1 PSA according to instructions in NUREG/CR-6350\textsuperscript{24}. Strictly speaking, only the failure rates of failure modes leading to the UA should be considered, but this could be solved in the fineness stage of ATHEANA application. For example, only pressure gauge failure mode with not low indication but high indication could contribute to 'inappropriate termination of pump'. Furthermore in the trial application it was assumed that only one failure of the plural measuring instrument causes operators to make EOC. This seems too conservative.

(7) The probability for lack of mental clarity seems unclear in both NUREG/CR-6350\textsuperscript{25} and NUREG-1624\textsuperscript{26}, which should be made clear in actual application.

4.\textsuperscript{.} Provide definitions of terms and parameters used in responses to the questions listed above.

The definitions of terms and parameters used are in accordance with NUREG/CR-6350\textsuperscript{27} and NUREG-1624\textsuperscript{28} (draft) [4, 9].

5.\textsuperscript{.} Provide thoughts on the relevance of the analyses method and findings to PSA:

From the above trial application, in order to apply ATHEANA to level 1 PSA for Japanese LWRs,
NUPEC (INS/IHF) plans to make the following tasks:

1. Re-evaluation of application of ATHEANA for SGTR
   Based on IG (Implementation Guidelines) and FOR (Frame-of-Reference) manual in NUREG-1624, appropriateness of screening for HFE will be clarified, taking into account allowable time to core damage, frequencies of the events and so on.

2. ASP analysis
   In order to understand the characteristics of EOC related events, we continue ASP analysis for foreign events relative to EOC such as TMI-2, Crystal River 3, North Anna 2, Salem 1 and so on, using ASP models prepared for Japanese plants. In this connection INS has ASP models for six kinds of plants for ASP analysis for Japanese LWRs, which have been utilized for not only domestic events but also foreign events. In ASP analysis for foreign events we could experience for ourselves what other countries have gone through. For example, we could find an accident sequence induced by malfunction of SI actuation signal in actually occurring events, which we have not explicitly taken into account in our event trees of level 1 PSA. It implies that these kinds of events have the potential of giving rise to new EOCs. ASP analysis for the events that involve EOC by level 1 PSA methodology seems very important to introduce EOC into level 1 PSA.

3. Preliminary investigation to identify EFC using the human characteristics experiments
   IHF has human characteristics experimental facilities to solve human factor problems effectively, where basic data needed to understanding human characteristics are collected and simulation verification tests are conducted. Table 1, for example, presents results of human characteristics experiments to verify human error mechanism at design basis accidents with another trouble being piled. If unsafe actions of operators are observed in the experiments, root cause analysis will be made. In the preliminary study the possibility of the use of human characteristics experiments will be assessed as follows:
   (a) how to identify EFCs among PCs and PSFs using the human characteristics experiments.
   (b) what kinds of capacity should be equipped with in the experiments.

4. Presentation of EOC scenarios for human characteristics experiments
   Referring the demonstration application of ATHEANA in NUREG-1624, important HFEs and UAs will be identified from the various points of view, namely the above trial application, the role of experiments, the methodology of experiments and so on. Candidate scenarios, for which EFCs will be identified in the human characteristics experiments, will be selected among these UA/HFEs.

5. Investigation for the use of PSA with ATHEANA applied
   How to use the PSA results with EOC considered should be pursued in risk informed management area.

---
<table>
<thead>
<tr>
<th>No.</th>
<th>Simulated initiating event</th>
<th>Additional troubles during initiating event (recoverable at control room except for No. 7)</th>
<th>Number of crews which identified the events and coped with them correctly</th>
<th>Number of crews which correctly identified the events but coped with them different from manuals</th>
<th>Number of crews which mis-identify the events and coped with them incorrectly</th>
<th>Number of crews which could not identified the events all and could do nothing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SGTR</td>
<td>High pressure injection pumps do not start automatically</td>
<td>8/8</td>
<td>0/8</td>
<td>0/8</td>
<td>0/8</td>
</tr>
<tr>
<td>2</td>
<td>SGTR</td>
<td>PORV leak</td>
<td>7/7</td>
<td>0/7</td>
<td>0/7</td>
<td>0/7</td>
</tr>
<tr>
<td>3</td>
<td>Drop of one control rod</td>
<td>Outlet MOV of PWT fails close</td>
<td>8/8</td>
<td>0/8</td>
<td>0/8</td>
<td>0/8</td>
</tr>
<tr>
<td>4</td>
<td>Loss of off site power</td>
<td>Charging pumps do not start automatically</td>
<td>6/8</td>
<td>2/8</td>
<td>0/8</td>
<td>0/8</td>
</tr>
<tr>
<td>5</td>
<td>Loss of off site power</td>
<td>Switch-gear of DG is locked.</td>
<td>7/8</td>
<td>1/8</td>
<td>0/8</td>
<td>0/8</td>
</tr>
<tr>
<td>6</td>
<td>Trip of main feed water pump</td>
<td>TD-AFWS pump does not start automatically.</td>
<td>8/8</td>
<td>0/8</td>
<td>0/8</td>
<td>0/8</td>
</tr>
<tr>
<td>7</td>
<td>Turbine bypass valve fails open.</td>
<td>Upstream valve of turbine bypass valve fails open. (recoverable at local panel)</td>
<td>5/8</td>
<td>0/8</td>
<td>0/8</td>
<td>3/8</td>
</tr>
<tr>
<td>8</td>
<td>Leak of PORV</td>
<td>Second reserve heater of PORV is locked.</td>
<td>6/8</td>
<td>0/8</td>
<td>0/8</td>
<td>2/8</td>
</tr>
</tbody>
</table>
Contribution from Switzerland: Conclusions from Occurrences by Descriptions of Actions (CODA)

Bernhard Reer
Paul Scherrer Institut, Switzerland

1. Method Description

The method is denoted as CODA (Conclusions from Occurrences by Descriptions of Actions). Details are published in Reer (1997a); a test analysis of 11 incidents is presented in Reer (1997b).

Purpose and Scope

The method presents guidance for the analysis of any incident that involves at least one human error. It specifies

- the retrospective identification of likely error causes with emphasis on cognitive aspects, and
- the prevention of errors in future performance.

The main elements of the guidance are:

- a list of key term definitions (each term of the list underlined the first time it is introduced in the main text),
- a step-by-step procedure for structuring the analysis together with rules for information gathering, and
- an extensible taxonomy of cognitive tendencies (CTs) that drive human performance.

Furthermore, the CODA method provides support for predictive Human Reliability Analysis (HRA) in Probabilistic Safety Assessment (PSA) of complex systems. Regarding the latter, a HRA version of CODA is under development (Reer et al. 1999).

Underlying Concepts

The main concepts of CODA are:

- using critical actions as a subjects for describing errors,
- using cognitive tendencies for explaining an error, and
- improving human hazard cognition for preventing an error.

The concepts can be applied for both retrospective and predictive analysis.

Using Critical Actions as Subjects for Describing Errors

CODA utilizes a well-known and simple key principle in error classification by viewing actions neutrally. The context determines whether a given critical action is inappropriate or required (and appropriate of course). On a basic observable level, two types of errors exist, namely,

(i) required action omitted (error of omission - EOO),
(ii) inappropriate action committed (error of commission - EOC).

This points to two basic characteristics of a critical action, (i) required, or (ii) inappropriate. In order to provide a perspective on error likelihood, CODA uses further characteristics that describe the
critical action’s context in a given performance situation. For that purpose, the action is defined as the subject, i.e. the description of an EOO or EOC is formalized as follows:

\[
\text{subject = action} \quad \text{predicate} \quad \text{object}, \text{ e.g.,}
\]

feedwater isolation matches panel of buttons the operator is referring to.

The relevant features of the situation are covered indirectly by the characteristics of the action - in terms of grammar, they appear as predicate-object combinations behind the subject. This has the advantages that the link to the error is directly transparent and that the subject (action) can be expressed shortly by a few words. Using the situation as the subject of information gathering (i.e. situation has/is ... ) has the disadvantages that the link to the error is not necessarily clear and that the subject (situation) cannot be expressed briefly because it usually consist of a combination of events.

Using Cognitive Tendencies for Explaining Errors

Action characteristics are grouped according to cognitive tendencies defined as typical human practices or attitudes in work performance. Table 1 presents a taxonomy of predicate-object combinations and the associated psychological phenomena expressed by cognitive tendencies.

<table>
<thead>
<tr>
<th>Group</th>
<th>Error-Driving Action Characteristic (generic error-producing condition)</th>
<th>Underlying Cognitive Tendency</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC1</td>
<td><strong>Action’s attraction</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(AC1.1) Required action causes a delay</td>
<td>(CT1.1) Impatience or curiosity</td>
</tr>
<tr>
<td></td>
<td>(AC1.2) Required action causes drastic side effect</td>
<td>(CT1.2) Reluctance toward something drastic</td>
</tr>
<tr>
<td></td>
<td>(AC1.3) Required action mismatches nearby aspect</td>
<td>(CT1.3) Fixation on (or fixing on) something nearby</td>
</tr>
<tr>
<td></td>
<td>(AC1.4) Required action is unnecessary or harmful in the likely case</td>
<td>(CT1.4) Non-conservative probabilistic reasoning</td>
</tr>
<tr>
<td>AC2</td>
<td><strong>Operator’s accuracy</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(AC2.1) Required action is needed after success perception</td>
<td>(CT2.1) Relaxation</td>
</tr>
<tr>
<td></td>
<td>(AC2.2) Required action is needed under time constraint perception</td>
<td>(CT2.2) Hastiness</td>
</tr>
</tbody>
</table>

For HRA implementation of activity-oriented ergonomics (De Montmollin 1991), the concept of cognitive tendencies was developed by the European Association on Reliability Techniques for Humans (EARTH, Mosneron-Dupin et al. 1998). In CODA, cognitive tendencies (CTs) are used to explain why errors occur, but they (CTs) are not defined as error mechanisms.

Inappropriateness is relative. As the context determines whether a given action is inappropriate, the context determines as well whether a given CT is inappropriate.

According to Semmer (1994), a tendency or mechanism concerns both producing success and producing error. Given a non-adverse context (i.e. the usual, most frequent variant of a working situation), cognitive tendencies contribute significantly to high human performance, e.g., the tendency fixation as the ability to focus on an important strategy. However, given an adverse context (i.e. the unusual, exceptional variant), cognitive tendencies often lead to errors, e.g., again the tendency fixation, but now as the ‘inability’ to abandon a wrong strategy. This central role of cognitive tendencies is illustrated in Figure 1.
Although CODA emphasizes cognitive aspects, the method is supposed to cover any performance shaping factor (PSF) that may have contributed to an error. PSFs are addressed from a cognitive perspective. For instance, the PSF *wrong procedural instruction* would be covered by Table 1 AC1.3: *required action mismatches nearby aspect* in the case of an EOO, or *inappropriate action matches nearby aspect* in the case of an EOC - nearby because the operators are supposed to follow the procedure. For both cases the underlying CT may be specified as *fixation on following procedural instructions*. The degree of PSF coverage depends on the scope of the taxonomy in Table 1. Thus the taxonomy is viewed as extensible regarding both size (list of CTs) and guidance for specification.

However, cognitive tendencies should be specified with care; cf. the precautionary notes presented in Mosneron-Dupin et al. (1998). Human attitudes and practices in work performance may vary from plant to plant and from situation to situation, e.g., in some situations it could be a common practice to ignore procedural rules. Therefore, the taxonomy in Table 1 should be used as a guidance for collecting on-site information.

Especially, the Table 1 links related to AC2 must be viewed with care. Compensations are possible. For instance, success perception may lead to the reduction of stress from a high level to an optimal level and consequently to a reduced error likelihood. More research is needed to specify the conditions that affect operator's accuracy in work performance, cf. the findings outlined by Wickens (1992) under the headings of *vigilance and attention*.

Furthermore, the analyst may consider that some CT categories overlap, e.g., CT1.1 and CT1.2, or CT1.3 and CT1.4. But such overlaps are of minor importance for the practitioner. The purpose of the CT taxonomy is to present a structured human-centered approach for analyzing errors rather than to present a perfect theory on human error. Note that other taxonomies on error causes include overlapping categories as well, e.g., NRC (1998, Tables 7.9 to 7.14).

What is the practical use of CTs for explaining errors? CTs provide a structured human-centered approach for enriching the space of search for error causes compared to the space known from a strict ergonomic approach. Side note: the term *cause* is meant here in the sense of a potential contributor to an error; it is clear that a perfect assignment to a single cause is extremely difficult.

Let us consider an occurrence where an operator failed to respond to a signal. A strict ergonomic approach would highlight technical layout features regarding the question whether the signal was clearly detectable. CTs bring features into play that are major error contributors even under optimal ergonomic design condition. Examples - according to the Table 1 taxonomy - are listed below.

**CT1.1** => Signal detection requires to interrupt the current work process and to refer to a panel in another room (cf. NRC 1998, page 7-38, *indications located in out-of-the-way locations*), or the response itself would require to go through a long procedure of checking tasks.

**CT1.2** => The response would result in the need to shut down the plant for days (cf. NRC 1998, page 7-38, *goals conflict*).

**CT1.3** => The operator is focusing his attention on another panel where the signal is undetectable (cf. NRC 1998, page 7-38, *more prominent indications*). The operator might be captured by another task for which the signal is irrelevant: the signal does not exist for him regardless how clear it is indicated.

**CT1.4** => The operator expects the signal to be spurious (cf. NRC 1998, page 7-36, *information rejected*). Usually, operators have experience with both a signal occurs spuriously and a signal fails to occur (cf. NRC 1998, page 7-39, *history of unreliable or faulty indications*).

**CT2.1** => The operator had solved already the major part of the problem and thus reduces his attention when dealing with the remaining part of the problem (cf. NRC 1998, page 7-39, *times when the operators alertness level is low*). Alertness is of dynamic nature.
The analyst must account for fluctuations during the performance time period under consideration.

CT2.2 => Fast changes of system parameters suggest that there is a need to respond quickly (cf. NRC 1998, page 7-38, perceived urgency). This might cause the omission to refer to the panel where the signal is detectable.

Neglecting nuances in wording, the CT-related error causes exemplified above are supported by the findings of the ATHEANA project (NRC 1998). Thus ATHEANA and CODA have common emphases on the scope of error causes that need to be addressed in future analyses. What is different is the strategy for identifying such error causes. While ATHEANA's search strategy is structured by human information processing stages, CODA structures the search by cognitive tendencies that are supposed to determine how attractive actions appear and how accurate operators will work.

![Diagram of SUCCESS and ERROR scenarios]

**Figure 1. The central role of cognitive tendencies in high-reliable systems.**

The shaded bar illustrates error prevention by human hazard cognition.

Improving Hazard Cognition for Preventing Errors

According to the discussion of Figure 1 presented above, CODA's error prevention concept highlights the improvement of hazard cognition (cf. Hoyos 1980), i.e. the ability to anticipate (identify, consider, recognize) adverse contexts. Hazard cognition is a key element of safety culture or awareness. This emphasis is based on the reasoning as follows:

- It is extremely difficult to foresee and avoid all specific types of adverse contexts. We have to accept that such contexts occur from time to time (more or less randomly). Thus human safety awareness should be viewed as one decisive barrier in preventing severe failures. This barrier is illustrated by the shaded bar in Figure 1.

- Furthermore, Figure 1 illustrates that any attempt to change cognitive tendencies is risky in the sense that the frequency of errors may increase. One important conclusion from the research of the EARTH group is: "cognitive tendencies are not themselves mechanisms of errors. They generally refer to adaptive mechanisms that play a positive part most of the time. Should a these cognitive tendencies not exist, the operators would have great difficulty in doing their work (Mosneron-Dupin et al. 1998, page 268)."

- Hazard cognition is a concept for a wide scope of users. It can be used by each participating person of the process of human error prevention, since operators, safety managers, authorities and analysts share a common task: to identify contexts where typical human practices or attitudes are inappropriate.
Short Guidance for Applying the Method

Wording Hierarchy

Figure 2 illustrates the hierarchy of the wording used in CODA. A data base contains a number of incidents. Each incident refers to a report (or observation) of the context of at least one system failure. An incident may include a number of occurrences. Following ASSET (IAEA 1991), the term occurrence is used here in connection with a deviation from the reference (normal, undisturbed) sequence. CODA focuses on directly observable errors. Such an error appears as an action-related occurrence (critical action inappropriately omitted or committed). Each underlying critical action is a subject of information collection in a CODA analysis. Not directly observable errors (e.g., failure to recognize a particular system state) are classified under the heading of cognition-related occurrences (deficiency of knowledge documented). They are considered as candidates of contributors to the directly observable errors.

Data base

Incident

Occurrence

Action-related occurrence
- Required action omitted
- Inappropriate action committed

Cognition-related occurrence
- Short-term deficiency of knowledge (e.g., failure to recognize system state)
- Long-term deficiency of knowledge (e.g., cross-check indicator is unknown)

Other occurrence (e.g., hardware fault, particular circumstance)

Figure 2. CODA wording hierarchy.

Analysis Steps

Figure 3 summarizes the CODA steps for retrospective analysis and illustrates the process. Step 1 requires to compile a short summary that includes the occurrences and their essential context without excessive technical details. As indicated by the internal feedback link in Figure 3, the presentation of the context of occurrences may be revised (updated) in view of the findings from Steps 2 to 5.

In Step 2 the analyst should prioritize major human-related occurrences, and describe the preceding situations, the critical actions (omitted or committed ones) and the links to the respective unsafe system states (error consequences). Furthermore, they have to be described in terms of actions characteristics and underlying performance conditions that are relevant for their context within the incident (Step 3). As outlined by the external feedback link in Figure 3, the performance of Step 3 will be facilitated if a taxonomy of cognitive tendencies linked to action characteristics (ACs) (such as in Table 1) is already available. Then the analyst may use the AC column in Table 1 as a structured guidance for identifying concrete (system/scenario-specific) performance conditions that may cause the ACs:

According to the basic concepts introduced above, the derivation of improvements (Step 4) should be conducted with emphasis on cognitive tendencies (CTs). CTs appear as basic driving factors in the causation of occurrences and thus provide insights for error prevention in future performance situations. Findings from incident analyses in terms of CTs can be used for planning simulator and training programs. Such findings support self-learning. Humans with knowledge about CTs in a
system performance context are sensitized to recognize error-driving conditions in their working environment.

If no CT taxonomy is available or if the intention is to extend an available taxonomy, CODA proposes to identify CTs by generalizing the items that describe the context of the critical actions. However, such generalization may be misleading. It is therefore recommended (Step 5) to seek for confirmation by consulting the personnel of the affected system or by reviewing findings from other incident analyses and behavioral science.

![CODA method steps and feedback for up-dating their outcomes](image)

Figure 3. CODA method steps and feedback for up-dating their outcomes.

2. Analysis Example

The CODA method application is illustrated by an analysis of the loss of feedwater incident at Davis-Besse plant in 1985. All the information about the incident was taken from the NRC (1985) report. The analysis emphasizes control room actions after the initiating event (total loss of main feedwater).

Step 1. Context of Occurrences

Compile a short summary about the context of the occurrences.

11 abnormal occurrences (in the sense of deviations from a fault-free sequence of events) were identified. They are underlined and numbered from #1 to #11. Their context is embedded in a narrative description of the event below.

PWR NPP during power operation, 1:35 (a.m.). Trip of one main feedwater (MFW) pump, reactor trip and main steam isolation (#1). The operators detect immediately the unavailability of the MFW system, since the source of steam for the second MFW pump turbine is isolated. They attempt (decide) to startup the auxiliary feedwater system (AFWS) manually (#2) before its automatic actuation expected after ###5 min. While attempting this, an operator pushes a wrong pair of switches resulting in the feedwater isolation of both steam generators (SGs) (#3) and subsequently in an over-speed trip of both AFWS pump turbines (1:41). At 1:42, the shift attempts to recover the AFWS failure by control room actions, but the feedwater isolation valves fail to re-open (#4). Shift opens the pressurizer (PZR) spray valve (in order to reduce the rate of the increase of the reactor pressure), and begins to attempt to recover the AFWS by local actions at the failed equipment. About 7 min later (1:49), the procedure requires the initiation of feed and bleed (F&B) since the AFWS remains unavailable and both
SGs are essentially dried out. However, the shift supervisor decides to omit the initiative of feed and bleed (#5) as he perceives the recovery of the AFWS to be imminent, and he decides to continue the AFWS attempts. While being involved in the AFWS recovery actions, the primary operator fails to recognize the initial pilot-operated PZR relief valve (PORV) opening/closing operations (#6) at 1:49 and 1:50. At 1:51 the PORV opens the third time and fails to close (#7). After returning to his working place, the primary operator perceives the PORV actuation signal "CLOSED" (front panel), but he fails to refer to the valve position signal "OPEN" (announced by an acoustic monitor at the back panel). Thus he fails to recognize the stuck open PORV (#8). However, he closes the PORV block valve (#9) and the PZR spray valve precautionary (1:52). Fortunately, the PORV re-closes by itself after this action. The primary operator fails to recognize the PORV by-itself closure (#10). One minute later, the operators succeed in the AFWS recovery (1:53). At 1:54 the primary operator re-opens the PORV block valve (#11) without knowing the PORV malfunction (#7).

This is an updated context presentation. It includes internal feedback from the CODA Steps 2 to 5 (Figure 3). Human-related occurrences (i.e. errors) are indicated by bold numbers. Critical actions (inappropriately omitted or committed ones) are printed in italics.

**Step 2. Critical Actions**

List and specify the critical actions.

Five critical actions were identified. They are grouped and listed below.

- Inappropriately omitted (EOO) action:
  - Feed & bleed initiation (#5)

- Inappropriately committed (EOC) actions:
  - AFWS startup attempted (#2)
  - Feedwater isolation of both SGs (#3, given #2).
  - Closure of PORV block valve (#9)
  - Opening of PORV block valve (#11)

The errors above refer to observable interventions. 'Non-observable' but documented errors include deficiencies of knowledge, namely:

- Failure to recognize initial PORV opening operations (#6)
- Failure to recognize stuck-open PORV (#8)
- Failure to recognize 'by-itself-closure' of stuck-open PORV (#10)

Step 2 also addresses the selection of critical actions for further analysis. According to the topicality of the EOC issue, the contexts of the commissions #2, #3, #9 and #11 is presented in Table 2. Occurrence #2 appears as a pre-condition of #3. For simplification, #8 and #11 could be seen as one entity, i.e. a perfect correlation between failure to recognize stuck-open PORV and opening of PORV block valve. It should be noted that occurrences #2, #9, and #11 were not classified as errors in the NRC (1985) incident report. However, as shown in Table 2, they are system failures or contributors to system failures according to the CODA terminology.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Error of Commission</th>
<th>System Failure Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of MFW. Before AFW signal.</td>
<td><em>Startup of the AFWS attempted</em> (#2)</td>
<td>Introduction of an unnecessary chance of AFWS degradation because AFWS startup is automated, and the buttons for manual AFWS startup are located on the same panel as the AFWS-failure-causing feedwater isolation buttons.</td>
</tr>
<tr>
<td>Feedwater isolation of both SGs (#3), given #2</td>
<td>AFWS failure (over-speed trip of both AFWS pump turbines).</td>
<td></td>
</tr>
<tr>
<td>MFW and AFW unavailable. Crew omits feed &amp; bleed. PORV fails stuck-open. Crew fails to recognize PORV status. PORV re-closes by itself. AFWS recovery success.</td>
<td><em>Opening of the PORV block valve</em> (#11)</td>
<td>LOCA, given that PORV fails to re-close and PORV block valve remains open. The PORV re-closed by itself after #9. Here the opening by crew is classified here as an error because it was performed without recognising the initial PORV re-closure problem (#7, #8), and PSA usually does not credit 'by-itself-closure' of a stuck-open valve.</td>
</tr>
</tbody>
</table>

**Step 3. Action Characteristics**

*Identify action characteristics and performance conditions.*

According to the external feedback outlined in Figure 3, this step was conducted by applying the action characteristics (ACs) presented in Table 1. Each of them was found to be a contributor to at least one of the errors listed in Table 2.

According to EOC-likelihood, all of them are grouped as follows.

- **(AC1) An inappropriate action has a high attraction**, if it:
  1. (AC1.1) avoids a delay, and/or
  2. (AC1.2) avoids a drastic side effect, and/or
  3. (AC1.3) matches a nearby aspect, and/or
  4. (AC1.4) is needed or harmless in the likely case.

- **(AC2) Operator's accuracy is needed but low**, if an inappropriate action:
  1. (AC2.1) is possible after a perceived success, and/or
  2. (AC2.2) is possible under perceived time constraint.

Links were drawn between each generic AC and one or more system/scenario-specific performance condition (PC). The opposite hierarchy was observed, too. One PC was linked to more than one AC. In total, 19 PCs were identified. Each of them appears as a quantifiable PSA event. The full documentation of assignments is presented in Table 3.
Table 3. Error-driving action characteristics (ACs) identified by CODA from the NRC (1985) Davis-Besse incident report and their specifications by performance conditions (PCs).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action...</strong></td>
<td>AFWS startup (R2)</td>
<td>Feedwater isolation of both SGs (R3)</td>
<td>Closure of PORV block valve (R9)</td>
<td>Opening of PORV block valve (R11) = stuck-open PORV not recognized (R5)</td>
</tr>
<tr>
<td><strong>(AC1.1)</strong></td>
<td>...avoids delay</td>
<td>Yes. (PC1) About 5 min delay until automated AFWS startup.</td>
<td>Yes. PORV opening possible before AFWS signal (see TMI 1979).</td>
<td>Yes. (PC11) RCS pressure has been at PORV set point. PORV opening can lead to a LOCA.</td>
</tr>
<tr>
<td><strong>(AC1.2)</strong></td>
<td>...inhibits drastic side effect</td>
<td>Yes. (PC2) Reactor coolant system (RCS) pressure is approaching the PORV set point.</td>
<td>Yes. PORV opening possible before AFWS signal (see TMI 1979).</td>
<td>Yes. (PC15) PORV closed&quot; signal at front panel. Nearby interface indicates that PORV block valve can be opened. (PC16) Pressurizer (PZR) spray valve open during AFW recovery, and (PC12) AFW recovery initiated after AFW startup failure. Nearby task matching. RCS depressurisation through open PORV can be attributed to RCS cooldown due to PC16 and initial success of AFW recovery.</td>
</tr>
<tr>
<td><strong>(AC1.3)</strong></td>
<td>...matches a nearby aspect</td>
<td>Yes. (PC3) Loss of MFW diagnosed before AFW signal.</td>
<td>Yes. (PC6) Feedwater isolation switch panel = AFW startup switch panel.</td>
<td>Yes. (PC11) RCS pressure has been at PORV set point. Nearby goal: avoidance of TMIs (LOCAs through-open PORV). (PC12) AFW recovery initiated after AFW startup failure. Actual goal: core cooling via AFW. If AFW recovery succeeds, then open PORV block valve is not needed for RCS depressurisation.</td>
</tr>
<tr>
<td><strong>(AC1.4)</strong></td>
<td>...is needed or harmless in the likely case</td>
<td>Yes. (PC5) Correct execution of AFW startup is more likely than incorrect execution.</td>
<td>Yes. (PC10) Feedwater isolation switch manipulation is reversible.</td>
<td>Yes. (PC13) PORV block valve closure is reversible. RCS pressurization is possible even if AFW recovery fails. PC12 AFW recovery initiated after AFW startup failure. AFW recovery success is more likely than its failure.</td>
</tr>
<tr>
<td><strong>(AC2.1)</strong></td>
<td>...is possible after success perception</td>
<td>Yes. (PC3) Loss of MFW diagnosed before AFW signal.</td>
<td>Yes. (PC3) Loss of MFW diagnosed before AFW signal.</td>
<td>Yes. (PC19) AFW recovery success.</td>
</tr>
<tr>
<td><strong>(AC2.2)</strong></td>
<td>...is possible under time constraint perception</td>
<td>Yes. (PC2) RCS pressure is approaching the PORV set point.</td>
<td>Yes. (PC2) RCS pressure is approaching the PORV set point.</td>
<td>Yes. (PC14) SGs are boiling out.</td>
</tr>
<tr>
<td>**</td>
<td></td>
<td>Yes. (PC12) AFW recovery initiated after AFW startup failure.</td>
<td>Yes. (PC12) AFW recovery initiated after AFW startup failure.</td>
<td>Yes. (PC12) AFW recovery initiated after AFW startup failure.</td>
</tr>
</tbody>
</table>
PC1 (about 5 min delay until automated AFWS startup) appears also as a decisive technical condition for the EOC (feedwater isolation) indicated by #3. This condition points to the exposure time, i.e. the time window where the EOC must be considered as critical. The 5 min window follows from physical system behavior. After loss of steam of the MFW pump turbines (due to closure of main steam isolation valves), the steam from main steam piping and moisture separator re-heaters allows to provide adequate flow for about 4.5 minutes (NRC 1985, page 3-13). After that time, the AFWS would start automatically, and the EOC can be viewed firstly as unrealistic.

**Step 4. Cognitive Tendencies**

*Derive improvements with emphasis on cognitive tendencies.*

Table 1 lists the underlying cognitive tendencies that correspond to the action characteristics identified under Step 3 (Table 3). They provide insights for preventing errors by hazard cognition. Some respective proposals addressing the safety awareness of operators are discussed below.

On the basis of the findings in Table 3, operators could be informed about cognitive tendencies in plant-specific contexts. An operator who understands the error-driving potential of a tendency in a few contexts of a system he is familiar with, may have a better chance to anticipate other contexts where this tendency may result in an error. Such training may be offered in simulator sessions or seminars that address the lessons learned from specific occurrences. Two example of a subject of hazard cognition training based on the finding in Tables 3 are outlined below.

- According to CT2.2 (hastiness after time constraint perception), attention should be given in training to the fact that fast transients (Table 3, PC2) often force unnecessary high-speed human responses. An operator who is aware of this tendency in a fast-transient situation, may reconsider the consequence of what he is doing, i.e. the probability of an error like #3 (feedwater isolation) would be reduced.

The operator may implement such reconsideration by referring to the procedure or by asking another operator in order to clarify the meaning of the label of the button before pushing the button.

- According to CT1.4 (non-conservative) and CT1.3 (fixation), the awareness should be trained that human decisions are often based on the anticipation of the most-likely consequence, especially, if this consequence is the most desired one (Table 3, PC11, PC12, PC13, #9). An operator who is aware of these tendencies may consider the consequence of the less likely (but adverse) consequence before implementing a risky decision.

These are simplified examples. Research is needed regarding detailed implementation of hazard cognition in the training of plant personnel.

Of course, some of the performance conditions presented in Table 3 point to more direct options for improvements, e.g., eliminating PC6 by local separation of the switches. Such kind of proposals are side products from applying the Table 1 CT taxonomy.

**Step 5. Verification of Findings**

Table 4 shows that the cognitive tendencies identified by CODA are supported by findings from behavioral science and other event analyses. Further support is outlined in Mosneron-Dupin et al. (1998) and Reer (1997b).

A revised and English version of the incident analysis results in Reer (1997b) is presented in Table 5. This table shows that the Table 1 CTs are applicable to error occurrences observed in various working situations. Each CT-underlying object of action characterization is specified. Thus the process of CT assignments is traceable and discussible on the basis of concrete items.

A verification on a detailed level, i.e. checking whether proposed improvement measures contribute to future error prevention, would require long-term investigations. Such investigations are out of the scope of the current state of development of the CODA method.
<table>
<thead>
<tr>
<th>Global tendency</th>
<th>Specified tendency</th>
<th>Links to other findings</th>
</tr>
</thead>
</table>
| (CT1) Discrimination (making distinctions) between attractive and less attractive responses | (CT1.1) Impatience or curiosity | • Operators tend to make ad-hoc decisions (Kauffmann 1995)  
• A conflict between immediate and long-term objectives (Williams 1988) |
| | (CT1.2) Reluctance toward something drastic | • Risk searching behavior in loss situations (Kahneman & Tversky 1979)  
• An incentive to use other more dangerous procedures (Williams 1988) |
| | (CT1.3) Fixation on something nearby | • Similarity matching (Reason 1990)  
• Omission of functionally isolated tasks (Rasmussen 1979; Wehner & Mehl 1986)  
• Rigidity (Reason 1990; Mehl et al. 1995)  
• Perceptual tunneling (Swain & Guttmann 1983)  
• A mismatch between an operator’s model of the world and the imagined by the designer (Williams 1988) |
| | (CT1.4) Non-conservative probabilistic reasoning | • Frequency gambling (Reason 1990)  
• Operators tend to make non-conservative decisions (Kauffmann 1995)  
• Incredulity response (Swain & Guttmann 1983)  
• A mismatch between perceived and real risk (Williams 1988) |
| (CT2) Fluctuation of performance accuracy | (CT2.1) Relaxation | • Very low task load; reduced attention to tasks considered as non-critical (Swain & Guttmann 1983)  
• Low alertness (NRC 1998) |
| | (CT2.2) Hastiness | • Time stress, heavy task load (Swain & Guttmann 1983)  
• Perceived urgency (NRC 1998) |
Table 5. Illustration of the CODA concept for describing actions for the purpose of operationalizing cognitive tendencies as contributors to errors under adverse contexts.

The objects in the headings are identified - specified beside the incident descriptions. Abnormal (or unusual) occurrences are underlined and referred to by >. Critical actions (inappropriately omitted or committed ones, respectively) are printed in italics. The incident descriptions are based on the information presented in: BMI (1977), Kier & Müller (1992), Kremers (1996), MosheroDupin et al. (1997), NRC (1985), Pev et al. (1981), Semmer (1994), Smidt (1979), Swain & Guttmanns (1983)Veenen (1993). Abbreviations: BWR - boiling water reactor; CP - chemical plant; NPP - nuclear power plant; PWR - pressurized water reactor; GWS - general work situation.

<table>
<thead>
<tr>
<th>Cognitive Tendency</th>
<th>(CT1:1) Discrimination between attractive and less attractive responses</th>
<th>(CT1:2) Reluctance</th>
<th>(CT1:3) Fixation</th>
<th>(CT1:4) Non-conservative</th>
<th>(CT2:1) Relaxation</th>
<th>(CT2:2) Hastiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adverse Context</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>EEO-driving Predicate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>• causes...</td>
<td>• causes...</td>
<td>• mismatches...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is unnecessary or harmful in the...</td>
<td>is needed after...</td>
<td>is needed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is needed under...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(EOC-driving Predicate)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• avoids...</td>
<td>• avoids...</td>
<td>• matches...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is needed or harmless in the...</td>
<td>is possible after...</td>
<td>is possible...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is needed under...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td>delay</td>
<td>drastic side effect</td>
<td>nearby aspect</td>
<td>likely case</td>
<td>perceived success</td>
<td>perceived time constraint</td>
</tr>
<tr>
<td></td>
<td>delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. NPP, BWR. A specific cable shaft is not free of leakers (occurrence #1). An operator is using a burning candle (#2) for the close-up check of this cable shaft. He detects a leakage (indicated by the flickering of the candle light) and seals it. However, there is still a remaining leakage (#3). Then he conducts the leakage test by using the candle again (#4). He fails to remove the candle (#5) when the sucking air stream (due to the remaining leakage) occurred. So the fire of the candle ignites foam and cables.</td>
<td>Delay:</td>
<td>Drastic side effect:</td>
<td>Nearby aspect: &gt;#2, task: checking for leakage &gt;#4, preceding event: first use of candle</td>
<td>Likely case: &gt;#5, no remaining leakage</td>
<td>Perceived success: &gt;#5, first leakage detection and sealing</td>
<td>Perceived time constraint:</td>
</tr>
<tr>
<td></td>
<td>delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. NPP, BWR, power operation. The number of allowable scrams per year is already reached (#1). Occurrence of a main steam leakage (#2) in the turbine hall. As part of the plan to detect the leakage (by inspecting the turbine hall), personnel inhibits the automatic scram actuation (#3).</td>
<td>Delay:</td>
<td>Drastic side effect: &gt;#3, exceeding the number of allowable scrams per year (requires shutdown for the rest of the year)</td>
<td>Nearby aspect: &gt;#3, goal: isolation of leakage (recovery of direct cause of the problem)</td>
<td>Likely case:</td>
<td>Perceived success:</td>
<td>Perceived time constraint: &gt;#3, system parameters are approaching the scram set point</td>
</tr>
<tr>
<td></td>
<td>delay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. GWS. A service operator has finished his scheduled work at a customer. He is going to visit the next customer. It is in the afternoon, the time of 'rush hour' traffic is imminent (#1). However, the current customer requests an additional task (#2), repairing a difficult accessible lamp. The ladder suitable for this task is placed five floors below in the building. But the operator uses a non-optimal ladder (#3) placed nearby. He works carefully, and succeeds in repairing the lamp. When leaving the ladder, he jumps down (#4) from the third rung, stumbles adversely (#5) resulting in hurt of one foot.</td>
<td>Delay:</td>
<td>Drastic side effect: &gt;#3, increased time until arriving at the next customer</td>
<td>Nearby aspect: &gt;#4, preceding event: time-saving use of non-optimal ladder</td>
<td>Likely case: &gt;#4, no harm even if using a non-optimal ladder &gt;#5, no harm even if jumping down from a ladder</td>
<td>Perceived success: &gt;#4, &gt;#5, lamp repaired under adverse conditions (difficult to access, non-optimal ladder)</td>
<td>Perceived time constraint: &gt;#3, &gt;#4, rush hour is imminent</td>
</tr>
<tr>
<td></td>
<td>Delay</td>
<td>Drastic side effect</td>
<td>Nearby aspect</td>
<td>Likely case</td>
<td>Perceived success</td>
<td>Perceived time constraint</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4. NPP, PWR, before initial startup. Operators check the closeness of the reactor cooling system (RCS). They do this by setting a pressure of 112 bars for the RCS. However, in spite of this action, the pressure remains below 112 bars because of a valve remained open (#1). They continue to increase the pressure (#2), but the pressure still remains below 112 bars. Then they start to diagnose the unexpected low pressure. They detect the erroneously open valve and close it, but they omit to reduce the pressure (#3). Thus, serious RCS damage occurs due to over-pressure.</td>
<td>-</td>
<td>-</td>
<td>&gt;#2, task: pressurization &gt;#3, preceding event: detection of erroneously open valve</td>
<td>-</td>
<td>&gt;#3, erroneously open valve detected</td>
<td>-</td>
</tr>
<tr>
<td>5. CP, process for producing near's foot oil. A plug causes a disturbance of the process (#1). Personnel attempts to recover the disturbance. For this purpose, they dismantle a flange. However, they omit to close the radiation valve (#2). Thus perchloric ethylene steam escapes.</td>
<td>-</td>
<td>-</td>
<td>&gt;#2, task: recovery of plug problem</td>
<td>-</td>
<td>&gt;#2, plug detected/ located</td>
<td>-</td>
</tr>
<tr>
<td>6. NPP, PWR, low power, during startup. After several delays (#1) due to &quot;slides&quot; in scheduling, a test to the Auxiliary Feedwater System (AFWS) has to be carried out. The operator fails to reduce power (#2), i.e., he performs the test at a power higher than required. After the test, a steam dump valve remains jammed half open (#3) due to mechanical failure. An overcooling transient begins. The operators suspect that the &quot;position-open&quot; indication given is erroneous since limit switch problems have already been reported. To confirm their diagnosis, they verify that the closure signal has indeed been sent to the valve. Therefore they do not isolate the leak (#4) which is the cause of the cooling of the reactor, and attribute overcooling entirely to the test that was not performed at the nominal power level. The crew believes it has the situation under control, and the operators inhibit safety injection (SI) when the first criterion appears (#5). Subsequently, the operators do not refer to an emergency procedure (although need for it is annunciated by an alarm); instead, they apply a normal-operation procedure (which would be correct for the absence of #3). and, according to this procedure, they inhibit SI at its second actuation criterion (#6). Later on, the shift supervisor detects the worsening of the situation, looks for the cause, detects the valve stuck open, and asks for the valve to be closed.</td>
<td>&gt;#2, &gt;#4 &gt;#5 &gt;#6, increased time until power operation</td>
<td>&gt;#4, &gt;#5, &gt;#6, cold water injection, pressurizer overfill possible</td>
<td>&gt;#2, &gt;#4, &gt;#5, &gt;#6, goal: avoid further delay in power operation &gt;#4, expectation (desirable system state): valve closed &gt;#4, &gt;#5, expectation of minor overcooling cause: non-nominal power during test performance &gt;#6, preceding event: first inhibition of SI</td>
<td>&gt;#2, higher power often (usually) does not cause problems &gt;#4, spurious &quot;valve-position open&quot; indication (is more likely than valve's failure to close) &gt;#5, &gt;#6, SI often unnecessary, conservative actuation criteria</td>
<td>&gt;#2, &gt;#4, &gt;#5 &gt;#6, to avoid further delay in power operation &gt;#5, &gt;#6, system parameters are approaching the SI actuation set point</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Scenario</td>
<td>Delay</td>
<td>Drastic side effect</td>
<td>Nearby aspect</td>
<td>Likely case</td>
<td>Perceived success</td>
</tr>
<tr>
<td>-----</td>
<td>----------</td>
<td>-------</td>
<td>---------------------</td>
<td>---------------</td>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>1.</td>
<td>CP, process for producing dye-stuff-related substances. An operator is mixing substances in a vessel. During the filling-in of soda-lye, he omits to switch on the stirring rod (#1). Thus the substances cool down as an inhomogeneous mixture. After detecting that the temperature of the mixture is too low, the operator heats up the mixture (#2). Later on, after detecting that the stirring rod is out of operation, he switches on the stirring rod (#3). This results in an unwanted exothermic chemical reaction and release of substances after opening of safety valves.</td>
<td>-</td>
<td>-</td>
<td>&gt;#1, preceding event: detection of low temperature. &gt;#3, event: detection of non-operating stirrer</td>
<td>-</td>
<td>&gt;#2, low temperature detected &gt;#3, non-operating stirrer detected</td>
</tr>
<tr>
<td>2.</td>
<td>Refinery: An operator is present in the control room (CR). A fire occurs (#1) in the process-related systems outside. In the CR, many alarms occur and many instruments behave abnormally. The operator omits immediate initiation of fire-fighting (#2). Instead, he runs upstairs and demands an instrumentation technician, “What’s wrong with my instruments?”. By the time he returns to the CR, it is too late to reduce significantly the loss due to the fire.</td>
<td>-</td>
<td>-</td>
<td>&gt;#2, effort/costs if fire-brigade comes, blame on the demander if no fire</td>
<td>-</td>
<td>&gt;#2, no fire even if some alarming (a fire is an extremely rare event)</td>
</tr>
<tr>
<td>3.</td>
<td>GWS: For rooms containing equipment under high voltage a safety system exists that inhibits the door (of the respective room) from opening before high voltage is switched off. Once an operator - who is working in such a safe room (i.e., free of high voltage) - leaves the room for a short duration (#1). When he intends to return to his work, he confuses the rooms, and attempts to enter into an unsafe room (#2) (i.e., not free of high voltage), but the safety system inhibits the door from opening. However, being deeply convinced standing in front of the correct (safe) room, the operator expects the door blockade to be spurious. Thus he circumvents the door blockade (#3), and enters into the unsafe room.</td>
<td>-</td>
<td>-</td>
<td>&gt;#3, task: returning to work after interruption</td>
<td>-</td>
<td>&gt;#3, returning to the right room after leaving it</td>
</tr>
<tr>
<td>4.</td>
<td>NPP, BWR, power operation. Trip of all recirculation pumps (#1). The operators attempt to implement natural circulation, but this fails, because they close two more discharge valves than required (#2). Thus core-coolant-level decreases in the center of the reactor vessel (while the level in edge remains normal). Later on, low-coolant-level alarms occurs. Firstly, the operators omit to take action for coolant makeup (#3). They expect the alarm to be spurious because they strongly believe in their correct implementation of natural circulation: if natural circulation then coolant level must be normal. Later on, the operators implement the correct action.</td>
<td>-</td>
<td>-</td>
<td>&gt;#3, success of preceding task (implement natural circulation)</td>
<td>-</td>
<td>&gt;#3, correct execution of an initiated task (implement natural circulation)</td>
</tr>
</tbody>
</table>
3. **Method Summary**

Table 6 summarizes the features of and the findings from the CODA method based on the questionnaire response outlined above as well as on the findings presented in Reer (1997a), Reer (1997b) and Reer et al. (1999).

<table>
<thead>
<tr>
<th>Table 6. CODA method summary.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Underlying concepts</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Steps and procedures</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Lessons learned: practical guidance; limitations</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Application of method</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Contributors to action / human factors mission failure</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Consequence and measures taken</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

An extended summary is outlined below, under two headings,

- methodological insights into **Error Analysis**, and
- insights concerning causes and consequence of **Errors of Commission**.

171
Error Analysis

1 Each error-underlying critical action (the inappropriately omitted or committed one) is the subject of information collection in CODA (Figure 3). The description of a critical action provides direct access to error-driving performance conditions (Tables 3 and 5).

2 For the human-centered identification of error causes, CODA uses the concept of cognitive tendencies as illustrated in Figure 1 and specified in Table 1. This concept provides a systematic tool for anticipating (operator) and predicting (analyst) error-driving performance conditions.

3 Among all CODA method steps (Figure 3), the implementation of Step 1 (Context of Occurrences) requires the highest effort. Previous insights into cognitive tendencies have lessened the effort required for Steps 3 (Action Characteristics) and 4 (Cognitive Tendencies).

4 The qualitative outputs from CODA incident analyses are:
   - error-underlying cognitive tendencies;
   - error-underlying action characteristics;
   - error-underlying performance conditions;
   - proposals for anticipating similar error-driving conditions in the future.

5 The quantitative outputs from CODA incident analyses are:
   - the number of the underlying cognitive tendencies (CTs) per error;
   - the number of the error-driving performance conditions (PCs) per error;
   - correlation coefficients regarding the common presence of CTs.

The first two output appears as a coarse error-likelihood-index estimates. The third output allows for index refinements regarding CT interrelations and weights.

Errors of Commission

6 Regarding cognitive aspects in error causation, CODA does not distinguish between and EOO and EOC. CODA uses the same list of pre-defined cognitive tendencies for analyzing both error types (Table 1).

7 A technical boundary condition (cf. Table 3, PC1) appears to be typical for an EOC: the error exposure time (t), since the likelihood of taken the inappropiate action seems to correlate positively with time; the longer the time where there is an opportunity for taken the inappropiate action, the higher the error likelihood. This is a hypothesis in contrast to the influence of the time (t) available for success defined for an EOO; here the likelihood of taking the required action is often supposed to correlate positively with time. In both cases, the action likelihood vs. time correlation is positive (i.e. P_{action} = 0 at t=0 and P_{action} > 0 for t>0), but the basic action characteristic (required vs. inappropriate) is different.

8 Two groups of global cognitive tendencies as EOC causes under adverse contexts appear as relevant:
   - (CT1) discrimination between attractive and less attractive responses, and
   - (CT2) fluctuation of performance accuracy.

Each group is specified (Table 1 and 4) by detailed cognitive tendencies and the corresponding error-driving action characteristics (ACs).

9 According to the specification within the attraction tendency group (CT1), an EOC is likely if an inappropriate action
- ... avoids a delay (AC1.2), and/or
- ... avoids a drastic side effect (AC1.2), and/or
- ... matches a nearby aspect (AC1.3), and/or
- ... is needed or harmless in the likely case (AC1.4).

According to the specification within the accuracy tendency group (CT2), an EOC is likely if an inappropriate action
- ... is possible after perceived success (AC2.1), and/or
- ... is possible under perceived time constraint (AC2.2).

Many inappropriate actions have ‘harmless’ consequences in the sense that they result in unsafe states but not in physical damages. This is a positive safety feature on the one hand, but a negative one on the other hand due to Table 1 AC1.4: actions that are usually harmless but inappropriate are likely to be committed. Therefore, retrospective event analyses should cover also actions that result in precursors of system failures. This would enhance the empirical information useable for HRA.

4. Glossary

The basic terms underlying the CODA method are defined below. Two main features of this system of definitions should be highlighted first:

- A human error is defined within the context of a considered system failure.
- The EOO/EOC dichotomy refers to direct observable behaviors (omitted/committed actions) only.

| Action | Human-induced intervention (active change of system state). |
| Action characteristic | Generic item that describes the context of a critical action. |
| Adverse context | Error-driving constellation of performance conditions. |
| Cognitive tendency | Typical human habit or attitude in work performance. |
| Critical action | Required or inappropriate action. |
| Error of commission | Inappropriate action implemented or attempted. |
| Error of omission | Required action not implemented or not attempted. |
| Error-producing condition | Performance condition resulting in an increased error likelihood. |
| Fixation on something nearby | Cognitive tendency concerning discrimination between attractive and less attractive responses. A response is attractive if it matches something nearby - an current task, a preceding event, an adjacent control and the like (see Table 5 for further nearby aspects). Performance is always based on selective perception - it is impossible to consider all stimuli. Thus humans focus on the stimuli that appear as nearby and consider inadequately other stimuli that might be relevant. |
| Hastiness | Cognitive tendency concerning fluctuation of performance accuracy. Humans work relatively fast under conditions that indicate that there is some urgency. This is appropriate if the priority of the respective fast response is so high that it acceptable to neglect side tasks such as verification checks. |
| Hazard cognition | Human anticipation (identification, consideration, re-cognition) of adverse contexts. |
| Impatience or curiosity | Cognitive tendency concerning discrimination between attractive and less attractive responses. A response is attractive if it avoids a delay. Humans dislike to wait or to accept delays or interruptions. |
Inappropriate action  
Action that results in an unsafe system state.

Incident  
Sequence of past events within the context of an unsafe system state.

Non-conservative probabilistic reasoning  
Cognitive tendency concerning discrimination between attractive and less attractive responses. A response is attractive if it is appropriate in the likely case. Humans tend to consider inadequately the consequence of the unlikely case. This may be appropriate if this consequence is (a) minor, or (b) extremely unlikely.

Occurrence  
Deviation compared to a normal or usual or undisturbed sequence of events.

Performance condition  
Any specification of a performance situation in terms of a well-defined event.

Relaxation  
Cognitive tendency concerning fluctuation of performance accuracy. Humans work less accurately (alerted) under stable/safe-seeming conditions; this may be appropriate if the conditions are indeed as stable as they seem, since - in the long term - human beings cannot work permanently with high level of accuracy. CODA views a perceived success as a plausible stimulus for stable/safe-seeming conditions. Research is needed to identify further ones.

Reluctance toward something drastic  
Cognitive tendency concerning discrimination between attractive and less attractive responses. A response is attractive if it avoids a bad side effect, e.g., plant shut-down for days. Humans seek for better solutions if a required response is accompanied by a severe loss.

Required action  
Action needed to avoid an unsafe system state.

Unsafe system state  
System failure (damage, loss, component unavailability) or unnecessary precursor of it.

5. PSA Relevance
CODA consequently links cognitive tendencies to observable action characteristics and quantifiable performance conditions in the analyzed system. Therefore, all CODA-related findings outlined above are of high relevance for predictive Human Reliability Analysis (HRA) in Probabilistic Safety Assessment (PSA) of complex systems. An outline of a CODA-based HRA method is presented in Reer et al. (1999).

6. References
BMI (1977), Besondere Vorfälle in Kernkraftwerken der Bundesrepublik Deutschland, Berichtszeitraum 1965-1976, Der Bundesminister des Innern, Bonn (D).


Hoyos, C. Graf (1980), Psychologische Unfall- und Sicherheitsforschung, Kohlhammer, Stuttgart (D).


Contribution from the Netherlands  
PWG-5 Task 97-2  

Gerben Heslingsa  
KEMA Connect, The Netherlands

1. Describe the method used to analyze errors of commission, including  
1a. A statement of the purpose and scope of the method used in the analysis

In general Errors of Commission (EOCs) can be analyzed in two ways, in a proactive manner and in a reactive manner. The purpose of the proactive manner is to predict in a systematic way where EOCs are possible in existing procedures and working instructions, its probability of occurrence and what the consequences may be. In this way, it is in principle possible to predict errors and their consequences not yet occurred. The reactive method considers incidents that have already occurred and, starting from the incident, potential (root) causes are identified. The focus is on the search for errors (e.g. EOCs) and its root causes on the basis of incidents or near misses to come to recommendations of improving the context. This improvement should result in a reduction in the error, probability or a change in the design so that human error cannot take place (e.g. due to automation).

Until last year, two nuclear power plants were in operation for which a number of PSA studies were made including modeling the human error errors: the Dodewaard nuclear power plant and the Borssele nuclear power plant. Last year the Dodewaard nuclear power plant closed and the remaining plant, the Borssele plant, was consulted to gather information on incidents involving EOCs in order to contribute to Task 97-2. Through this, the method for reactive analyses of EOCs was investigated. At the same time the way EOC is modeled in a proactive manner as part of the PSA was studied.

1a1. Purpose and scope of the proactive analysis of EOCs

In the past the scope of the proactive approach in the Dutch PSAs was on Errors of Omission (EOO). This means that the non-performance of an action was only taken into account. The analyses that are made of complex installations appeared not to present the reality correctly; in particular the EOCs that occur at disastrous accidents may have a significant impact on the accident sequence. A couple of years ago the PSA studies were extended with modeling ECCs.

One of the main difficulties in the proactive analysis is to determine beforehand which incorrect actions a person may undertake. Techniques like HAZOP and FMECA¹ are too limited to predict these errors if no analysis constraints are defined. This is particularly caused by the many possibilities for a human to fail making such an analysis too extensive. In order to come to a method that is able to make realistic predictions of human errors and the consequences that may follow attention has to be paid to:

- the combination of conditions (both of the plant and of the environment during the accident sequence) that put humans on the wrong feet
- and the presence of influencing factors (such as the presence of procedures, having the right education, etc.).

This combination is termed error forcing context (EFC).

¹ HAZOP: Hazard and Operability studies
FMEA: Failure Modes and Effects Analysis
The scope of the proactive analysis of EOCs in the Borssele PSA was first to study EOCs during normal power operation and later during low power conditions. In principle all possible failure modes that may occur in following the procedure available were distinguished and analyzed. To make the analysis practical, a successive screening was used to identify those EOCs with the highest potential of occurrence. The overall purpose was to identify the most significant EOCs on the basis of consequences, recovery potential and likelihood.

1a2. Purpose and scope of the reactive analysis approach

The reactive approach at the Borssele power plant is based on the HPES (Human Performance Enhancement System) developed by INPO. In applying this approach no distinction is really made between EOO and EOC. Also equipment performance problems are taken into account. The scope is to evaluate equipment and human performance problems, uncover the causes and determine corrective actions to prevent recurrence.

The reactive method includes three major areas of evaluation:
- what happened
- how it occurred (mechanism) where a number of behavioral factors may be identified (e.g. spatial misorientation, confusion, unawareness, etc.)
- why it happened (causes) where a number of causal factors can be identified to explain the behavioral factors

Information about the WHAT, HOW and WHY may be gathered through:
- interviewing
- task analysis
- change analysis
- barrier analysis
- events & causal factors analysis

The way Borssele is performing the proactive and reactive analysis is given below (step 1C) in more detail.

1b. A description of the underlying concepts of the analysis method used (that is, reference to human sciences, if relevant)

The proactive approach and the reactive approach are largely focussing on the observable behavior in first instance. Usually, the typical definition of human error is the non-performance or incorrect performance of desired activities, provided that adequate conditions for correct performance are present. The 'adequate conditions' is in fact the crucial part where it can be decided whether undesired performance is assigned to the human or to other sources (e.g. technique, organization, etc.).

The trend in Borssele is to go beyond observable behavior and to distinguish behavioral factors and causal factors that may lie outside the human. The proactive and reactive approach adopted is considering not the human to fail but more the context to fail. This is in line with ATHEANA approach of the EFC. Although the term 'human error' is still used it is more seen realistic and in line with insight from the behavioral sciences to talk about inappropriate (non) performance or unrequired actions induced by the context.
1c. A summary of the steps taken or the procedure used for conducting the analysis

A distinction is made to describe the procedure for the proactive and reactive analysis.

1c1. Procedure for the proactive analysis as applied in the Borssele PSA

The larger part of this procedure can be found in Heslinga (1999). This section contains a summary of that. The text was largely taken from Borssele (1997).

EOCs were studied in a proactive way in the Borssele PSA for both the full power mode of operation and the non-full power mode of operation. The approach for both modes of power in the Borssele EOC study was essentially the same and consisted of the following steps:

- identification of the human system interactions that provide opportunities for errors to occur,
- identification of the failure modes of functions, systems, or components that could occur as a result of those errors (to be termed error expressions),
- identification of the most significant error expressions.

In more detail these steps are as follows: The first step in the analysis is to identify the opportunities for EOCs, opportunities which are sought on the basis of any requirement for operators to interact with the plant. The interaction may be a response to an unexpected change in plant conditions or an essential part of a specific evolution. Such activities may lead to errors whose impact is immediately revealed or to errors that have latent effects. The latter concern errors made during maintenance, test and calibration activities and may not be revealed directly during the full power mode. These errors however may lead directly to equipment malfunctions in the shutdown mode. Possible opportunities for errors and their impact on the plant can be obtained from: an understanding of the activity and the context within which it is taking place. These "error expressions" correspond to failure modes of equipment or functions. In the Borssele EOC study Operations and Maintenance activities have systematically been reviewed. Post-accident activities have been categorized into cognitive responses (global and local misdiagnosis) and executions for which the proactive and systematic HAZOP style was followed regarding 'What IF' questions.

The next phase of the analysis is a screening analysis to assess the importance of these error expressions whether their probabilities of occurrence need to be calculated. Screening may be done on consequence, on likelihood, and by identifying recovery mechanisms. Due to the nature of the shutdown analysis itself, an initial screening on consequence is performed during the search for error expressions. The only error expressions identified are those that either result in an initiating event, or have a significant impact on the accident development or mitigation. Screening on likelihood is done by successively identifying possible modes of error, and then searching for possible causes of those errors. The causes are expressed in terms of influencing factors for which the number and character can be different for power mode analysis (where they are termed Performance Influencing Factors, PIFs) and the non power mode analysis (where they are termed Error Producing Conditions, EPCs).

The approach adopted in both modes described above is generally the same but in detail there are differences. First, in the non-power mode, the identification of EOCs leading to initiating events

---


related to loss of a critical safety function is more important than the errors that lead to a reactor trip. As a result, there are more possibilities outside the control room, e.g. maintenance, to cause the initiating event. In full power PSAs, errors resulting in initiating events are rarely modelled explicitly, particularly because the response in most cases is independent of the cause of the trip and because its EOC probability of occurrence is incorporated in an overall frequency of that event. In the non-power mode, it is important to identify the relation between the cause of the initiating event and the response since they usually involve the same function. Secondly, the operator responses may not clearly be guided by procedures as in the full-power case. Thus, misdiagnosis is potentially a much more significant concern. However, the diagnosis is more focused on the root cause of the loss of a single function rather than identifying a type of accident. An additional consequence of the "root-cause-driven" response is a stronger dependence between what causes the initiator and how the operator responds to it.

1c2. Procedure for the reactive analysis

The method that Borssele uses for the reactive analysis is aimed at understanding incidents that occur during different modes of operation in order to learn about deficiencies in the whole organization (including procedures, education, etc.). The method is somewhat different from the original HPES method of INPO in the sense that a subset of the factors is considered that the HPES method is using in describing the three areas of evaluation (i.e. the factors to describe the WHAT, HOW and WHY of the incident). The steps applied in Borssele are as follows:

1 Situational analysis; this step aims at defining the situation in terms of 'when, where, what, job & shift characteristics, etc.' Although the HPES method applies a number of forms to support this step, it is not used as such. The situational analysis forms may be used as a checklist in describing the situation during which the incident occurred.

2 Behavioral factors analysis; this step identifies the factors that explain how the inappropriate action(s) occurred. Information is gathered by interviewing the person(s) involved or by performing a 'walk-through' task analysis. More than one behavioral factor may be present for each inappropriate action involved in the event. The method distinguishes approximately 50 factors and a distinction is made between internal and external factors. Examples of internal factors are cognitive overload, habit intrusion, spatial misorientation, etc. Examples of external factors are unusual plant conditions, lack of fidelity between simulator/training and plant, task interruptions, etc. Borssele only distinguishes two factors, viz. Personnel and Procedures/organization. In addition to these behavioral factors Borssele adds Technique as a 'how' factor. The distinction in three factors is made because a similar distinction already existed in Borssele, i.e. TOPA (Technique, Organization, Personnel and Administration). These three 'how' factors may be termed circumstances by Borssele.

3 Causal factor analysis; this step aims to identify the causal factors that - combination - produce the behavioral factors identified in the preceding investigation phase. These causal factors can be regarded as 'why' the inappropriate action occurred and the behavioral factors can be viewed as 'how' it happened. A distinction is made between human aspects and technical aspects. For the human aspects twelve categories of causal factors exist containing approximately 150 factors. Borssele is considering all of these factors to explain the behavioral factors Personnel and Procedures/organization. To explain the Technique factor approximately 100 factors are used. To gather the causal factors a number of analyses may be used, viz. task analysis, barrier analysis, etc. The behavioral factors are indicators of the
applicable causal factors. How to why matrices may be used that show the most likely causal factors for the behavioral factors.

Borssele may use the event and causal factor charting to illustrate the incident. This is a method to graphically display the sequence of events plotted on a time line and to which the behavioral factors and the causal factors are mapped. Borssele is applying the analysis method and the charting in a pragmatic manner. First the events that occurred are identified and these are displayed in the charting with a diamond. To each event the 'how' factor (Personnel, Procedures/organization, Technique), i.e. the circumstances is coupled. These circumstances are displayed with ovals. The cause of each circumstance is then sought for and displayed in ovals shaded with one end. Terminal events are shown by circles; these are in fact the events that were the reason to start the reactive analysis.

2. Describe in detail the event or sequence analyzed

It appeared not to be possible to find an event in Borssele in which human errors had occurred during an accident scenario from the set of events that were selected for this study (the events from 1995 until now). It was however possible to find an incident in which an EOC occurred and where a turbine trip and reactor scram occurred. This incident will be depicted with the description of the sequence of events, the behavioral and causal factors and it will be illustrated through an event and causal factors diagram.

The event started with a limitation of cooling water with the plant not operating at full power. During increase of the power, condenser vacuum appeared to be too low. It was decided to clean the condensers one by one, starting with condenser I. This cleaning is done by creating a return flow in a part of the condenser so that debris is removed. Due to this process cool water flow became lower and as the operator did not control the generator power properly before starting cleaning the condenser, the condenser pressure increased too much in relation to the generator power. This resulted in a turbine trip. The main steam pressure consequently increased so that a reactor scram occurred. Subsequently there was a trip of the main condensate pumps and the operator started a main condensate pump although the conditions were not met. This led to an undesired opening of the turbine bypass valves.

This incident was a repeat of a similar incident that occurred four years earlier. The measures that were taken in terms of adaptation of instructions appeared not to be sufficient.

The following three events were distinguished:

A  During cleaning condenser 1 the condenser pressure increases so that a turbine trip occurs
B  Increase of main steam pressure to > 81,4 bar so that a reactor scram takes place
C  Turbine bypass valves open whereas the control is on manual; the operators did not expect this as they started a main condensate pump.

Each event was further analyzed regarding the HOW and the WHY and a chart was drawn. The figure below shows this chart. As can be seen an EOO and an EOC occurred. The causes of these errors can be found in poor written communications, management methods and system design.
3. Describe the findings from the analyses, including

3a. Findings regarding the method used, especially theoretical insights, practical lessons learned (e.g., software requirements, expertise requirements, resource requirements), and data input and output

The operators cleaning the condenser without decreasing the generator power beforehand might be regarded as an EOO and the start of the main condensate pump whereas the proper conditions are not met as an EOC. Whether we should term these as 'errors' is subject of discussion as the retrospective analysis described above revealed root causes and a context that force the operator to fail. In total three root causes were distinguished:

- communication in writing, i.e. insufficient written rules: rules/criteria regarding the condenser vacuum minimally needed in relation to allowable generator power where one condenser is allowed to be cleaned.
- management methods: the corrective actions (adaptation of instructions) was insufficient to prevent repetition. It was in fact a limitation in the ergonomics which could not be compensated through written measures.
- system/component design and analysis, i.e. bad ergonomics: the control concept for the turbine valves deviates from control concepts that are used at other control devices.

These three root causes formed a constructive starting point in Borssele for improving the working situation to reduce the probability of EOOs and EOCs that may occur in similar situations.

3b. Findings regarding errors of commission, especially contributors to these errors and consequences of these errors in the event or accident sequence analyzed

In this section a distinction is made between the proactive and reactive analysis approach.

3b1. Findings regarding the proactive analysis approach in Borssele PSA as compared to ATHEANA

The way EOCs are incorporated in the Dutch PSA seems to follow - in large steps - a similar approach as in ATHEANA, i.e. the three basic steps as identification of human/system interactions, the systematic search for error expressions and the determination of causes are overlapping. In ATHEANA particular events in the PSA related to incorrect human performance, i.e. the Human Failure Event (HFE), are modeled and from these Unsafe Actions potentially causing the HFE are modeled. The causes of the Unsafe Action are modeled by use of the so-called Error Forcing Context (EFC). The EFC is a combination of Performance Shaping Factors present and the plant state. The model assumes that the EFC is the basic cause for human error.

The main difference between ATHEANA and the study on EOCs in the Borssele nuclear PSA (Borssele, 1997) appears to be the structure in identifying EOCs and the search for causes. More structure becomes visible in the Borssele study in which more proactive and systematic search is made for opportunities for error, such as through the application of HAZOP or FMEA. ATHEANA claims that this is also done in their method but this seems to have much more the character of a brainstorm. Such a brainstorm approach is then particularly used in establishing unsafe actions and the

EFC. In the Dutch PSA the interaction between process and human forms much more the basis on which a systematic search is done to come to the possible unsafe actions.

May the search for opportunities be more systematic and proactive in the Borssele study, the search for causes of the EOC seems to be more extended in ATHEANA. However, neither ATHEANA, nor the Borssele analysis of EOCs uses a proper model for team behavior. A team is reduced to one person to whom a probability has to be assigned. The communication within a team that can form a reason for yes or no error committed is underdeveloped in the current analyses. This drawback is however applicable to many PSA studies.

Although ATHEANA is claimed to be a method for inclusion of EOCs in a PRA in a proactive manner the way ATHEANA is applied up to now (USA, 1998) does not show this proactive approach yet. For some events it has been used in a reactive way to describe the EFC present before and during the incident. It seems that the current state of adopting both processes is as follows: the Borssele EOC study was performed and led to inclusion of potential EOCs in the PSA thus updating the PSA, whereas the ATHEANA has not been extensively applied to be included in a PSA as such but only as a reactive tool to describe the EFC of various incidents.

The cognitive aspects of rational (and irrational) problem solving are usually not properly modeled for the prediction of EOCs in many studies, including the Borssele EOC study and ATHEANA. KEMA therefore studied cognitive tendencies (see Heslinga, 1999) which may be a common mode for a number of EOCs to be committed during accident sequences. In our work in the EARTH working group we studied the notion of cognitive tendencies in analyzing a number of nuclear power plant incidents. We were able to explain how a number of cognitive tendencies were related to human errors committed during the incident. The use of cognitive tendencies to be able to better explain and predict EOCs has to be developed further as the use of a similar approach to describe the EFC (such as in ATHEANA) is insufficient. A strong recommendation is therefore given here for the adoption of such cognitive tendencies in the prediction of EOCs.

3b2. Findings regarding the reactive analysis approach

Similar retrospective analyses have been performed in Borssele, most of them being much more complex than the one described above. The retrospective analysis method as applied by Borssele on a number of events revealed insights in the root causes of events, some of these causes dealing with deficiencies in the direct working environment, the technique and the organization. The measures that can be taken have direct effect on preventing similar events to occur and also presumably on other events that have not yet occurred because of the search for root causes preventing only the treatment of symptoms. None of the information gathered has been used to improve the PRA. Measures are however taken in most situations to remove the contributor of these errors resulting in qualitative reduction of the possibilities for incident to occur.

The breakdown of the event as it is done in the Borssele retrospective method requires much expertise and may become a lengthy exercise with complex incidents. However the systematic structure that is applied using particular categories for the HOW and the WHY helps to consequently analyze the

---

5 USA (1998), U.S. Nuclear Regulatory Commission’s Peer Review meeting of ATHEANA, June 11-12, 1998, Seattle, USA.


7 European Association on Reliability Techniques for Humans, Mosneron-Dupin, et al., 1997
incident in similar and comparable ways. Through this, results are obtained on root causes that can be compared and can be discussed between different users of the method on the basis of using the same 'language'.

It appears that in the way the retrospective method is applied in Borssele on numerous incidents no clear distinction is being made between the EOO and the EOC. This can be explained by the fact that for such a reactive approach such a distinction is of less interest. In this case they were classified after the incident has taken place by considering whether that something should have been done and has not been done, or that something was done which was wrong. For determining the root causes such a classification in EOO and EOC is for the retrospective analysis as performed in Borssele not relevant and in fact too broad regarding the mere detailed classification that is used in Borssele for the WHAT, the HOW and the WHY.

The EOC\textsuperscript{6} was defined here in a rather straightforward way as it is done by a number of other authors (see Heslinga, 1988)\textsuperscript{5}. In defining the EOC is this way there is ambiguity as it applied through using the phrase 'adequate conditions'. What is adequate or not is a subjective and debatable issue and it often becomes clear that in considering the root causes of the EOC one can in fact not talk about an error. The retrospective analysis in this report shows that the two events that were termed EOO and EOC were definitely not caused by the human operator but through inadequate conditions in the documentation, management methods and system design. Whether something is an EOC or not (and this does not only account to EOC but also to the EOO) depends on how someone sees the conditions as being error forcing or not (see also the discussions in Gerdes, 1997\textsuperscript{10}, and Heslinga, 1988)\textsuperscript{11}. In both the proactive and reactive analyses we are not interested in the error but in the deviation, either caused by man, by machine or even by the organization to come to constructive measures to prevent those deviations to occur. The term EOC is as such even a misleading construct, whether the focus is on a proactive or reactive analysis.

\textsuperscript{5} The error of commission is the non performance of a desired activity provided that adequate conditions are present.


Acknowledgement

The author is indebted to the N.V. Elektriciteits-Produktiemaatschappij Zuid-Nederland for their contribution to this report.
Contribution from The Netherlands
TASK 97-2: Errors Of Commission

Dr. Linda J. Bellamy
SAVE Ingenieurs/Adviesbureau

Dr. Louis Goossens and Professor Dr. Andrew Hale
Delft University of Technology / Safety Science Group
The Netherlands

Q.1a Purpose and Scope of the Method Used in the Analysis

A report of the OECD/NEA committee on the Safety of Nuclear Installations\(^1\), recognizes, among other issues, the importance of modelling errors of commission. Within the OECD Nuclear Energy Agency, a task has been established, task 97-2, to investigate these Errors Of Commission (EOCs) in two phases:


The current report concerns Phase 1, concentrating on a method, ATHEANA\(^2\), \(^3\), A Technique for Human Error Analysis which is of interest to the Nuclear Safety Department of the Dutch Ministry of Social Affairs and Employment (SZW) and the Ministry of Environment (VROM), Directorate for Chemicals, External Safety and Radiation protection.

The work was undertaken jointly by SAVE Consulting Scientists (Dr Linda Bellamy) and the Technical University of Delft Safety Sciences Group (Professor Andrew Hale and Dr Louis Goossens). Our relevant expertise is in research and application of human error modelling, safety management systems modelling and auditing, risk assessment and major hazards. We took an approach within the chemical industry in order to benefit from a hybridisation (chemical x nuclear) of methods and ideas, and fulfil a number of convergent aims of the project participants.

The main aspect of the ATHEANA methodology which differentiates it from other methods is its focus on 'error forcing conditions' which recognizes the interactions between human-centred aspects of error (the psychological mechanisms) and the specific nature of plant conditions in a particular failure scenario.

For the chemical industry, there is a continuing dependence on the nuclear industry for human error modelling and quantification in risk analysis. The current project therefore provided an opportunity to look at a new human error-modelling tool not only in the nuclear context but also from the chemical industry perspective. That is, for the Ministry of VROM with respect to its role in QRA regarding major


hazard chemical installations, and for the major hazard policy group of the Ministry SZW with respect to it role in chemical hazard control and the inspection of major hazard sites. This is particularly valuable at a time when the new European Seveso II Directive places so much emphasis on the identification by companies of 'scenarios' and their chance of occurrence.

The Netherlands occupies a leading edge position, in Europe at least, with respect to the linking of the Safety Management System to Technical Systems in risk management. The ministries of VROM and SZW have supported development work in organization and safety, the development of inspection tools for the Labour Inspectorate and cross-disciplinary modelling approaches, such as the EC project I-Risk. The concept of 'error forcing conditions' in ATHEANA fits in well with this human-technical linking approach.

The aims of our approach were therefore focussed towards the chemical industry, while at the same time providing answers to the PWG-5 questionnaire for which a chemical industry application could provide new insights. The Steering Group therefore included both nuclear and chemical persons from the two ministries. The agreed aims were as follows:

To explain what an error of commission and error forcing context is in the chemical industry context, with emphasis on accident scenarios involved in major hazard accidents involving dangerous substances.

Application of the ATHEANA method to analysing a serious chemical accident to identify whether it provides additional information and understanding about causes.

Investigation of whether this accident could have been predicted by the use of the ATHEANA method.

From the results of 1-3, to provide an evaluation of the ATHEANA method, indicating strengths and weaknesses of the method.

Consideration of the value of applying ATHEANA to chemical installations in the context of existing schemes for evaluating the risks of major hazard chemical installations, particularly for those involved in the assessment and inspection of major hazard sites.

Methods for the modelling of human error for Probabilistic Safety Assessment (PSA) or Quantitative Risk Assessment (QRA) tend to concentrate on the modelling of the human error in the post-initiator accident sequence. However, the technical model for QRA in the chemical and petrochemical industries differs

---


from that used in PSA even though the basic principles of risk analysis are the same. There is much less emphasis placed on the modelling of human errors in the chemical industry because post-initiator modelling in QRA concentrates on the functioning of safety systems which are part of the design. For example, the Dutch "Handbook for Producing and Assessing an External Safety Report" specifies human error modelling requirements mainly in terms of describing:

- Any human action causes of Loss Of Containment (LOC) events and
- Omission errors in shutting off a release following LOC.

Fault tree analysis might be used for certain specific scenarios. Apart from the mentioning of the above, the main emphasis in the QRA modelling is hardware/software failures.

The approach taken in the current study relies heavily on the application of QRAs for the chemical industry. We do not consider methods to just identify errors of commission as stand-alone events. The input to a QRA is generally threefold:

Technical failures are identified through design scrutinizing methods like HAZOP (system flow approach), FMEA (component level), and other appropriate techniques. The result is either that potential failures are designed out of the system by redesign, or identified to provide input information for developing the accident scenarios of the QRA. The input can be qualified as accident precursors: initiating events, component and subsystem failures. The methods are capable of identifying almost all failures, but there will always be a potential for undetected failures which eventually may lead to unidentified, but very relevant accident scenarios.

Job safety analyses and/or task analyses are capable of identifying human errors in the operational and maintenance phases of the manual work to be done by workers. Generally speaking, these techniques enable one to identify most errors of omission. Errors of commission will probably not be detected. Chemical reactivity analyses identify potential chemical reactions, in particular those which are different from the intended chemical reaction. If the reaction mechanisms are associated with exothermic reactions, there is a great potential for major hazards events: runaways. Not all possible runaways will be detected.

Standard QRAs use historical datasets and the modelling of the accident scenarios is not (sufficiently) driven by management factors. These factors may influence the QRA output drastically, as they may increase the individual failure rates and human error rates, but they may also introduce couplings between subsystems which are modelled as independent subsystems in the QRA. Moreover, the management factors can be responsible for a large potential of human errors of commission.

In a series of research studies analysing the kind of data that underlies the Generic Failure Data used in chemical QRAs, the causes of Loss Of Containment were found to be about 70% structural failures (corrosion etc.) and about 30% human error causing containment to be bypassed. That is, human error as an immediate (not latent) cause. Latent errors, such as maintenance omission errors in safety systems or failing to blank off open containment, could result in either structural failure or

---


By evaluating past performance, for instance by applying methods such as the Accident Sequence Precursor Technique\footnote{Bellamy, L.J. and Geyer, T.A.W. (1992) Organizational, Management and Human Factors in Quantified Risk Assessment Report - Health and Safety Executive Contract Research Report 33/92}, it may reveal where management factors are indeed dominant. Another useful input which has been developed from a theoretical point of approach can be found in the European I-RISK project\footnote{Hurst, N.W., Bellamy, L.J., Geyer, T.A.W., Astley, J.A.A. (1991) A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies. J. Hazardous Materials., vol.26, no.2, 1991, p.159-186.}.

The direct linking of safety management systems to the technical system has recently been achieved in the chemical industry through examining accident scenarios for specific equipment using an approach described in\footnote{Goossens, L.H.J. and Cooke, R.M. (1997) Applications of some risk assessment techniques: formal expert judgement and accident sequences precursors. Safety Science Vol. 26, No. 1/2 pp. 35-47, 1997.} Such an approach gives optimism for the identification of the Safety Management System "gene" which characterizes a particular site or installation and which stamps its mark on everything. However, this is well outside the scope of the current study, and we barely, if at all, touch on management systems and their common mode effects. This is perhaps an area where the chemical industry could provide wisdom to the nuclear industry in the future.

Compared to the nuclear industry then, the chemical industry has put much more emphasis on Safety Management Systems in preventing accidents than it has on human error and human error modelling (also reflected in the 1996 EU Seveso II Directive).

\begin{alltt}
\end{alltt}
Our scope in examining ATHEANA is in the context of the value of this as a tool for identifying Errors Of Commission which may play a significant role in contributing to chemical accident risks by causing:

- accident sequences hitherto unrecognized in the QRA model
- escalation of events in the accident sequence

Q.1b Underlying Concepts of the Analysis Method

Previous Definitions of Error of Commission (EOC) in the Context Of Nuclear PRA
A report to WG5A CSNI, OECD, on Errors of Commission from the British HSE NII 20 gives the following definition:

An error of recognition, diagnosis or intention, that leads to a series of acts formed with well-meaning intentions, but which are inappropriate for the technical scenarios that pertains.

Or,

An isolated error introduced with an otherwise appropriate series of actions that may arise from a random aberration in behavior, or may be induced by the inappropriate application of an habitual task behavior.

The definition given in NUREG/CR-626521 is:

An overt, unsafe action that, when taken, leads to a change in plant configuration with the consequence of a degraded plant state.

An important point which the authors make is that: “By this definition, the EOCs of interest do not include all random actions that occur in the plant. Rather, one of the important goals of the project is to focus more narrowly upon those EOCs that degrade plant safety and, therefore, should be included within the scope of PRA” (p. 4–1).

NUREG/CR-635022 refers to unsafe actions which are:

those actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition.

In this context, an error of commission represents:

either the inappropriate termination of a necessary safety function or an initiation of an inappropriate system.

Errors of commission represent the impact of incorrect operator responses and should not be modelled as non-responses which has been past practice [p. 2–17].

---


Errors of commission can occur in the pre-initiator, initiating event, or post-initiator phases of the Probabilistic Risk Assessment (nuclear)/Quantitative Risk Assessment (chemical) plant logic model (fault trees, events trees and initiators). In the ATHEANA context these failures are not point occurrences in time, because the effect may not be immediate and may be recoverable for a period of time after they occur. In this respect the EOC is a failure of a whole process which ultimately results in an irreversible change in plant status.

In the nuclear context, Cooper et al.\textsuperscript{21} identified 4 ways in which operators can fail plant functions through EOCs (in the post-initiator phase):

- by turning off running equipment
- by bypassing the signals for automatically starting equipment
- by changing the plant configuration such that plant defences are defeated
- by depletion or diversion of plant resources (e.g. water supplies) to which is added in\textsuperscript{20}:
- by inappropriate initiation of a system
- by increasing/decreasing control of the system impact.

A distinction should perhaps be made between errors where there is a degree of intentionality in operator actions (such as from misdiagnosis), and hence a dependency between a sequence of actions, and where actions are unintentional (a slip or execution error), in which case it is argued that the dependency in a sequence of actions is more related to the dependency through feedback from the plant\textsuperscript{25}. Such a distinction can apply equally to errors of omission which are not of interest in this study.

Error Forcing Context (EFC)

NUREG/CR-6350\textsuperscript{26} identified 4 common characteristics of (commission) error forcing context to emerge from accident analysis:

1. The plant behaviour is outside the expected range
2. The plants behavior is not understood
3. Evidence of the actual plant state and behavior is not recognized
4. Prepared plans are not applicable or helpful


A key requirement for which ATHEANA was designed was to guide the search for non-nominal accident conditions (outside the normal range of typical PRA models), and include the influences of deficiencies in procedures and training etc., with respect to applicability to non-nominal accident scenarios. These non-nominal conditions with the combined influence of complicating plant conditions and complicating human conditions are the error-forcing contexts which "virtually guarantee human error." (7, p.1-4).

The observable influences on human performance are the error forcing contexts: the combined effect of performance shaping factors and plant conditions. (The 'observable' aspect requires that such contexts are auditable). The EFCs trigger internal psychological mechanisms which leads to a refusal to believe evidence that runs counter to the initial misdiagnosis or failure to recognize that evidence, resulting in subsequent errors of commission (and ultimately an accident with catastrophic consequences).

Because the EOC (in the definition of 88 concerns the whole process of failure, inclusive of error recovery, the EFC must address not only the initial error, but also the failure to recover.

The psychological mechanisms involved in EOCs are not described in detail here. The important point to appreciate, however, is the link between the EFC and the triggering of error mechanisms. These error mechanisms may be ones which under other circumstances are 'good' in the sense that they allow speedy skilled actions to take place through a kind of short-cutting. For example, like chess players studying a position, operators do not have the time to study every possible scenario and so they take short cuts in problem analysis. Training and procedures provide one context to short-cut. But excessive short-cutting (such as under the time stress of a particular scenario) or poor pattern matching (where the operator is 'fooled' by the plant conditions) can result in an error 89.

The point being made is that error mechanisms can occur when operators apply normally useful cognitive (thinking) processes. Discussion of psychological mechanisms involved is given by Reason 90.

Reason 90 gives a variety of explanations for intentional errors. The mental model of the current situation is wrongly constructed for a whole range of possible reasons. From the psychological perspective, these errors are 'mistakes' in that the wrong intention is formulated. Mistakes should be distinguished from 'rule violations' since different mental mechanisms are involved in the latter. For unintentional errors (actions not as planned) the psychological mechanisms tend to be those associated with strong habits and routinized actions with perceptual and attentional 'slips' and memory 'lapses' being involved.

SAVE-TU Delft Classification With Consideration For the Chemical Context
Our aim was to develop a tight definition of what we were going to look at in this project, with respect to identifying Errors of Commission (EOCs) and Error Forcing Contexts (EFCs) in the chemical industry (major hazard) context.

---


'Commission' is an external error mode (it involves a wrong action). The internal error mode is found in the psychological mechanisms which are involved. These mechanisms are associated with terms such as attention, memory, perception, understanding, motivation, assessment, decision making, response selection- which are not directly observable, but which are important in human information processing activities connecting stimuli and responses. The mental representation of the situation, whether conscious or not, and its translation into action, are what are important. An error of commission always involves a significant mismatch between the mental model of the situation and the reality. Failures in information processing, such as attentional failures for example, are referred to in ATHEANA as Psychological Error Mechanisms.

ATHEANA points to the detrimental effect that a commission error has on plant conditions. The starting point for defining EOCs is the external error mode which can be identified as important in Quantitative Risk Assessment.

An Error Of Commission which is of interest in a risk model is:

Definition 1
An action that leads to a change in plant configuration with the consequence of a degraded plant state.

This is a slightly modified definition of that given in

And:

In addition, the psychological aspects are important in defining an EOC. We have taken previous definitions (see Section 1.2.1), namely:

Definition 2
An error of recognition, diagnosis or intention, that leads to a series of acts formed with well-meaning intentions, but which are inappropriate for the technical scenarios that pertains.

Or,

Definition 3
An isolated error introduced with an otherwise appropriate series of actions that may arise from a random aberration in behavior, or may be induced by the inappropriate application of a habitual task behavior.

For the purpose of identifying EOCs to be incorporated into the into the risk assessment model it is also necessary to define Error Forcing Contexts (EFCs) which cause them.

The Error Forcing Context (EFC) can be defined as:

Definition 4
The combined effect of performance shaping factors and plant conditions that trigger psychological error mechanisms, and which must address not only the initial error but also the failure to recover it.

Here, Performance Shaping Factor (PSF) means:

Definition 5
Any factor which influences human performance in the interaction between the human and the system upon which they are acting.

Different Human Reliability Assessment methods identify different sets of PSFs, but they commonly include competence, procedures, man-machine interface design (displays, controls, labeling), task design factors (workload, stress), and organizational factors with a direct influence (communications, supervision). The interaction between these factors in specific contexts is not well defined or understood, but these factors are considered to influence the occurrence of error because of relationships identified in, for example, accident analysis, and from experimental studies.

One aspect crucial to the definition of EFC is, we believe, the question as to how people can take an action which is legitimate in some circumstances and not others. ‘Legitimate’ has the same kind of meaning here as ‘intentional’. On the other hand, there are also EOCs which are actions which fall outside the consideration of ‘legitimate’ where the action is unintentional.

We will not exclude these unintentional errors from consideration in EOCs. For intentional EOCs the underlying psychological mechanisms are important, such as:

The choice to take the (wrong) course of actions for reasons that looked good at the time which gives the operator a mind set not to deviate from their course of action, such as a frequency matching response (the situation looked like this in the past and the response was appropriate then).

2. The choice to take the (wrong) action because this is a new problem and the operator responds (inappropriately) dependent upon his current knowledge base.

In this respect, the mental database that the operator taps into during the sequence of responses is appropriate for consideration.

For unintentional errors, such as a slip in following a procedure, the underlying mechanisms are different, but may have the same effect on the plant. The EFCs must be different in these 2 cases.

The EOC which is of interest to us is the one which ultimately triggers a dynamic response in the process conditions. But we are stuck with the problem of how far back do we go? Suppose temperature is driving a chemical process. The operator puts in the wrong mixture and it affects the temperature change which is then misdiagnosed and this leads to an EOC. The entering of the wrong mixture is as much of interest as the misdiagnosis and subsequent error.
The important thing is therefore to consider the dynamic change from the Risk Assessment point of view. There may be many causes of dynamic change (of temperature, say), one or more of which may be an unintentional EOC. Mismatch possibilities arise between the mental picture of what has happened and the actual situation based on a) these various possibilities, b) the mental database of the operator and c) dependent upon the extent to which the plant condition signals distinguish between the causal possibilities.

It is difficult to think of a definition of EOC without considering the risk (QRA) model. Dynamic change in the process is a crucial feature of the accident sequence which contains one or more EOCs. EOCs are conditioning the probabilities in QRA in the sense that the probability of failure is bigger than that considered from a design only point of view because there are scenarios where the EOC plays a significant role. These EOCs we consider to be of the following types:

EOC1 = A human action which is an initiator. It directly causes a dynamic change which initiates the accident sequence.
EOC2 = A human action which defeats a safety system during the post-initiator sequence
EOC3 = A human action in the post-initiator sequence which makes the situation worse (e.g. accelerates the dynamic change).
EOC4 = A human action which defeats a safety system at some time before it is needed (before the initiating event)
EOC5 = A human action which defeats the information system at the same time as it is needed (such as switching off an alarm during the post-initiator period)
EOC6 = A human action which defeats the information system before it is used (such as making errors in a written procedure, wrongly calibrating an instrument).

These EOC types are located in the model shown in Figure 1:

This set of EOCs extends the definition of EOC found in ATHEANA for the purpose of covering what is of interest in chemical QRA. The events leading up to a loss of containment involving a release of hazardous material need to be modeled in such a way as to enable the influence of EOCs on the chance of such a release occurring to be modeled. Chemical manufacturing processes are extremely diverse and the identification of the influence of EOCs on possible causal events leading to Loss Of Containment cannot be covered by the 6 ways described in the ATHEANA method (see 1.2.1) in which operators can fail plant functions through EOCs. Pre-initiator actions are not given.

Figure 1: An information processing model to show the relationship between EOCs Psychological Mechanisms, and Plant Conditions.
Errors of Commission and QRA Modelling

In chemical QRAs human errors are modeled in the fault trees and event trees where appropriate. Human errors are presented as Errors of Omission (EOOs) and (almost never) contain contributions of Errors of Commission (EOC). Human errors are taken into account either as initiating events or as basic events of failures of Lines of Defense (LODs) in the technical system.

In the ATHEANA process flow model (see Figure 2 in Section 1.3) the PRA-model (in nuclear terms) is put somewhat aside (the block is shown by dashed lines), which seems logical from a retrospective analysis point of view. In a pro-active analysis the PRA-model should get more emphasis, deriving from the ATHEANA process the requirements for further analyses.

Projecting QRA-modeling onto the ATHEANA multidisciplinary HRA framework (see Figure 3 in Section 1.3) foresees for design-based QRAs almost no human failure events being modeled. Scenarios are based on plant design conditions. In current procedures it is not customary to take account of the management system, which essentially finds the place for (some of) the EOCs. What is required is that QRA modeling stretches out over the design envelope and takes account of the full consideration of error forcing contexts (EFCs) and human errors (both error mechanisms and unsafe actions).

In our view the EFCs are the most important ones to model as the EFCs enable plant conditions to be expressed in the context of other modes of the life cycle, in particular during operations and possibly also for maintenance. In other words, instead of using design configuration we can now use operational configurations of plant conditions.

A quite important shift in our thinking occurred in respect to the Error Forcing Context in QRA. That was the idea that, in the consideration of failure modes of the design, the analyst should evaluate the possibilities of failure outside the normal expectations of the behavior of the design (e.g., what if the temperature went over 250 deg C?) in order to examine potential operational configurations. This should be done even though it may not be possible to conceive the cause. This subject is brought up again later in Section 5. Its relevance is apparent in the accident analysis (Section 2.1), which shows events occurring outside an expected range of the temperature behavior of a chemical reaction.

In modeling EFCs completely the EFCs may provide three types of outcomes with respect to scenarios in the QRA-models:

Outcome 1: Increasing probabilities or frequencies of occurrence of initiating events or failures of recoveries and safety systems in the event trees, and/or basic events in the fault trees (using already existing scenarios). After applying ATHEANA to improve the QRA, this type of outcome only updates the probabilities (even in a qualitative manner). This would be simply a factoring up of HFEs, which may increase the top event probability.

Outcome 2: Adding new scenarios to the set of already existing scenarios. The EOC adds a new scenario with an additional event tree (new situations). There are more routes to get to Loss of Containment LOC). This would be a very interesting outcome as new scenarios broaden the perspective of the QRA. The question is, of course, whether ATHEANA really leads to new scenarios not previously established.

Outcome 3: The EOC introduces couplings between basic events in the fault trees, initiating events, and safety system failures in the event trees. The result should be modeled through dependent failures which can drastically increase the probability of an LOC. This is difficult to model
in QRA, and Management Factoring approaches address this problem.

By applying the six types of EOCs defined in Section 1.2.3, the following can be deduced:

EOC type 1 leads to Initiating Event.

Two possibilities:

The EOC might increase the frequency of occurrence of the initiating event. The post-initiator safety functions should correct this adequately.

The EOC introduces a new scenario, of which it is not clear whether the post-initiator safety functions can cope with that adequately.

EOC type 2 leads to Post-initiator safety system failure.

One possibility:

The EOC defeats a safety system, such that the system fails with a probability = 1.

EOC type 3 leads to Post-initiator safety system failure

Two possibilities:

The situation leads to a new scenario, and the EOC introduces another route in the required safety systems, for which none adequate are available.

The EOC defeats one or more safety systems, because the current capacity is too low, and not because the safety system is switched off, again p.failure = 1 (or almost).

EOC type 4 leads to Post-initiator Safety System failure

One possibility:

The EOC defeats one or more safety systems prior to having the initiating event (e.g., a stand-by pump or engine is left under maintenance all the time).

EOC type 5 gives a basic failure in a Post-initiator Safety System.


One possibility:

A new basic event must be added to the fault tree for which Safety System failure is the top event.

**EOC type 6 is a causal factor for an Initiating Event or Safety System failure.**

One possibility:

The causal factor can be relevant for an initiating event or a safety system, in which the frequencies or probabilities of failure are increased each, or as a combination (such as leaving out maintenance for all pumps at one time).

<table>
<thead>
<tr>
<th>EOC type</th>
<th>Increased probabilities</th>
<th>New Scenarios</th>
<th>Couplings and large increase in probabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>5</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Three major problems are identified:

- It is difficult to understand how new scenarios can be found within the technical design of the installation. Human error does not contribute directly to the technical escalations of the processes.

- It might be an overwhelming task to define all possible human error routes. How can this be linked through the “Human error” box without ending up in millions of possibilities.

- The same is true for the definition of all possible couplings.

A potential solution for this is to link the “scenario definition” to the “Human failure events” in the multidisciplinary HRA framework (Figure 3, Section 1.3.1) more directly, within the design envelope. Maybe (this is not explored fully yet) design techniques (like tailor-made HAZOP, FMEA techniques) are useful tools to further develop in this sense.
Q.1c Summary of Steps Taken in Conducting the Analysis

Overall Approach

Our overall approach was aimed at testing the ATHEANA method. To this end, we undertook three main tasks:

1. Define the key concepts of ATHEANA in the chemical industry context
2. Analyse the chemical accident to identify all the components specified by the ATHEANA model
3. Analyse the same chemical installation, but this time looking at the scenario modelling in QRA applying the ATHEANA approach.

For this study we are primarily interested in EOC identification and not their quantification. The WG5 report on human reliability modelling describes the task steps. The steps we followed are summarized below and cross-referenced to Figure 1 which is from the original source document. More details in applying the model to our task is given in 1.3.2 for task 2 and 1.3.3 for task 3.

Step 1: Identification of the candidate Human Failure Events (HFE) to be modelled. These HFE's are the events in the risk model at the function, system or component level. Failure modes are "similar" to those caused by hardware faults (e.g., failure of a safety function to start on demand). Note: ATHEANA looks only at the event tree branches but we want to look at pre-initiators too. We are interested in more than the plant safety functions post-initiator. Is the ATHEANA support going to be sufficient for this?

Step 2: Identification of potentially important types of Unsafe Actions that could cause each HFE.

Step 3: For each type of unsafe action, the most significant reason for its occurrence including the failure to recover it. The approach requires looking for "rational" explanations for unsafe acts (responding in accordance with the rules).

Step 4: For each type of unsafe action and its associated reason, identification of the potentially significant error forcing contexts. This is the summarizing and analysing of the information gathered to deal with step 3, with particular emphasis on plant condition factors.

The quantification steps are reported here for completeness (although we do no quantification):

1. Estimate likelihoods of error forcing contexts and consequent error forcing contexts.
2. For each HFE, for potentially important causal unsafe acts, sum the Error Forcing Context likelihoods and consequent probabilities.

The ATHEANA approach is summarised in Figure 2:

*Figure 2: The ATHEANA Process Flow Diagram (adapted from [1])*
Figure 3: Multidisciplinary HRA Framework (After [1]) showing position of chemical QRA

Plant Design QRA

Error Forcing Context

Human Error

PRA Model

Risk Management Decisions

Plant Design, Operations And Maintenance

PSFs

Error mechanisms

Unsafe actions

Human Failure events

Scenario Definition

Plant conditions
Application to Chemical Accident Analysis

We selected a chemical accident which had an Error Of Commission as one of the necessary causes in the accident sequence. It was a big accident resulting in fatalities and major damage, and one that had not been "foreseen". For application of ATHEANA to the accident analysis we used Steps 2-4. The results were easiest to show in the form of a table (Section 2.1). The data were collected from detailed written confidential accounts and particularly from discussions with persons who conducted the accident investigation. The data collected were structured in such a way as to pull out the information relevant to identifying EOCs and their causes.

The following fields were identified:

Act number:
Sequential numbering of each procedural action, whether leading to error or not.

Time:
The actual time at which the action was performed.

EOC Type:
If the action was an error of commission, this was subcategorized according to our own definitions developed for the different EOC types (see Section 4).

Normal procedure:
This describes what the normal procedural step was for the operation of the chemical process.

Unsafe actions:
Unsafe actions carried out according to the meaning of Unsafe Action in ATHEANA (see Section 4 Definitions).

Error forcing context (EFC):
This is divided into Plant Conditions and Performance Shaping Factors which together comprise the EFC.

Recovery Potential:
Since Error Of Commission is a process (a failure not recovered) the potential for recovery needs to be described. This was not made explicit in ATHEANA as something to look for.

Error mechanisms:
These are the unobservable psychological mechanisms which mediate between the Error Forcing Contexts and the Unsafe Acts

Application to Scenario Modelling
For application of ATHEANA to scenario identification we used steps 1-4, then developed a fault tree model to show candidate HFE’s.

The analysis was of the same vessel which featured in the accident analyzed for this study. The idea was to try to carry out an analysis as though it were pre-accident, and as though we were doing the QRA for the first time. The scenario was a catastrophic failure of a reactor vessel and the idea was to try to identify candidate EOCs.
The modelling process was carried out by two risk assessment persons on the basis of technical data that had been provided about the design and operation of the plant prior to the accident. No human factors expertise was provided and there were no discussions with plant personnel. The risk assessors had not been involved in the accident analysis, although they were familiar with the general context of the accident.

The approach taken was one which could be easily followed in the process of doing any chemical QRA according to the Dutch approach for external safety assessments. The QRA approach is far more simplified and quicker to perform than the extensive PSAs in the nuclear industry. Therefore, it has to be understood that the depth of the approach in using ATHEANA matches a level of effort that one might expect in a real context.

The basic principle was to consider where there were human interactions with operating the system. Had we been looking at the whole plant, this would have involved identifying other equipment where there was also a human interaction.

The sequence of steps were as follows:

1. Describe the process and equipment
2. Describe the process sequence by defining the procedural steps/actions involved
3. Identify the function of the step and possible outcomes (good and bad). This leads to consideration of the possible functional failure which is a candidate Human Failure Event.
4. Inventorise the possible Unsafe Acts and Error Forcing Contexts for each step in the process which in combination lead to the Error of Commission which gives a negative outcome.

Group the common outcomes in terms of the relevant Human Failure Events (Errors Of Commission).

Had we be doing this for real, there would have been more data collection at the site on technical and management issues in order to investigate the possibilities for the error forcing context, and the results would have been developed in a much more plant specific way and in relation to the actual management system.

Q.2 Detailed Description of the Event Analyzed

Retrospective Analysis of the Accident

The accident took place in a chemical batch processing plant, which made resins according to recipes. The resin was tailor made, which meant that the recipes were regularly changed. On this particular occasion, an operator fed the wrong mixture into the reactor vessel. Recipes were made up by lining up the relevant storage vessels and feeding the correct quantities into the reactor. The recipe that the operator used was itself wrong and the operator had followed it exactly. As a result of the wrong mixture, the normal procedure for getting the polymerization reaction going did not work and the temperature was taking an abnormally long time to reach the goal point. Eventually more heat was added in an attempt to speed up the process. However, an unstoppable runaway reaction had started, and had in fact caused localized polymerization around the heating/cooling coils thus precluding heat transfer. Ultimately the reaction caused the vessel to BLEVE, destroying most of the site, and causing 3 deaths. During the several hours after the wrong mixture had been fed into the tank up until just before the BLEVE, no-one recognized the situation despite the abnormal plant conditions. Lack of knowledge, design and procedural weaknesses, and a focus on production conspired to generate a powerful Error Forcing Context. However, the temperature behavior of the product, under such conditions, was at that time barely known in the industry.
as a whole and therefore there was no attention for safety systems for dealing with the possibilities for such a runaway and plant personnel certainly did not expect it. Even in the last moments of the accident when the conditions within the vessel had gone off the scales of the temperature and pressure instrumentation, fire fighting personnel were standing close to the vessel some still without protective clothing on. No site alarm had been given.
<table>
<thead>
<tr>
<th>Act No.</th>
<th>Time</th>
<th>EOC type</th>
<th>Normal procedure</th>
<th>Unsafe actions</th>
<th>ERROR FORCING Plan conditions</th>
<th>CONTEXT Performance shaping factors</th>
<th>Recovery potential</th>
<th>Error mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*****</td>
<td>6</td>
<td>Quality Lab produces recipe for a resin, involving 3 chemicals: C9 DCPD Codimer</td>
<td>A typing error was made in the recipe by the head of the quality lab. Instead of typing the tank number for C9 as 632, the laboratory worker typed 634. He typed..... Sort: C9 DSM Tank: 634...... Another substance was in 634: in fact DCPD which is 95% resin forming as opposed to C9 which is 59% resin forming.</td>
<td>- Possible attentional distractors? - Why was he thinking of 634? - The head of the quality lab knew all the numbers by heart so probably worked from memory - Tank 634 was not often used - The head of the lab expected to self check, but being a routine may have weakened this process - The lab had no idea about the risks of having too much DCPD. They were close to Production and distanced from the knowledge of the research lab.</td>
<td>Why didn’t the lab personnel self check and recover their own error? Was it really a typing slip-up or was it a genuine mistake with the tank number?</td>
<td>- Could be an unintentional slip typically associated with routine highly practiced actions. But it could also be a mistake. Maybe the lab actually thought C9 was in 634. 2 and 4 are not next to each other on the keyboard.</td>
<td>- Complete lack of knowledge about the risks of DCPD.</td>
</tr>
<tr>
<td>Act No.</td>
<td>Time</td>
<td>EOC type</td>
<td>Normal procedure</td>
<td>Unsafe actions</td>
<td>ERROR FORCING Plant conditions</td>
<td>CONTEXT Performance shaping factors</td>
<td>Recovery potential</td>
<td>Error mechanisms</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| 2      |      | Recovery failure of Act 1 | Four persons in the organization check a changed recipe: Head of quality lab (see Act 1), Production Manager, Process Engineer, Shift Supervisor | No one noticed the typing error. | - Since the resin was tailor made, recipes were being changed every day.  
- Receiving a variation to a standard recipe was a routine procedure.  
- There was no formal procedure for checking variations to standard recipes, only for new ones.  
- People only looked for points of their own interest  
- Production personnel were skilled "hands-on" kind of people (doing rather than thinking).  
- The main focus was on production (get it done as fast as possible), not safety, so there would have been no consideration of safety risks resulting from an error.  
- Production seemed to have been severed from safety knowledge. The research lab knew that DCPD was a very reactive stuff and that too great a quantity could be dangerous. The company had no up to date knowledge about DCPD behavior from external sources. | The recipe also specified the name of the chemicals required in the recipe (correct). The correspondence between tank number and what was in it was wrong and the error could have been identified at this point. | Detection failure: The persons reading the recipe were experienced enough to spot the error in correspondence between the tank number and contents, but they did not. |
<table>
<thead>
<tr>
<th>Act No.</th>
<th>Time</th>
<th>EOC type</th>
<th>Normal procedure</th>
<th>Unsafe actions</th>
<th>ERROR FORCING Plant conditions</th>
<th>CONTEXT Performance shaping factors</th>
<th>Recovery potential</th>
<th>Error mechanisms</th>
</tr>
</thead>
</table>
| 3      | 02:30-03:00, 5 days later | 1 | Fill tank HP1 according to recipe. It was normal practice to go out to the tank farm with just the list of tank numbers and quantities. | Operator filled HP1 according to feedstock indicated by the tank numbers | Unseen by the operator HP1 is now filled with too much reactive chemical (DCPD). The contents are at ambient temperature. | - The recipe procedure was incorrect  
- The operator was a trainee.  
- The operator was unsupervised  
- Manning/workload pressures  
- Man-machine interface: the only measures of tank contents are temperature and pressure | The name of the material was written at the tank. If the operator had written down the name of the material as well as the tank number he would have noticed the discrepancy and could have recovered the error. A supervisor would have spotted the mistake and could have prevented the filling with the wrong mixture. Experienced personnel knew what was in the tanks. Normally the same basic materials are used in the recipes, but there are variations because feedstock vary in quality and customer requirements vary. | The trainee made a mistake which he was not capable of recognizing given the insufficient information he took to the tank farm according to the normal procedure. |
<table>
<thead>
<tr>
<th>Act No.</th>
<th>Time</th>
<th>EOC type</th>
<th>Normal procedure</th>
<th>Unsafe actions</th>
<th>ERROR FORCING Plant conditions</th>
<th>CONTEXT Performance shaping factors</th>
<th>Recovery potential</th>
<th>Error mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>03:40</td>
<td>Recovery failure of Act 3</td>
<td>Stir the mixture a bit, take a sample and label it and take to the laboratory.</td>
<td>Sample not checked before starting the process. This was a routine omission.</td>
<td>- No connection had ever been made between composition of materials in the vessel and the safety of the process. (See also Act 2). - No requirement to check the contents before starting heating - Purpose of sampling was to post check when quality spec not met, not safety - The laboratory did not work in the night - Heavy workload - The trainee was too busy to do the check himself, with the heavy workload, and anyway was probably not competent to do so.</td>
<td>- Had the sample been analyzed at this point it would have been seen that there was a wrong mixture in the vessel. - The operators could have analyzed the sample themselves, but in practice these analyses were not normally carried out.</td>
<td>Detection failure. Routine intentional omission.</td>
<td></td>
</tr>
<tr>
<td>Act No.</td>
<td>Time</td>
<td>EOC type</td>
<td>Normal procedure</td>
<td>Unsafe actions</td>
<td>ERROR FORCING Plant conditions</td>
<td>CONTEXT Performance shaping factors</td>
<td>Recovery potenti- al</td>
<td>Error mechanisms</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>03:45</td>
<td>1</td>
<td>Begin the stirrers and start the heating process using steam until 180 degC.  (Polymerization starts around here although this was only known by the operators and not by the mother company who thought it started at about 240 degC). This usually takes 3-4 hrs. The operator should check the temperature every 30 mins. When it gets to 180 degC switch to oil heating until heated to 240 degC to accelerate the reaction.</td>
<td>Operator starts the heating process and does checks without purpose (no follow up required)</td>
<td>Steam passes through the steam coils. The temperature in the vessel rises much slower than normal.</td>
<td>- The control panel indicates temperature and pressure, and also the historical trend</td>
<td>Due to other poor design factors (safety valves only designed for steam pressure, cooling system inadequate, can't remove vessel contents etc.) the runaway was probably unstoppable at this point</td>
<td>Situation assessment failure: At the beginning there was no way that the operator could recognize his mistake. However, the slow rise of the temperature in the vessel should have indicated something different from normal.</td>
</tr>
<tr>
<td>6</td>
<td>06:45-07:00</td>
<td></td>
<td>Shift change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act No.</td>
<td>Time</td>
<td>EOC type</td>
<td>Normal procedure</td>
<td>Unsafe actions</td>
<td>ERROR FORCING Plant conditions</td>
<td>CONTEXT Performance shaping factors</td>
<td>Recovery potential</td>
<td>Error mechanisms</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Between shift change and 09:00</td>
<td>3?</td>
<td>Normally the oil heating is only done last (for economic reasons)</td>
<td>Also started the oil heating</td>
<td>- By now the process has been going on for about 5 hours without it reaching 180degC. [Unseen: resin covers the steam coils preventing heat transfer.]</td>
<td>- The operators are focused on the height of the temperature because this is what controls the reaction. - Operators are taught to do not ask -This operator did not have long experience</td>
<td></td>
<td>Situation assessment failure: There is still no knowledge that the wrong mixture is in the vessel, or even any concern that something could be wrong</td>
</tr>
<tr>
<td>8</td>
<td>around 09:00</td>
<td></td>
<td>Close valve for steam and open valve to test the cooling system. Normally the temperature would go down 2 or 3 degrees. It didn't</td>
<td></td>
<td>- The temperature doesn't respond to cooling</td>
<td>[Resin covers the steam coils preventing heat transfer. Due to poor design, the steam coils are also used for cooling. Therefore, the cooling test fails because in reality no heat transfer is taking place]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Act No.</td>
<td>Time</td>
<td>EOC type</td>
<td>Normal procedure</td>
<td>Unsafe actions</td>
<td>ERROR FORCING Plant conditions</td>
<td>CONTEXT Performance shaping factors</td>
<td>Recovery potential</td>
<td>Error mechanisms</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>09:20</td>
<td></td>
<td>Use the fire pumps if the cooling water pressure is not high enough. Routine violation (safety system now unavailable).</td>
<td>Extra cooling is applied using the fire pumps, thereby resulting in unavailability of the firewater system. This was a routine action. In fact, this has no consequence for the actual accident scenario even though we recognize it here as an unsafe act. When the fire pumps failed to achieve cooling they tested the temperature of the water going in and out and found it was the same. Time was wasted: people could have been evacuated (Error of omission).</td>
<td>- Temperature and pressure continue to rise.</td>
<td>- the cooling water pressure is sometimes not high enough to achieve cooling anyway - using fire pumps had become a routine substitute - no formal procedure for what to do if there was a cooling test failure (normally the fire pumps worked) - man-machine interface (in and out temperature from heating/cooling coil not measured/displayed)</td>
<td>None</td>
<td>Situation assessment failure (mismatch): Since the cooling water pressure sometimes wasn't high enough (and it had become a regular practice to connect up to the fire pumps) they thought on the day that it was a water pressure problem. Still do not know they have a wrong mixture.</td>
</tr>
<tr>
<td>Act No.</td>
<td>Time</td>
<td>EOC type</td>
<td>Normal procedure</td>
<td>Unsafe actions</td>
<td>ERROR FORCING</td>
<td>CONTEXT</td>
<td>Recovery potential</td>
<td>Error mechanisms</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>----------</td>
<td>------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>---------</td>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td>Tried to relieve pressure by opening interlocked valve in the vapor line.</td>
<td>- Opened vapor line valve just closes again [because interlocked]</td>
<td>- No other way to relieve pressure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Time was wasted: people could have been evacuated (Error of omission).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>09:45</td>
<td></td>
<td>Fire alarm sounded.</td>
<td>&quot;Silent&quot; fire alarm (only fire brigade warned) which was routine procedure for solving cooling problems. -Company fire brigade spray tank and area with water to deal with hot resin which they expected to be released from the safety valves when they opened (not for the purposes of cooling, since this would have been pointless as the vessel was insulated). The error is that they were present in the area, making the impact of the accident, when it happens, worse.</td>
<td>- Plant behavior not understood - Lack of knowledge of consequences of the high temperature/pressure -No plans exist for this situation</td>
<td></td>
<td>Failure in response planning. Rather than mitigating the effects by evacuation, the presence of people round the vessel and the failure to evacuate the site is putting people at risk</td>
<td></td>
</tr>
<tr>
<td>Act No.</td>
<td>Time</td>
<td>EOC type</td>
<td>Normal procedure</td>
<td>Unsafe actions</td>
<td>ERROR FORCING Plant conditions</td>
<td>CONTEXT Performance shaping factors</td>
<td>Recovery potential</td>
<td>Error mechanisms</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>----------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>12</td>
<td>approx. 09:45</td>
<td>Lab carries out the sample test!</td>
<td>Error of omission. This should have been done earlier.</td>
<td>- the mixture is found to be incorrect (double amount of DCPD)</td>
<td>- The analyst in the lab knows that DCPD is very reactive stuff but consequences unknown or detailed analysis is needed to be precise. (But time runs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 13     | 09:55    |          |                  | People standing around vessel. Man exiting lab (unaware of what is happening) gets caught in the fire blast. 3 deaths, 11 hospitalized. | - Equipment starts to fly off the vessel.  
- The 2 safety valves open.  
[They've only been designed for a pressure of 10bar (for the steam) and have a very small diameter].  
- Escaping vapor ignites and the burning cloud spreads rapidly across the site (flash fire?)  
- The vessel BLEVEs and is launched around 200m.  
- Most of site affected/destroyed (not the tank farm). Heavy parts up to 1km away | - As for 11, and  
- No time to escape  
- Many people standing around without protective clothing  
- No one has been evacuated  
- Some personnel did not even know there was a problem | - Personnel could have been evacuated. | Failure in response planning. Rather than mitigating the effects by evacuation, the presence of people round the vessel and the failure to evacuate the site resulted in 3 deaths and 11 |
Predictive Analysis
The description of the process

Production process
At the site two techniques are applied:
• heat polymerization;
• catalytic polymerization.

In the following special attention is paid to the heat polymerization.

General description
In the heat polymerization process different raw materials (resin oils) are transferred to a reactor.

After mixing the temperature is raised and polymerization takes place.
The raw materials are unsaturated hydrocarbons, that combine to long chain products during the polymerization. The reaction is exothermic. The extra heat from the reaction is withdrawn by cooling of the process.

The total process can be divided in:

• filling of the reactor 2 hours
• heating 5 hours
• polymerization 10 hours
• depressurizing 1 hour
• emptying reactor 2 hours

(N.B.: this information is derived from the process some years after the accident so it is not sure that the same applies to the situation at the time of the accident).

In total there are about 60 different types of resins. This number is a total number, including standard recipes and 'tailor-made' recipes. The tailor-made recipes are derived from the standard recipes through adjustment of the substances and/or quantities.

The reactor was a pressure vessel made of steel with the following dimensions/specifications:

• diameter 2.75 m
• length 9.20 m
• wall thickness 21mm
• design pressure 20bar
• design temperature 300°C

The reactor had two mixers, driven by electro-engines.
Two safety relief valves were present on top of the vessel. To prevent blockage of the valves a bursting disc was present (diameter 2 inch).
To relieve vapor from the light oil fractions a vapor line was present on the reactor.

Control of the polymerization process
The whole process is controlled from the control room. The process is controlled on basis of the temperature in the reactor. Both temperature and pressure are recorded on (writing) measuring devices.
Heating and cooling of the process
The reactor is equipped with two coils.

One coil is connected to an installation that delivers (thermal) oil at about 240°C. The other coil has two functions:

• heating with superheated steam up to 180°C;
• cooling with water (from the river).

The raw materials are stored in a (one or more?) tank farm on the west side of the site. The tanks are identified through a number between 600 and 700 (600-series).

Question: is each tank a dedicated tank?

The process sequence
In this section we describe the whole process by defining the different steps/actions, that are necessary for producing a certain batch.

Step 1  The Recipe
The recipe for a batch is drawn up by the head of the laboratory (Question: what is the information, where the recipe is based upon?) The recipe is drawn up by typing the following information: substance name, tank number, the percentage of resin forming substance, density of the substance volume percentage and quantity of the different substances (in dm³/litres).

Step 2  Distribution of the Recipe
A copy of the recipe is distributed to Head of Production, Process Engineer, Company Administration and Manager Manufacturing.

(Question: who is responsible for the distribution?).

Step 3  Instruction of the Operator for Filling the Reactor
The Head of Production transfers information to an operator for filling the reactor. Based on that information the operator goes to the tank farm.

(Question: how is the information transferred to the operator?).

Step 4  Filling of the Reactor
The operator selects the tanks in the tank farm with the proper substances, probably using the recipe. He opens valves from the tanks and valves in the distribution pit. He gives the quantity for each substance and starts the transfer pump.

(Questions:
• what does the operator do, when he actually gives the quantity?
• how many pumps are available?
• is there a check on the pumping and the quantity?
• how many valves must be opened and how can the operator see/check, whether he opens the right valve?
• what is the actual sequence of his actions?).

Step 5  Mixing of the Reactor Content
After filing the reactor the mixers come into operation to produce a homogeneous mixture. After some time the mixing is stopped.

(Questions:
• is someone checking the liquid level in the reactor after filling?
• if so, who is responsible and how is it done?
• who starts and stops the mixing process?
• how much time is needed for mixing?).

Step 6  Sampling
An operator takes a sample of the reactor content, identifies the sample and brings it to the laboratory. In the laboratory the sample is placed in an acid chamber.

(Questions:
• how does the operator know when to take a sample?
• how does he know which reactor must be sampled?
• how is the sample identified?
• is there one unique place where the sample is delivered?).

Step 7  Starting the mixers and the heating process
After sampling the operator starts the mixers and the steam heating.

(Question:
• how is steam heating started?).

Step 8  Additional Heating with Thermal Oil
At a temperature of about 100°C heating is fastened by activating the thermal oil system.

(Question: how does the operator activate that system?).

Step 9  Precooling of the Reactor
Polymerization starts at about 180°C.
At 200°C heating is stopped. After that cooling water is supplied to the reactor.

(Questions:
• how does the operator stop the heating process?
• how does he start the supply of cooling water?).

Step 10 Stopping of the Precooling
If the process temperature drops on the recorders in the control room pre-cooling is stopped.

(Question: how does the operator stop the pre-cooling?).

Step 11 Cooling of the Reaction at 245°C
After the stopping of the pre-cooling, the temperature will rise because of the exothermic reaction.
At about 245°C cooling is started again and the process control system maintains the temperature at 245°C.

(Questions:
• how does the operator start the cooling again?
• is it necessary to activate the process control system?
• how does the control system control the process temperature?).
Step 12 etc.
After 2 hours of reaction the process is out of the dangerous zone, because most of the raw materials have reacted. The amount of heat that can be generated after that period is limited.

For the purpose of the analysis this part of the polymerization process is not taken into consideration.

Identification and analyses of the candidate EOC's from the process description

Based on the process description, it has been attempted in this analysis to identify the candidate EOCs and to analyze these in terms of types of unsafe actions (UA) and error forcing context (EFC).

It is important to emphasize that this analysis has been made without knowledge of the accident.

The objectives of this analysis are:

- to see whether the ATHEANA method can be applied as a predictive safety analysis or not;
- to see what level of detail can be obtained depending on the process information;
- to verify whether the identified HFE's (Human Failure Event) also could have been found with other identification methods used with QRA's or not.

For the analysis the process has been broken down into a sequence of steps.
For each step an inventory of possible EFCs and UAs has been made by analyzing the basic function and outcome of each step.

The basic idea is that at each step one or more combinations of different UA's and EFCs might occur (see Figure 4), leading to an EOC.

Figure 4 Concept used to analyze EOC's for each process step

```
   EOC
  /   \
/     \ 
UA_1   UA_2 EFC_2 EFC_3
```

Step 1: The recipe
Function: definition of process input data for operators
Outcome: a recipe document to be used by the operators
Status of outcome: good recipe:
- wrong recipe: EOC may lead to EFC later on;
- not clear recipe: may lead to EFC later on.

The underlying conditions (EFCs) for a wrong recipe could be:
EFC_1: many almost identical recipes;
EFC_2: a completely new recipe or concept or raw material;
EFC_3: wrong basic data.
The unsafe actions could be:
UA_1 - the switching of known numbers/data of similar recipes.
UA_2 - the extrapolation of figures to new recipes or raw materials;
UA_3 - applying not verified information on own judgment.
The underlying conditions (EFCs) for a not clear recipe could be:
EFC_1 - bad standard document lay out;
EFC_2 - bad editing by the author;
EFC_3 - too few information/missing information.
The unsafe actions later on could be:
UA_4 - own interpretation of operator based on his judgment.

Step 2 Distribution of the recipe
Function : control of documents
Outcome : availability of controlled documents
Status of outcome  : only controlled documents are available;
                   - wrong or not clear recipe is used because controlled documents are not revised in time;
                   - wrong or not clear recipe is used because old documents are still in use at the same time.

The underlying conditions (EFCs) for use of old documents could be:
EFC_1 - no link between process changes and implementations in documents;
EFC_2 - no active and controlled distribution of documents.
The unsafe actions could be:
UA_1 - production makes its own 'revision' based on info of process changes;
UA_2 - production uses its own set of copies of recipe documents.

Step 3 Instruction to the operator for filling the reactor
Function : input information for line up next batch
Outcome : clear and complete instruction
Status of outcome  : clear and complete instruction;
                   - wrong instruction;
                   - not clear instruction.

The EFCs and UA's are similar as for 'wrong recipe' and 'not clear recipe' in step 1.

Step 4 Filling of the reactor
Function : filling operation
Outcome : a properly filled reactor
Status of outcome  : reactor properly filled;
                   - reactor not properly filled.

The underlying EFCs for reactor not properly filled could be:
EFC_1 - lay out of the plant (no logical routing);
EFC_2 - many similar tanks, pipes and valves;
EFC_3 - temporal changes tanks, pipes;
EFC_4 - wrong, not clear recipe (see steps 1 and 2);
EFC_5 - wrong, not clear instruction (see step 3).

Unsafe actions could be:
UA_{13} - operator uses his 'optimal' routing;
UA_{13} - mixing of tanks, pipes or valves by own 'logic' judgment;
UA_{43} - operator uses his own interpretation.

Step 5 Mixing of reactor content
Function : create proper/safe starting conditions for batch
Outcome : well-mixed content
Status of outcome : - content is well mixed;
• content is not sufficiently mixed;
• content is not mixed at all.

The underlying EFCs for bad mixing:
EFC_{1} - no well-defined instruction for mixing;
EFC_{2} - no well-defined check on mixing process being performed;
EFC_{3} - no (instrumental) control on mixing performance.

Unsafe actions could be:
UA_{1} - operator uses his own judgment based on general recipe;
UA_{13} - operator thinks that mixing is properly performed.

Step 6 Sampling
Function : to verify the (important) properties of the mixture
Outcome : mixture properties
Status of outcome : - well-performed sampling;
• bad sampling, wrong conclusion;
• no sampling at all.

The underlying EFCs for wrong conclusion:
EFC_{1} - sample not correctly taken;
EFC_{2} - wrong test criteria being used;
• wrong interpretation of results.

The unsafe actions are:
UA_{12} - mixture considered to be OK, where it is not;
UA_{12} - additions to mixture, where it should not have been done.

The final result of HFE's including EOCs in steps 1 to 6 could be a wrong (off-spec) mixture in the reactor without the operator knowing it (see figure 5).

Steps 7 to 12 Batch process control
The steps 7 to 12 concern the batch process control by means of heating and cooling. These steps are grouped into one batch process control step.
Function : control of temperature conditions during process
Outcome : the required temperature curve
Status of outcome : - controlled thermal behavior;
• not sufficiently controlled thermal behavior

The underlying EFCs for not sufficiently controlled thermal behavior could be:
EFC_{1} - cooling/heating capacity not available;
EFC_{2} - heating/cooling capacity deviates from expected capacity;
EFC₁ - temperature curve deviates from expected curve (off spec mixture);
EFC₄ - little response time for operator/no correction time

The unsafe actions are:
UA₁ - process starts without system check;
UA₂ - misinterpretation with respect to process progress, adjustment on own experience;
UA₃ - omission (not applicable)

It should be clear that the process can only be controlled completely if the maximum thermal conditions (T and dT/dt) are within the design limits of the system.

This means that the dynamic response of the control system should be fast enough at all circumstances. In order to meet this criterion one should:

- be able to identify and to define the most critical condition;
- activate a (back-up) system before the critical conditions occur at all times to control the process behavior.

Summary
The results are summarized in a logic diagram suitable for incorporating into the risk model, as shown in Figure 5.

Note: The wrong reactor content could be a variety of possibilities, some leading to extreme off-spec process condition, others not. That is a quantification problem which is not dealt with here.
Q3 - Findings From the Analyses

Q.3a - Findings Regarding the ATHEANA Method

Overview of Strengths and Weaknesses
An overview of the key strengths and weaknesses of ATHEANA (pre-\(^\text{a1}\)) are given below, based on primarily\(^{a1,a2,a3}\):

(-) Poorly defined terms
(-) The method is not (currently) a toolbox
(+ ) Could be made into a toolbox
(+) Good 'central' concepts: Error Forcing Context (Plant conditions and PSFs), Error mechanisms
(-) Poor support for understanding and using the central concepts in applied context
(-) Poor prioritization system (for homing in on the most important areas/highest risks)
(+) New 'mindset' focussed on error forcing context, particularly attention on plant conditions
(-) Too complicated for risk assessment analysts who are inexperienced in its use
(-) Too vague for experienced HRA analysts
(-) Requires extensive technical knowledge of the behaviour of the technical system to be able to consider plant conditions in the Error Forcing Context.
(+) Good basis for discussion with management

Basis For the Evaluation
The following points are based on examination of documentation\(^{a4,a5,a6}\) and pre-\(^{a7}\):

(-) Poorly defined terms
This is true not just of ATHEANA but also the whole area of EOCs in general. We had to come up with some tighter definitions for EOC, including dropping the words 'overt unsafe', for identifying what is of interest for a risk model, and for identifying the key attributes of EOCs which are important in the definition. It is noted that similar criticisms have been made by Dougherty \(^{a8}\).


Terms used in ATHEANA: Human Failure Events, Unsafe Acts, Error Forcing Context, Performance Shaping Factors, Plant Conditions, Error Mechanisms... are all very poorly defined in the sense of giving support to the analyst. The result is that the analyst does not know how to properly apply the concepts for the steps in the ATHEANA procedure.

(-) The method is not (currently) a toolbox [NOTE: This comment was based on§]
A tool is something which is supposed to make getting a job done easier. ATHEANA is currently a set of concepts and a vague procedure for how to apply them. There are no tools. This means that the success or otherwise of using ATHEANA is subject to enormous variability, more dependent on the user than the method. This makes a benchmark study impossible at this stage.

(+) The method could be made into a toolbox
There is no reason why the procedural steps of ATHEANA could not be supported by tools, and the central concepts developed as checklists, for example. These should give a tight structure to using ATHEANA such that the results are produced in a systematic way. A tool might be a checklist, for example, flow sheets, or a clear recipe for carrying out a particular step (necessary ingredients and what you do with them). In addition, it may be necessary to develop new representations to work on - just as HAZOP uses P&ID’s of the plant, what should ATHEANA work on? We discussed the possibility of using the error mechanism as the central focus of ATHEANA, and some sort of ‘P&ID’ of the human, in order to systematically generate relevant EOCs rather than being reliant solely on what the analyst can dream up. (Note: Although it contains more detail than§, it is still not easy to follow).

(+ Good ‘central’ concepts: Error Forcing Context (Plant conditions and PSFs), Error mechanisms
The overall concepts of ATHEANA are good ones, since they cover more of the important aspects in accident causation than previously by bringing together the whole human-technical system and their interactions under the eye of the analyst. Particularly important in this respect is Error Forcing Context which analysts have previously not considered. Retrospective accident analysis which we carried out using data collection fields stimulated by the method gave a new perspective to examining the causes of the accident and gave rise to questions not previously considered, (although it wasn’t very good at homing in on the important management factors which were the underlying cause of the accident). The EFC aspects and error mechanism analyses were particularly valuable in enhancing the data collection and analysis. The fields used included:

EOC Type: If the action was an error of commission, this was categorized according to the definitions developed in Report 1§ for different EOC types.

Normal procedure: This described what the normal procedural step at the plant was.
Unsafe actions: Unsafe actions carried out, where unsafe action was considered to mean an action which did or could have resulted in a degraded plant state.

---


Error forcing context: This was divided into Plant Conditions and Performance Shaping Factors which together comprise the EFC.

Recovery Potential: Since Error Of Commission is a process (a failure not recovered) it was considered that the potential for recovery needed to be described. This was not made explicit in ATHEANA as something to look for.

Error mechanisms: These were considered to be the unobservable psychological mechanisms which mediate between the Error Forcing Contexts and the Unsafe Acts

(-) Poor support for understanding and using the central concepts in applied context (Note: This is based on review of 

When we tested the method in an applied context, using risk analysts, they used the method according to their own interpretation of it, and not always as ATHEANA intended. This does not mean that there was not a successful outcome, but that the method will show extensive variability across analysts and will depend more on the analysts’ abilities than the method. ATHEANA did give some structure to the results, particularly since unsafe acts and error forcing contexts were being identified, but how to fit it all into the big picture (risk model) was unclear and there were no stopping rules.

There was no guidance on how to formulate the Human Failure Events in the fault/event trees, or how to select relevant ones. EFCs identified by the analysts tended to focus more on PSFs than plant conditions since these were easier to think of. The analysts had to write up their own procedure beforehand, some of it based on very brief and buried descriptions of what to do in the ATHEANA documents. In conclusion, the thinking process of the analyst who must dream up the EOC scenarios was very poorly supported indeed.

(-) Poor prioritization system (for homing in on the most important areas/highest risks)
The application of ATHEANA to even just a small part of an installation could be a lifetime’s work, dreaming up all the possibilities of EFCs and unsafe acts. Since the idea should be to cover all the major risks (risk assessment should be ‘total’ in this sense), it is no good having a technique which cannot home in on the important areas of the plant, procedures and risk model on the one hand, and ensure complete coverage on the other. There has to be a prioritization system that allows effort to be allocated in an appropriate way. Also, since the analyst can go on dreaming up EOC scenarios forever, there have to be stopping rules. The important thing about EOCs is that there can be scenarios not previously thought about in the risk model which could significantly affect the risk. How do we know where to look for them and which ones are the most important? There needs to be homing-in support.

(+) New ‘mindset’ focussed on error forcing context, particularly attention on plant conditions
Previous HRA techniques have tended to be overly human-centred, ignoring the whole socio-technical system. Technical aspects of chemical plants (such as whether they are batch or continuous process, for example), significantly affect the task of the human operator in safe control. Not only this, but the technical aspects also influence the way a plant is organized. Organizational factors, including aspects such as whether a plant is old or new, big or small, affect human tasks and have different strengths and

---

226

weaknesses. This is described in detail in a study undertaken in the context of the Dutch chemical industry. ATHENA is rather weak on the organizational and management aspects, but the EFC could be extended to include that, and would be much enhanced.

(-) Too complicated for risk assessment analysts who are inexperienced in its use and too vague for experienced HRA analysts (Note: This comment based on assessment of a)

For a risk assessment analyst, the ATHENA method description is not easily accessible, and seems overly complicated. On the other hand, it is too vague for the experienced human factors analyst who wants to know more detail and be more constrained than having to use his/her own knowledge to back up the analytic process.

(-) Requires extensive technical knowledge of the behaviour of the technical system to be able to consider plant conditions in the Error Forcing Context

In the chemical accident we analysed, one of the reasons for the EOCs was the lack of knowledge at the time of how certain chemical mixtures behaved. A wrong mix led to previously unknown effects. In the chemical context at least, the knowledge of plant and process behaviour will have to be very good to be able to really come up with the plant and process behaviour which an operator could be faced with. The ATHENA method clearly requires a team of people (as is said in the ATHENA documentation) but how easy will this be to achieve (in fact, a real test of the method in this respect has yet to be carried out)? The method needs to specify the requirements/expertise for team members in carrying out the different steps in the process.

(+ ) Good basis for discussion with management

Currently there are no techniques which provide a good basis for evaluating human error risks with involvement of the (chemical) company. ATHENA could fill this gap. However, unlike with HAZOP, it lacks a system for formal follow-up (by the company) of identified risks.

**Findings Regarding Errors Of Commission**

Details of errors and error forcing contexts are provided in Section 2.1. One cannot really describe an accident in detail without putting some interpretation on what happened. In the retrospective analysis of the accident (section 2.1) we were able to apply two of our 6 EOC type definitions, showing this accident to be the result of an unrecovered EOC type 6 (information error) which led to an EOC type 1 (initiator). The link between the errors themselves and the recovery failure should be apparent. The EOCs are not independent and EOCs and the recovery failure are not independent because the very fact of not knowing an error has been made sets up the potential for the wrong mental model for interpreting the plant conditions.

We found ourselves in disagreement about the distinction between the recovery failure of an EOC which would be part of the EOC process, and classifying a recovery failure as an error of omission. This emphasises the need for tight definitions but does not really add much to the analysis.

---


The first error which occurred in our accident analysis could have been a random slip or it could have been a mistake. We assume it is probably a slip, but we do not actually know.

What was important was that the Error Forcing Context that this simple error triggered had everything to do with Design and with Management. The psychological mechanisms, once the wrong mix in the vessel generated unusual process behaviour are hardly of interest since virtually no one knew about the behaviour of such a mix of chemical (let alone an inexperienced operator who was just trying to meet the demands of the production procedures).

The performance shaping factors surrounding a slip could be endless. Maybe, as one of the accident investigators said, the person in the lab got a phone call when he was typing the recipe which momentarily distracted him. Similarly, the operator may have been given recipe that had been carried around in someone overalls and one of the numbers had been rendered difficult to read by some dirt. We do not want to address the problem at that level.

Indeed, having recognized (now) that wrong mixtures can cause runaways which can destroy an entire installation, it is the increase in the recovery potential at the earliest possible stage that has become important, and hence the introduction of the step to sample the mixture before starting up the reaction. Having introduced such a step, though, the interest is now more on the EOCs associated with sampling and analysis of the mixture. Previously, sampling was just a routine omission. In that respect it is the technical procedure which makes the error, not the psychological mechanism.

Q.4 - Definitions Of Terms and Parameters Used

The following are definitions of terms we used in this study.

Error Of Commission (EOC):

An action that leads to a change in plant configuration, with the consequence of a degraded plant state and:

An error of recognition, diagnosis or intention, that leads to a series of acts formed with well-meaning intentions, but which are inappropriate for the technical scenarios that pertains, or an isolated error introduced with an otherwise appropriate series of actions that may arise from a random aberration in behavior, or may be induced by the inappropriate application of an habitual task behavior.

Error Forcing Context (EFC):

The combined effect of performance shaping factors and plant conditions that trigger psychological error mechanisms, and which must address not only the initial error but also the failure to recover it.

Intentional EOC

EOC (as defined) where the action was intended.

Unintentional EOC

EOC (as defined) where the action was not intended.
A Conditioned Probabilities:

Probabilities of failure of a (chemical plant) design, as used in QRA, which are also conditional upon the chance of EOCs and which are therefore greater than would be expected from failure of the design alone.

EOCs which Condition the Probabilities used in Chemical QRA:

EOC.1 = A human action which is an initiator. It directly causes a dynamic change which initiates the accident sequence.
EOC.2 = A human action which defeats a safety system during the post-initiator sequence
EOC.3 = A human action in the post-initiator sequence which makes the situation worse (e.g. accelerates the dynamic change).
EOC.4 = A human action which defeats a safety system at some time before it is needed (before the initiating event)
EOC.5 = A human action which defeats the information system at the same time as it is needed (such as switching off an alarm during the post-initiator period)
EOC.6 = A human action which defeats the information system before it is used (such as making errors in a written procedure, wrongly calibrating an instrument).

Initiating event B chemical industry
The event leading to Loss Of Containment.

Loss Of Containment (LOC) B chemical industry
In the chemical industry context, this is the release of material from the containment. It is the central point in the, between the fault and event tree. Hence it is the top event of the fault tree and the beginning of the event tree.

Performance Shaping Factor (PSF):
Any factor which influences human performance in the interaction between the human and the system upon which they are acting.

ATHEANA PSFs are identified as:
Procedures
Training
Communications
Supervision
Staffing
Human-System Interaction
Organizational Factors
Stress
Environmental conditions

Unsafe Action
Actions inappropriately taken or not taken when needed that result in a degraded plant safety condition 56.

Human Failure Events (HFEs)
HFEs are the events in the risk model at the function, system or component level.

p(HFE_p) = p(EFC_p)p(UA|EFC_p)p(not.R|EFC_i,UA,E_p)

The probability of a Human Failure Event (HFE_p) equals the combined probability of the error forcing context (EFC_p) occurring and the probability of the unsafe action UA, from which the HFE results being carried out, given (EFC_p), and the probability of it not being recovered (not.R) given the occurrence of the EFC, the UA, and the existence of additional evidence (E_p) following the UA.

Line Of Defense (LOD)
A defense against some component of the system which prevents (ultimately) loss of containment. Lines of defense may be physical (like the containment itself and the engineering standards to which it is built), systems of work or rules of behavior (like procedures, speed limits), organizational (like having a supervisor check the work of contractors), cultural (like whether the culture allows production to stop for safety reasons), man-machine interface (like quality of labeling) etc. For any one failure case, there is usually a complete Lines Of Defense system which has failed, in many cases because the otherwise independent defenses are coupled by a poor management system. The Line Of Defense concept underlies the AVRIM2 methodology used by the Dutch labor inspectorate. \(^{37}\) \(^{38}\)

When we got together with the other group who were looking at nuclear accidents, we were immediately at odds over the EOC definition. It seemed that the other group did not acknowledge the existence of error in the first place when it was induced by an external context. We had to content ourselves with talking round something which in the end we agreed to call:

An unrequired action which could be induced by an Error Forcing Context (and usually is) an error forcing context implies that, if the context exists, the chance of an unsafe act is virtually 1. It was argued by the nuclear group that one can hardly call error an action which is due to context and not due to a failure in the psychological mechanism. That we should be making a distinction between something called error and something called an unwanted.

However, our group had been looking at error from the perspective of predicting and preventing unwanted events in a technical system resulting from certain kind of human actions. We saw it as virtually impossible to predict EOCs (our definition) related to, for example, unidentified chemical behaviour. The ATHEANA method was not going to help there. We saw scenarios as being better predicted from an examination of:

- Contexts (plant conditions) outside the design window, whether it was believed possible or not (such as temperature extremes thought impossible) Y. In this sense automated systems which perform the same functions as humans can also make errors
- Defining the task steps of the process, and then defining the Lines Of Defence (LODs) which keep that step within the acceptable design.
- Link EOC to the defeat/circumvent/deplete/etc. of the Line Of Defence (this is the real Human Error bit where we look for the unsafe acts). The 6 EOC types can be used here.
- Link LOD=s to the management system.


One of the critical weaknesses of ATHEANA is the difficulty it has in dealing with prioritizing what needs to be covered in the QRA. One of its great strengths is that it provides a basis for a convincing discussion with management about the possibilities and consequences of human failure.

Certainly, in the Netherlands, the regulator is severely lacking in tools which address the human error aspects of chemical manufacturing safety. Whereas ATHEANA was intended to be a quantification method, it is actually better functioning as a method to bring management and operators and risk analysts together to discuss the human error problem. What it lacks is formal the follow-up mechanisms one finds in conventional HAZOP for example. This is a management commitment problem which the ATHEANA method could be developed to overcome.

In this respect we view ATHEANA in a positive way, that it could fill a gap currently lacking a human error tool. The Steering Group of the project considered that the analysis of a chemical installation could be approached as follows:

<table>
<thead>
<tr>
<th>Process part:</th>
<th>Process Safety Analysis, Hazop, QRA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Part:</td>
<td>Audit</td>
</tr>
<tr>
<td>Human interactions:</td>
<td>ATHEANA</td>
</tr>
</tbody>
</table>

Comments on the ATHEANA procedure

Finally, we make some detailed points according to the ATHEANA application steps given in NUREG-1624**, Section 7.

Step 1: Scoping

ATHEANA focuses explicitly on post-initiator human failure events (HFEs) whilst it is clear from the accident analysis that the main (and perhaps only) value of the method in chemical applications is for pre-initiator analysis. The dynamics of chemical failures make post-initiator intervention of limited value.

Later in the method (step 4) it is made clear that it should be applied to HFEs lying behind both the initiator itself as well as the actions and hardware responses in the event tree responding to the initiator. It therefore becomes crucial to define what is considered to be the initiator. If we define a wrong mixture in tank or even wrong recipe as an initiator, then all of what we have done in the analysis falls within the scope as defined in *8. This would, however, be a major expansion in scope.

In nuclear applications there is therefore a well defined event tree, which defines what should happen to keep the plant within the safe, given an initiator. This anchors the start of the EOC identification process quite securely, since generically EOCs can be defined as the operator defeats/circumvents/turms off/depletes/etc. step or system element X which has a necessary place in this sequence. ATHEANA then defines generic deviations from the event tree path and links them to generic types of EOC.

---


For use in the chemical industry we need to have another representation of the process in which we can anchor the errors. We have sought this in a task step representation linked to the process procedures. This seems to work well in the predictive accident analysis and links with the idea, which is also present in ATHEANA, that a HAZOP-like analysis may help in identifying failures and errors. Tabular task analyses lend themselves to this approach, since the task process can be seen as a flow which can deviate for a finite number of reasons, which can be captured with guide words. The description which follows belongs logically by steps 4 et seq from the ATHEANA method (see below), but the overall approach cannot be understood without summarising here the representation proposed, since it strongly influences all the subsequent steps.

We do not arrive at an equivalent to the ATHEANA anchoring of EOCs just by substituting a task flow for an event tree. We have to develop the equivalent of the generic deviations and EOCs. A possible approach would be to define per step of the task flow explicitly what are the lines of defence (LOD) which keep that step within the acceptable. Then we can link the EOC to the defeat/circumvent/deplete/etc. of the LOD. Conceptually this is very like defining fault trees per step, with as top event the failure of the process or task step. For quantification purposes this may indeed be a preferred representation, but it is felt that it would be a poor way of deriving the HFEs, since fault tree representation tends to make users think only in terms of EOOs.

This approach was not carried out explicitly in the predictive accident analysis reported in section 2 of this project. There, the task or process steps have been defined, but this was followed by a direct listing of possible errors in the step itself. This means that some of the errors defined are actually EOOs (e.g. not do sampling, not mix at all). We are concerned to generate the EOCs as well. It is clear from studying the analysis that an implicit step was probably thinking about the Lines Of Defence. However making the LOD explicit is likely to provide a more transparent way of working. Some examples of LODs are given under step 6 below to clarify the definition. The lines of defence are, in many senses, further specifications of the original process or task step, plus a specification of the critical resources and controls that are needed to carry it out. Use can therefore be made of the work carried out in the EU-project AI-Risk, (the full results which are due to be published in early 1999), That is, the generic specification of controls and resources for risk-critical actions in chemical plants. This project defined 8 generic types of control and resource and the appropriate management systems for ensuring that they were delivered to the right place at the right time for the critical actions. Such a list can be used as checklist or set of guidewords for analysis. See also step 6.

We therefore propose using this representation of procedural or task flows and LODs as an equivalent to the ATHEANA fault and event tree representation.

Scoping the study then becomes a question of deciding which steps in the task flow are the critical ones and how far back in the process to go. In this respect the same issues arise as discussed in". However it could not always be assumed that the company already has an HRA (as ATHEANA does).

---

of all ingredients and parameters with all others in order to identify ones which lead to the reaction getting into uncontrollable space-states. Such a matrix should have come up with the mixture which actually caused the problem (but the analysts may not have fully understood the potential consequences).

The question is then whether it would have been necessary to go any further in making an analysis, or whether the accident which happened would have become credible enough to be taken seriously. If it was taken seriously, then the checking routines could have been strengthened and proceduralised better, and supervised rigorously (thereby requiring a string of EOOs to occur before the EOC could lead to serious consequences).

Steps 7-14. Identify unsafe actions and causes for unsafe actions, either mistakes & circumventions (relevant rules, belief that the wrong rule/unsafe action is the right thing to do, persistence in that belief) or slips & lapses (recoverability, likelihood to lead to mistake, causes, EFCs).

The critical aspect here, in looking for reasons for EOCs is to get over the initial prejudice of analysts that a certain sort of EOC is too unlikely to be credible, and hence is rapidly dismissed, or hardly even entertained as possibility. (e.g., it is not credible that someone would turn off the cooling during a reaction: everyone knows that it is always absolutely necessary for the first two).

In a generic sense the question is always the same for each step and for its LODs and is: what could have led the person to think that the action they chose was the right one? (or what led them not to question that a previous step had set them on the wrong path?)

These steps are very much the same for a chemical application as for a nuclear ATHEANA and the tables and support tools proposed would be valuable here also. In particular the method now places considerable emphasis on recovery.

That seems to have been an important issue in the accident with the initial recipe mistake not being picked up in the checking routine (for reasons not clear from the data available to our analysis), nor in the drawing of the mix (novice operator with no tacit knowledge), nor in the sampling (analysis delayed until after the start of the polymerisation, perhaps because it was seen not as a safety but as a quality check, which never indicated any serious problems in any case), nor during the process (slow temperature rise not seen as signal that an unexpected reaction was taking place, or even that the heating system might be malfunctioning, which might result in just as inefficient working of the cooling once the reaction did get under way).

Particularly in an analysis in a pre-initiator phase, where there is significant time for recovery (or in a post-initiator with the same characteristics) this seems to be a vital part of the analysis, i.e. there should be explicit attention to the possible and planned recovery paths from whatever deviation can logically occur.
but does not necessarily offer an investigative or identification process for considering error. As an approach, however, it is probably best used to assist abstract understanding, coupled with reinforcement of concepts delivered by case studies of psychological error.

2.1.2 SHERPA (Systematic Human Error Reduction and Prediction Approach)
This technique was developed by Embrey (1986a). SHERPA has been evaluated by one licensee in a pilot study and found to be helpful. The particular organisation concerned has not used the method subsequently and it is thought that this is because ‘freethinking’ approaches were found to be equally successful in identifying error potential, whether that be errors of commission or otherwise. This outcome is perhaps somewhat unsurprising as the analysts involved were highly experienced human factors specialists.

Like GEMS, SHERPA offers a behavioural classification of psychological human error. It is a simpler technique than GEMS and through a series of simple questions, usually presented in flowchart form, it seeks to determine whether behaviour is likely to be skill, rule, or knowledge-based.

SHERPA offers an analytical process that moves through task analysis, behavioural classification, error identification, quantification and remedial actions. It is thought by some to be particularly useful for establishing when behaviour is likely to be cognitive. It achieves this, in effect, by filtering out other possibilities.

2.1.3 HUMECA (Human Error Mode Effects and Criticality Analysis)
This is another technique developed by Embrey (1991). A slightly earlier version of this method by the same author is called SCHEMA. The method is known to have been used within the chemical process industry on a number of occasions, but it is not known to have been used within the nuclear industry.

The method considers 22 specific error types and is similar in content to SHERPA. Error types are classified as action, checking, retrieval, transmission or selection. HUMECA places an emphasis on the linkage between the error types and the possible consequences of such errors. When compared with SHERPA, there is a greater emphasis on a screening risk reduction and remedial process. In particular, the method has considerable value because it prescribes an organisational approach to reducing error and, hence, risk. It then provides a means for evaluating the effectiveness of intervention measures.

2.1.4 IMAS (Influence Modelling and Assessment System)
This technique was developed by Embrey (1986b), and it, too, has been used within the chemical process industry, but not apparently within the nuclear sector. The technique takes a somewhat different approach from the previously described techniques. IMAS centres on the consideration of operator mental models and the mental mapping by operators of problem spaces. It seeks to identify causes of mental model limitations, such as in their scope or completeness. The method also seeks to identify causes and circumstances where there is a risk of the inappropriate application of otherwise generally appropriate mental models. The resultant understanding of errors and their cause that might arise, is then coupled to a consideration of consequences.

2.1.5 CADA (Critical Action and Decision Approach)
Gall (1989) published this approach, which was developed by himself and colleagues. The technique has been applied within a pilot study, but its use has not been pursued beyond this initial exercise. CADA is derived from Murphy diagrams and Rasmussen’s eight-stage decision model (Rasmussen, 1980). It is implemented as a set of checklists, one of which is relevant to each of the Murphy diagram nodes. The approach allows analysts to identify which elements of a task are most likely to fail, so that they can focus their analysis upon these.
An evaluation study has suggested that CADA is as successful as an expert assessor for revealing human error potential. However, although it been used to check the findings of an informal analysis, the method has not been applied by any of the UK licensees.

2.1.6 Reversed Murphy Diagram
This method is again based upon the Murphy Diagram and was devised by human factors specialists working on the Sizewell 'B' PWR project, within the UK's Central Electricity Generating Board. The concept was proposed by Williams (1988) who provides an overview of the findings of a specific application performed by Umbers and Reiersen (1988). The technique was applied as part of the process of furnishing evidence of defences against cognitive and conceptual error during the Sizewell 'B' project. It has not been used subsequently.

The technique is termed 'reversed', because it is used in anticipation of the possibility of error, rather than retrospectively after an error has arisen. All stages of the Murphy Diagram are therefore referred to in seeking to identify where error might arise.

The technique was verified by means of two analysts attempting to identify errors that arose during the Ginna event. The results of these two analysts, when pooled, identified 75% of the stages in decision making and their associated Murphy Diagrams that were considered to have failed in the actual event.

A description of this technique and its use is provided as an attachment to this document. This is given in order to provide a more detailed example of the application of a method for identifying errors of commission. It is extracted from a paper intended for publication that is currently in preparation by I.G.Umbers and E.M. Hickling.

2.17 Short MORT
This is a condensed form of the MORT (Management Oversight Risk Tree) technique which was originally devised by Johnson (1980) and subsequently shortened by Whalley.

The Short MORT simplification is based upon the notion that some of the oversights identified by the MORT technique are more likely to happen than others and are also likely to make a greater contribution towards systems failure. Thus, the set of errors considered is reduced relative to MORT. The technique has been applied at some UK offshore oil and gas installations, but has no known application in the nuclear industry. In contrast with the other techniques that have been identified, Short MORT has the unique advantage of focusing analytical attention on potential failure mechanisms in management. These differ somewhat from the mechanisms involved in, for example, process control and therefore make Short MORT potentially uniquely suited to the identification of possible sources of, and defences against, errors of commission within administrative or management systems.
Step 2. Assemble and train multidisciplinary team

In a chemical application this step is identical. The advantage of using a technique in the chemical industry which shares many of its characteristics with HAZOP is that the majority of plants will already have teams used to this approach. Training should therefore not be too difficult. The major element in it, however, would be training in the way of thinking of the psychological precursors and error forcing conditions. Also, training in thinking outside the design space, in order to generate potential operational configurations relevant to EOCs. HAZOP teams up to now concern themselves largely with technical failures and those that are within the design space.

Step 3 Collection of background information.

This step is similar to the ATHEANA step. It would also require extensive collection not only of the formal design and procedures (how things should be done) but also of information about current practices, informal rules and expectations (how things are done).

Step 4-6 Establishing priorities for examining different initiators and event trees, prioritizing plant functions/systems to define candidate HPEs, identifying candidate HPEs

The steps relating to prioritization are even more crucial for a chemical application than a nuclear one, since we have already argued that chemical application must go much further back into pre-initiator events (or define initiators as further back from damaging outcomes). Hence the chemical scope is greater.

Given our proposals (see step 1) for representing the chemical procedures and process related tasks and LODs, the process of prioritization must be based on how the analysis team sees the importance of the steps and defences for critical events (e.g., runaways).

We have proposed that the steps and LODs should be explicitly defined, and have suggested that a generic prompt list based on the I-Risk insights into risk management could be a starting point. This study proposed the following 8 factors:

availability of personnel
competence of personnel
commitment of personnel
availability of a user friendly plant/task interface
availability of correct spares and replacements in maintenance tasks
procedures/rules/plans/goals for the action/task/process step
communication and coordination of multi-person tasks
resolution of conflicts between safety and other (usually production) goals

In addition to delivery of these to the task step, it is essential that there are checking and correction loops to ensure that the step has been completed.

Applying this to a couple of steps from the accident case we arrive at the following. The list shown here is not necessarily complete, since it derives only from the research team insights, but could be set up and completed by the multidisciplinary team proposed in step 2.

Taking the step of making the recipe:

The Lines of Defence which ensure that the correct recipe is chosen or made, are, among others:
recipe is put together by a competent person who is available when needed and knows what he is doing, and/or accurate copying occurs from a reliable source which is correctly identified and the recipe (plan) is readable and available at the point it is needed (by the tanks) checking occurs to verify that no slips or mistakes have been made etc.

If we specify these in such a way, we can use the same approach as suggested in the ATHEANA method to track down potential errors: for example someone can circumvent the first LOD by deciding that they themselves are competent enough, or that competence is not needed (e.g. when the normal operator is away). The second and/or third can be defeated by using other sources (e.g., a personal copy of the original recipe kept in a dirty overall pocket and so degraded as to make it hardly readable, or not updated), or by sloppy copying. The final LOD can be left out (more an EOO than an EOC), or be done by the person making the original copy, who does not see his own mistake.

Taking the case of the Polymerisation step:
The LODs to keep the mixture out of the runaway space-state are:

The cooling
The stirring

Avoidance of concentrations/compositions of the mixture which generate very great amounts of heat beyond the capacity of the cooling & stirring

The cooling can be defeated by turning it off or failing to turn it on when needed. The stirring idem ditto. The final LOD is dependent on the earlier step of getting the right recipe mixture (see the first part of the example) or could be defeated by adding things later (e.g., during the process, if that is feasible) which will bring things into the uncontrollable space-state.

These steps are very much equivalent to the approach proposed in ATHEANA and could use the support tools defined there, though these would need to be expanded, since the consideration of pre-initiator events would broaden the type of human actions and tasks to be considered. Prioritization would need to focus primarily on the question as to whether the failure of a given step could have serious consequences. This is a question which HAZOP teams are used to answering. Given the emphasis of this method on EOCs, the team would need to be warned particularly that they should look at the issue of recoverability in assessing this (see especially step 14 which considers whether operators will persevere in their wrong action - or whether others may pick it up)

For example a simple deviation analysis (HAZOP-like) of the steps in the procedure should result in the identification of wrong recipe as a very real possibility. That would pose the problem that there are an almost infinite number of incorrect recipes which could be made.

The next question would be how to decide whether there was a subset of wrong recipes which was a) more likely to occur, b) dangerous enough to matter (leaving aside that most wrong recipes will result in poor product quality and/or waste of the raw materials).

Conceivably a behavioral analysis could assist in narrowing down a); e.g., typing errors are reasonably predictable in terms of wrong adjacent keystrokes or reversed order numbers/letters, similar sounding names can be typed by mistake, etc. However, it is unlikely that such reasoning could really narrow down the range of errors enough to be useful.

Perhaps reasoning from the chemical side could help much more here, by looking at a matrix of mixtures
2.2 Error Elicitation Methods

These methods are those which are used as a part of an analytical activity and are intended to assist analysts to 'discover' where errors might happen. Unlike the previously considered methods, which provided some form of taxonomy and/or a model, these approaches rely upon the analyst's understanding of the phenomenon of human error, but are intended to provide a means to identify external error modes.

2.2.1 Human HAZOP

Like the conventional HAZOP (Hazard and Operability Analysis), this approach relies on the use of guide-words or phrases to elicit thoughts about the effects of human actions. Whilst the approach may be informally claimed by many in the UK, it was first formally published by Whalley (1988). This technique has been used within the UK nuclear reprocessing industry on the initiative of individual assessors, but this use has not been formally documented. Conventional HAZOP is used extensively in the design and assessment of the nuclear chemical plants and it was felt by the practitioners who were interviewed, that the human HAZOP perspective is applied as an integral part of the conventional HAZOP processes even though the use of the method is neither documented nor followed rigorously.

Typical error identification phrases considered in a Human HAZOP are: too early, too late, too much, too little, etc. Thus, the orientation of the technique is more towards the possible consequences of error, with the more detailed consideration of causes and error mechanisms left to the analyst. The technique has considerable potential in assisting the analyst with a strong human factors orientation to consider as fully as possible the consequences of identified human errors.

2.2.2 PREDICT (Procedure to Review and Evaluate Dependency in Complex Technologies)

This technique is an enhanced version of the human HAZOP approach combined with the principal features of the Barrier Analysis method. It was devised by Williams and Munley (1992). Like Human HAZOP, it relies upon structured verbal reasoning, but develops the HAZOP keyword concept by testing to destruction the tacit safety-critical and safety-related assumptions that have been made by the analyst. The method is not thought to have been applied within the nuclear industry, but has been piloted within the UK oil and gas industry by its authors with some apparently beneficial results.

Three increasingly penetrating sets of phrases, such as - 'confirmed by,' 'not recalled because' and 'defeated by' - are used to test the analyst's assumptions. The technique explicitly recognises that the analyst's ability to identify errors (and this is especially true of some commission errors) is entirely dependent upon their insight and imagination. The technique is intended to identify 'bizarre' and otherwise unpredictable behaviours and circumstances that might lead to error. Unlike most techniques, which are constrained by a consideration of the factors intrinsic to the environment and the execution of a task, this approach attempts to address those factors that have sometimes been seen in real incidents and which may not be invoked by analysts in many formal analytical methods until the event has happened.

2.2.3 PHECA (Potential Human Error Causes Analysis)

PHECA is a comprehensive computer-based tool developed by Whalley (1987), which allows the analyst to consider a task step and the possibility of error in considerable detail. It elicits from the analyst an assessment of the type of mental involvement that is necessary to perform the task. This limits the action type of the task performer to a subset of the total number of action or response types available in PHECA. The analyst then chooses the appropriate action type. This, in turn, indicates the forms of human error that are possible. For each of the chosen human error types there are suggested performance shaping factors.
PHECA provides a comprehensive and complete structure from task to error. The method has no known application so far within the UK nuclear industry, it has been applied successfully within the UK chemical and offshore industry sectors.

2.3 Identification of System Affordances
These approaches to identifying human error, focus on the possibilities offered by a system for an error to occur. Two techniques have been identified that are both intended to identify system affordances.

2.3.1 COPE (Credible OPerator Errors)
This technique was devised by Holloway and Waters (1987), when working for the Safety and Reliability Directorate of the UK Atomic Energy Authority. The technique has not apparently been piloted or used.

COPE is based on the notion that, although it is not always possible to predict what error an process operator will make, it is possible to define features within the system that will cause the operator to reassess the appropriateness and success of their intervention thus far. Therefore, the method is focused upon the possibilities of cognitive error in the form of a mistaken diagnosis or plan, leading to the systematic overturning or compromising of designed lines of defence provided within the hardware.

The philosophical and modest stance of Holloway and Waters is that cognitive error is very hard to predict and, therefore, it is, to all intents and purposes, analogous to failures of hardware. They suggest that the space within which randomness can arise is described:
- by the content of the mental model of the operator
- as a functional model of the plant

By considering a functional model of the plant it becomes possible to determine where human mistakes will have unacceptable consequences. Having identified the system's vulnerabilities, it is possible to consider how the operator might err. The technique is considered to be analogous to deterministic criteria, in that it is intended to be applied to single failures of the human.

The COPE approach then goes on to liken feedback to the users about the states of systems that causes them to reconsider their position, as being functionally comparable to the mitigation of hardware failures. Thus, the method ultimately focuses upon the functional requirements for feedback that would cause task performers to trap their own mistakes.

2.3.2 TAFEI (Task Analysis for Error Identification)
TAFEI, developed by Stanton (1994) and (1996), provides an even more structured and much more detailed approach to systems affordances than COPE. The predominant use of TAFEI has been in consumer equipment assessment. It has, however, been applied with notable success to operations involved in electrical supplies by Glendon (1995). The specific tasks examined have entailed rerouting and isolating modifications.

TAFEI explicitly models the interaction between the human and machine by mapping human activity onto machine states. The method integrates three established techniques: hierarchical task analysis,
Contribution from the United Kingdom: Identification of Errors of Commission in UK Nuclear Utilities and Formal Methods

Health & Safety Executive, Nuclear Safety Directorate
United Kingdom

Report to Principal Working Group 5-A Task Group on Errors of Commission
Committee on the Safety of Nuclear Installations, OECD, Paris

March 1998
CONTENTS

1. Introduction

2. UK Methods for Identifying Errors of Commission
   2.1 Psychological Error Mechanism Description Models
      2.1.1 GEMS (Generic Error Modelling System)
      2.1.2 SHERPA (Systematic Human Error Reduction and Prediction Approach)
      2.1.3 HUMECA (Human Error Mode Effects and Criticality Analysis)
      2.1.4 IMAS (Influence Modelling and Assessment System)
      2.1.5 CADA (Critical Action and Decision Approach)
      2.1.6 Reversed Murphy Diagram
      2.1.7 Short MORT
      2.2 Error Elicitation Methods
         2.2.1 Human HAZOP
         2.2.2 PREDICT (Procedure to Review and Evaluate Dependency in Complex Technologies)
         2.2.3 PHECA (Potential Human Error Causes Analysis)
      2.3 Identification of System Affordances
         2.3.1 COPE (Credible Operator Errors)
         2.3.2 TAFEI (Task Analysis for Error Identification)
         2.3.3 EOCA (Errors of Commission Assessment)
         2.3.4 HEIST (Human Error in Systems Identification Technique)

3. Identification of Errors of Commission - Discussion

4. Conclusions

5. References

Glossary of Acronyms and Abbreviations

1. Introduction

This document describes some of the approaches that are currently used for the identification of errors of commission amongst nuclear licensees in the UK. It also describes those methods which have been developed within the UK that have the potential to be used for the identification of errors of commission.

For the purposes of this document, an error of commission is defined as being either:

An error of recognition, diagnosis or intention, that leads to a series of acts formed with well-meaning intentions, but which are inappropriate for the technical scenario that pertains.

Or,

An isolated error introduced within an otherwise appropriate series of actions that may arise from a random aberration in behaviour, or may be induced by the inappropriate application of an habitual task behaviour.

In the UK, as elsewhere, it is generally customary to exclude explicit consideration of errors of commission from consideration within PSAs. By way of contrast, however, the human factors assessments that are undertaken in support of PSAs do not deliberately exclude the identification or further consideration of errors of commission. This is achieved because there is a long UK tradition of involving human factors specialists in human reliability assessments (HRA) within the probabilistic safety assessment (PSA) process. Many of these specialists have a degree or further degree qualification in psychology or ergonomics. Also, as can be seen in the methodological descriptions that follow, there is a consistent history in the development of methods for addressing the issue of human error in general. This has both an academic basis, particularly at the Universities of Manchester and Birmingham, and a practitioner basis as derived from the industry and its consultants, where there has been a steady stream of methodological developments in practical methods for the identification and quantification of human error.

These circumstances are probably driven and influenced by several principal factors. First, the human factors community within the UK is a relatively small but coherent professional group who tend to be members of the British Psychological Society, the Safety and Reliability Society, or the Ergonomics Society. Many practitioners performing human reliability assessments have ready access to, and are stimulated by, the significant research on the character and incidence of human error. In many instances there has been an interchange of roles for individuals who have passed from consultancy/practitioner roles to academic and back again. Most practitioners communicate regularly with each other and there has been a persistent interchange of working relationships between specialists in the field.

The second highly influential factor has been the insistence by H.M. Nuclear Installations Inspectorate (NII), for around 15 years, that all human reliability assessment should be underpinned by well-documented task analysis. There has been no prescription or strong recommendation of which particular analytical approach should be taken, but regulatory attention has been paid to ensuring that the methods address issues wider than the immediate concern of populating the chosen assessment method. This has often produced task analyses which have identified likely sources of error irrespective of whether they may be classed as omission, inadequate task performance, etc.

The individual human reliability specialists have also been privileged in many instances to have gained a wide experience of nuclear and non-nuclear technologies in both civilian and military applications, and this is an influential third factor. Technologies to which these individuals have been exposed include power station operations, fuel production and reprocessing, refuelling, weapons production and waste
disposal and storage. This, coupled with the regulatory environment and the expertise of a wide range of analysts, has stimulated the development within the UK of a number of bespoke approaches to meet the particular and diverse challenges of the technology being assessed.

Even within a nuclear process grouping such as power stations, there is little replication and considerable diversity in design. For example, the principal power plant designs which have received human factors assessments are: AGR, Magnox, PWR, SGHWR and PFR technologies. This rich and varied technological environment has also stimulated and required a persistent level of original analytical thought, with little opportunity to replicate assessment models directly from station to station. As a result, there have been a number of methodological developments that can assist in the identification of errors of commission.

2. UK Methods for Identifying Errors of Commission

In contrast to the informal approach to identifying errors of commission, there are a number of structured methods which have been developed in the UK that have the potential to be used for identifying commission errors. Not all have been used within the nuclear industry, but each method has been applied to human factors issues comparable to those within the nuclear industry. The methods naturally fall into three categories: Psychological Error Mechanism Description, Error Elicitation and System Affordances.

A brief description of each of these methods is given below, based upon these three categories. For each method described, the number of times it is known to have been used within the nuclear industry is reported.

2.1 Psychological Error Mechanism Description Models

The methods described in this section are methods which are psychology-based and, accordingly, these models describe the phenomenology of human error in psychological terms.

2.1.1 GEMS (Generic Error Modelling System)

Whilst the GEMS approach has been largely applied in the post-hoc analysis of incidents within the nuclear industry and elsewhere, it is frequently cited by specialists as being influential in their thinking during the analyses that they undertake for nuclear PSAs. It has not so far been used formally within a UK PSA.

GEMS is a classificatory scheme of psychological error that was developed by Reason (1987). It considers error mechanisms that can be classified as skill, rule or knowledge-based. It addresses the constructs of psychological performance derived from consideration of the human as an information processor, then adds to this approach cognitive considerations, particularly by considering internal representations of context and events termed schema, which are used to form intentions. Reason stresses that human error tendencies have their origin in useful and adaptive processes. They arise from the natural tendency to reduce cognitive strain. Accordingly, Reason argues that there is a tendency to over-utilize stored knowledge structures, heuristics and shortcuts in coping with the complex informational problems posed by modern technological systems. The GEMS approach deals, therefore, with cognitive responses to events in the form of heuristic processes, rules of thumb and habitual responses, and suggests when performance may change from skill to rule-based, or rule to knowledge-based, behaviour.

GEMS is, in effect, a comprehensive means for the analyst to understand many aspects of psychological performance. This, in principle, makes it more likely that the analyst will postulate errors of commission,
state-space diagrams and transition matrices. These three representations show: tasks, machine states and interactions during state transitions. The transition matrix provides the required integration by showing:

- fully legal transitions
- legal interactions to be used with caution,
- illegal transitions
- impossible transitions

The technique is very detailed and powerful. One very successful application of the technique has been to the analysis of distributed manual switch-gear operations, which resulted in effective design and procedural amendments. It has been found possible to identify many potential errors using the approach. In particular, it would be appropriate to use the technique with a software mediated interface, where many permutations of interaction are possible and therefore difficult to understand, without a systematic approach to description and recording of interactions.

The technique has been compared experimentally with a simplified form of SHERPA, which removes reference to psychological error mechanisms (Called PHEA). The TAFEI technique had the same accuracy as PHEA, but it proved to be more economical in terms of the use of time. It also had a remarkable 100% inter-analyst reliability.

2.3.3 EOCA (Errors of Commission Assessment)

This approach has been applied once to the formal assessment of errors of commission for the Hinkley Point 'A' Nuclear Power Station and is documented by one of its originators (Kirwan (1994a). The technique is a multidisciplinary approach which involves risk assessors, PSA modellers and human factors analysts. It is judged to have produced a comprehensive and insightful analysis of the potential errors of commission that could be influential with respect to the assessed risk at the level of event trees. The characteristic UK reliance upon task analytical approaches, is reflected in this methodology, which found errors of commission not only during responses to faults but also in the form of latent errors committed upon standby safety systems.

2.3.4 HEIST (Human Error in Systems Identification Technique)

Kirwan has undertaken further development work based upon the approach of EOCA and this has been published in Kirwan (1994b). This description provides comprehensive tables of check questions, psychological mechanisms and error reduction guidelines. These, in turn, are related to the possible external error modes which might include errors of commission.

This approach has been used as an adjunct to other approaches in several non-nuclear reliability assessments since its publication. Analysts report having found the technique to be consistently helpful.

3. Identification of Errors of Commission - Discussion

An informal telephone survey of seven representatives of the UK licensees was undertaken during November 1997 by a human factors consultant to establish their chosen approach to identifying errors of commission. Those interviewed were mainly human factors or ergonomics specialists, with the remainder being experienced and closely involved in the application of human factors techniques. In addition, a further four individuals responsible for the development of relevant methods were also interviewed.
There are four areas that respondents reported where the application of techniques such as those listed in Section 2 above would be appropriate:-

Construction of a fault schedule,
Technical Specification or Operating Rules Compliance Assessments,
Human Reliability Assessments (HRAs) in support of Probabilistic Safety Assessments,
Task analysis in support of procedures design, or validation.

In the UK, errors of commission are first identified during the construction of the fault schedule for a PSA. It is known that in at least one instance, GEMS has informed the thought processes that have led to errors of commission being identified and included within the schedule.

As an integral part of the periodic safety reviews that are performed on all the UK nuclear power plants, there is an independent assessment of the Compliance of each Station with its Operating Rules and supporting Identified Operating Instructions. This is undertaken to ensure that there are no potentially significant human events omitted from the fault schedule. This process examines any relevant reports of past incidents and also includes a qualitative human factors assessment of the particular mechanisms employed to achieve compliance and the consequences of any transgression of the rules. The assessment not only examines the ease with which the compliance mechanism is implemented, but also the understanding and beliefs of users about the purpose and the effectiveness of the rules. Clearly, misconceptions about the rules or difficulties in achieving compliance (e.g. due to limitations in the provision of instrumentation) may lead to errors of commission.

The interviews with representatives of the licensees established that no established formal, or proprietary, methods are being consistently used by licensees, or their contractors, for the identification of errors of commission within the PSA models. Three reasons emerged for this:-

1. It is felt that the extensive application of task analytical techniques, especially by human factors specialists, captures the significant errors of commission. However, there are instances where the methods listed above have been used separately, or in combination, as an adjunct to wider human factors approaches.

2. Whilst there is as yet no licensing requirement for a formal method to be used for the identification of errors of commission, task analyses do reveal errors of commission which are in effect systematic errors of omission and therefore potentially significant contributors to the risks that must already be assessed.

3. Because many analysts have both knowledge and expertise in human factors, they do not believe they are missing errors of commission that significantly affect risk.

There appear to be several reasons why errors of commission are actually identified in the application areas where such errors are relevant:-

All nuclear power plant and many other process plant HRAs are heavily based upon extensive task analytical processes (see above) that involve plant operators in extensive walk and talk-through exercises and some simulator studies, where this is appropriate.
Many analytical process, especially on complex or novel technologies, are undertaken by human factors specialists whose main concern lies in identifying strengths and weaknesses in human performance, irrespective of the often confining requirements of the PSA model.

Reference is nearly always made to operational experience and feedback data which often links strongly to errors of commission.

There is close liaison between human factors and PSA modelling specialists so that issues which map closely onto errors of commission, in particular diagnostic errors and human dependencies, are well addressed by models. This is further supported by task analytical processes, many of which examine crew availabilities, workload levels, time scales and task difficulty in considerable detail.

Given the above, it is perhaps not surprising that most interviewees felt that the concept of an error of commission, either as a useful term or as a uniquely describable phenomenon, was somewhat questionable. It was pointed out by almost all respondents that other external error modes often describe scenarios that might less usefuly be termed an error of commission. In particular, external error modes such as too early, too late, too much, right action wrong train, or wrong action right train, were all thought likely to represent typical errors of commission and accordingly, it was judged that there were several causal phenomena at work which were more likely to be identified if more precise descriptors of external error modes were used.

The view was also expressed that in some plant analyses (e.g. nuclear chemical), the comparative simplicity of the processes might mean that there would sometimes be less concern regarding the potential effect that major errors of commission might have on human factors models. The relative simplicity of most fault scenarios led the majority of the respondents to the view that most, if not all, significant errors of commission are identified correctly and in full.

Overall, the prevailing belief among UK licensees appears to be that the vast majority of errors of commission are generally identified as an inherent and natural part of performing task analyses and human reliability assessments. There was also a clear feeling amongst those with a more formal human factors background, that such errors are not as difficult to conceive as is sometimes thought (provided that one confines attention to the thoughts and acts of the rational person).

Despite the confidence that the interviewees felt regarding the ability of analysts to identify errors of commission in practice, the contrast between the apparent effort to develop techniques and their uptake requires further explanation.

It will be apparent that, in the main, formal techniques for identifying errors of commission are not applied very frequently in the UK nuclear context. Instead, the majority of the techniques that have been developed in the UK have been applied more frequently in other high hazard process industries such as chemical or oil and gas. The greater perceived need within these other industries for such techniques may possibly be explained by a combination of their less well-developed approach towards risk assessments and perhaps the more frequent use of analysts with less experience or background in human factors. Without further information, however, this apparent difference in relative levels of application remains somewhat unclear.

Another equally valid explanation may be obtained by considering further the views from within the industry that are expressed above. Ultimately, the success of any technique must be reliant upon the
understanding that an analyst has of the phenomenon (in this case errors of commission) and their personal ability to either detect the existence of mechanisms that might lead to such error, or to synthesise the possibility of such mechanisms coming into being, within the human-machine system that they are examining. Put another way it is the analyst that acts both as the detector and the interpreter of 'data'. The extent to which they must be reliant upon a formal method to do this successfully will be a function of:

- their training
- their experience
- the availability of relevant data
- the analytical methods in use that can identify the phenomenon.

4. Conclusions

A wide range of techniques for the identification of errors of commission has been developed in the UK over the last 10-15 years. Even though few if any of these methods have so far been applied in the nuclear industry, some of them appear to show sufficient promise in other high hazard applications that they could, no doubt, be applied to good effect in any future analytical work in this area.

It should be noted that, at present, in the UK nuclear industry, a substantial proportion of its human reliability analysts are generally formally qualified in a behavioural science subject, experienced in human factors and nuclear technology, and also have access to the specific operational feedback data that is applicable. Moreover, there are analytical processes (e.g. design and hazard reviews) other than the basic task analysis methods for supporting HRA that also have the capability to assist the identification of errors of commission. Accordingly, the need for analysts to be reliant upon formal methods to identify errors of commission may be somewhat diminished. Nevertheless, it is apparent that there is a large formal and informal knowledge-base in this area which, it is hoped, could find ready application to the work of the Task Group.
5. References


### Glossary of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CADA</td>
<td>Critical Action and Decision Approach</td>
</tr>
<tr>
<td>COPE</td>
<td>Credible Operator Errors</td>
</tr>
<tr>
<td>EOC A</td>
<td>Errors of Commission Assessment</td>
</tr>
<tr>
<td>GEMS</td>
<td>Generic Error Modelling System</td>
</tr>
<tr>
<td>HAZOP</td>
<td>Hazard and Operability Analysis</td>
</tr>
<tr>
<td>HEIST</td>
<td>Human Error in Systems Identification Technique</td>
</tr>
<tr>
<td>HRA</td>
<td>Human Reliability Assessment</td>
</tr>
<tr>
<td>HUMECA</td>
<td>Human Error Mode Effects and Criticality Analysis</td>
</tr>
<tr>
<td>IMAS</td>
<td>Influence Modelling and Assessment System</td>
</tr>
<tr>
<td>MORT</td>
<td>Management Oversight Risk Trees</td>
</tr>
<tr>
<td>NII</td>
<td>Her Majesty's Nuclear Installations Inspectorate</td>
</tr>
<tr>
<td>PHECA</td>
<td>Potential Human Error Causes Analysis</td>
</tr>
<tr>
<td>PREDICT</td>
<td>Procedure to Review and Evaluate Dependency in Complex Technologies</td>
</tr>
<tr>
<td>PSA</td>
<td>Probabilistic Safety Assessment</td>
</tr>
<tr>
<td>SHERPA</td>
<td>Systematic Human Error Reduction and Prediction Approach</td>
</tr>
<tr>
<td>TAFEI</td>
<td>Task Analysis For Error Identification</td>
</tr>
</tbody>
</table>

This text describes in more detail the application of the reversed Murphy diagram approach used by CEGB and its successor Nuclear Electric during the Sizewell 'B' Project. The text is extracted from a paper about defences against cognitive and conceptual error intended for publication. This is written by Dr. I.G. Umbers of Nuclear Electric Ltd. and E.M. Hickling formerly employed by Nuclear Electric.

2.3 Murphy Diagrams

Murphy Diagrams were originally developed by Pew et al (1981) as part of a retrospective analysis of four nuclear power plant incidents. Murphy diagrams are based on Rasmussen's (1976) Decision Making model (sometimes referred to as the Stepladder model). In the Murphy diagrams the Rasmussen model was extended to include potential sources of performance error associated with each decision making stage. The Diagrams invoke the principle that, if anything can go wrong, it will. Eight diagrams comprise the complete set, with each diagram depicting a different stage of the decision making model. The eight stages are identified as:

- Detection
- Observation
- Identification of system state
- Interpretation
- Evaluation of alternatives
- Goal selection
- Procedure selection
- Procedure execution

For each stage two possible outcomes are shown: "Success" (S) and "Failure" (F). Linked to each failure outcome are a series of common reasons for errors in performance in the particular decision stage. These are classified as "proximal" sources of error and "distal" sources of error. Pew et al (1981, p2-10) explain that these terms were chosen to convey an impression of immediacy of the source of error to the error itself. The "proximal" sources are intended to indicate the "state of understanding and/or awareness of the crew prior to the final exit from the decision element". The "distal" sources represent possible reasons for the "proximal" sources of error. Another way of interpreting these distinctions is to think of the "distal" sources as providing an answer to the question "why" did the "proximal" sources occur and for the "proximal" sources to provide answers to "how" the particular decision stage failed. Thus failure to identify state of plant could be due to "not all known plant states being evaluated" which in turn could be due to a "training deficiency".

For Murphy diagrams to be used to identify potential sources of error, the critical operator decisions or activities have to be determined. Each critical decision or activity then has to be matched to the appropriate Diagram by identifying the salient characteristics of the activity, e.g. determining whether it involves identifying plant state, executing a procedure, detecting a plant signal etc. Two practical problems in the application of the Murphy diagrams are apparent. The first is in unambiguously identifying the relevant diagram on the basis of the information available, i.e. being clear which stages in the Rasmussen decision model are appropriate. The second is that many of the "distal" sources tend be very general, e.g., training deficiency, display deficiency etc., and do not pinpoint the exact nature of the deficiency. A third problem is concerned with the generality of the diagrams and, in particular, whether (a) the Rasmussen decision making model covers the range of behaviours exhibited in a nuclear power plant and (b) the "proximal" and "distal" sources of error are comprehensive.
2.4 Choice of Method
Despite the potential problems with Murphy diagrams it was concluded that they provided the only method then currently available which could be applied [for identifying the requisite defences against cognitive and conceptual error] without requiring significant development work. However, in view of the problems identified above, it was considered desirable to test the adequacy of the diagrams before using them for a particular application.

2.5 Validation
The adequacy of the diagrams was tested by applying them to a well documented nuclear power plant incident with a view to determining whether they could have predicted some of the sources of human error. The Steam Generator Tube Rupture at Ginna, INPO (1982), was chosen because it had been subjected to a detailed human factors analysis in which the operator actions and the reasons for them are described. In addition, the analysis reproduces the relevant procedural steps which enables the Diagrams to be used as envisaged in a real application. This procedural information was examined by two analysts (ergonomists) who had some familiarity with nuclear power plant operations. The analysts attempted to identify in which decision stage and associated Diagram a failure could have occurred. Both analysts then examined the reasons given in the incident report for the operators' errors and selected the diagrams which accounted for the actual operator failures in terms of the "proximal" and "distal" sources of error. The two sets of Diagrams were compared and the extent to which the two analysts had been able to predict in which decision stage a failure had occurred was assessed. The Diagrams were also assessed for their completeness in accounting for actual sources of error and any omissions were identified and recorded.

The percentage of decision stages predicted correctly was 44 and 56 for each analyst respectively. The percentage of decision stages correctly predicted was 75 (12 out of 16 decision stages) when the predictions of the two analysts were combined. These "accuracy" figures need to be treated with some caution since it proved difficult in some instances to identify from the incident report the decision stage in which an error actually occurred. This tended to happen in the "higher level" decision stages where complex thought processes are invoked, and where either insufficient information was available in the incident report to identify them or where the behaviour of the operators could best be described by a number of interacting decision stages rather than one. In considering the issue of accuracy, it should be noted that a 100 % prediction accuracy could be achieved by the inefficient strategy of invoking all the Murphy diagrams; thus accuracy needs to be qualified by efficiency. Efficiency was assessed as 50 % by expressing the number of irrelevant diagrams actually chosen as a percentage of the maximum number of irrelevant diagrams which could be chosen.

Identification of the correct decision stage does not necessarily ensure that the correct proximal or distal source of error will be identified. Examination of the Ginna incident report showed that in some of the diagrams the distal sources of error were insufficient to account for all the error sources which were identified as contributing to the event. For example, procedural deficiencies were not identified as being a distal source in any of the diagrams. The adequacy of proximal sources as descriptions of how errors occurred was difficult to assess in some decisions. As with the decision stages, the chief reason for this was that the incident report did not provide sufficient information about the operators' thought processes to enable the relevant proximal source to be identified for each decision.

2.6 Application
Despite the problems identified above in applying the Murphy diagrams in a prospective manner, the results seemed sufficiently encouraging to warrant application of the diagrams to some important decisions points in the Sizewell "B" outline procedures. The aim was to use the diagrams to identify
potential sources of cognitive error and then examine the design of Sizewell "B" to see what safeguards were available to prevent such errors occurring.

The diagnostic decision chosen for analysis was concerned with distinguishing between a Steam Generator Tube Rupture, a Loss of Coolant Accident or a Secondary Depressurisation. The relevant steps in the procedure were examined by an analyst not directly involved in the design of Sizewell "B". Two decision stages were selected which were thought to represent the cognitive processes of the operators who would be following the procedures. These were: Identification of Plant State and Observation/Data Collection. The analyst then worked through each diagram postulating possible deficiencies by combining the various proximal sources of error with their associated distal sources of error. For example, if the proximal source of error was "not all possible states known" and an associated distal source was "training deficiency" then these were combined to give "The operators may not have been trained to be aware of all plant states". In another example the proximal source was "too few data acquired" which was combined with distal source "equipment malfunction" to give "display/instrument failures may make it difficult for the operators to distinguish between faults with similar symptoms". In generating these deficiencies it was noticed that, in addition to the omission of "procedural deficiency" from the distal sources of error, "communication deficiency" was not included in any of the diagrams. These distal source omissions were rectified by including them with plausible proximal sources of error. For example, "communication deficiency" was combined with "too few data acquired" to give "operators do not obtain relevant information because of (a) communication system failure, (b) distorted or ambiguous message, (c) message not recorded, (d) high ambient noise levels". The list of potential sources of error generated by this process were reviewed by the design team who then identified the safeguards against these error sources which existed in the Sizewell "B" design. Two general conclusions were drawn from this exercise. The first was that Murphy diagrams could be used in a prospective manner with a degree of confidence provided that they were modified to address identified inadequacies. The second conclusion was that the defences against the errors identified by the application of the Murphy diagrams were fairly well known and were already available or being developed within the design of Sizewell "B".

3. Assessment of the Application

Although the results of the Murphy diagram application were viewed positively by those involved, an independent review of the trial identified certain potential shortcomings with the approach which could undermine confidence in its ability to identify potential sources of error within the design of Sizewell "B". In particular it was felt that, the lack of detail on the derivation of the diagrams, the identified omissions in sources of error, coupled with the considerable degree of interpretation required to identify specific sources of potential error, raised doubts about the completeness and precision of the approach. From a practical view point it was concluded that application of the Diagrams would not be cost effective because of the large number of procedural steps which would have to be analysed and the potential duplication of effort involved. Finally, since the Murphy diagrams are scenario orientated they do not give confidence that safeguards for events which are not covered by the selected scenarios are addressed.

To address these concerns it became evident that a different approach was required in which the origins were traceable and the interpretation required to identify potential sources of error was minimised. In addition, application of the method needed to be cost effective and provide some confidence that the defences which were assessed were not confined to those associated with a limited number of fault scenarios.
To overcome the concerns about traceability it was decided to carry out a review of the literature with the aim of distilling those features of human cognition relevant to the identification of potential sources of cognitive/conceptual error and the defences against them. The intention was then to explore ways in which the results could be applied directly by those responsible for the design of Sizewell "B" and thus provide a method of addressing cognitive/conceptual error which was cost effective and not scenario limited. In this respect it was considered that more emphasis should be placed on identifying the existence/absence of defences since this would require less interpretation and be easier for system designers to apply."
Contribution from the United States
Summary of ATHEANA

Dr. John Forester
Sandia National Laboratories, United States of America

This paper describes the most recent version of a human reliability analysis (HRA) method called "a technique for human event analysis" (ATHEANA). The new version is documented in NUREG-1624, Rev. 1. The development of ATHEANA is the result of efforts sponsored by the Probabilistic Risk Analysis (PRA) Branch in the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research (RES). ATHEANA was developed to increase the degree to which an HRA can represent the kinds of human behaviors seen in accidents and near-miss events at nuclear power plants and at facilities in other industries that involve broadly similar kinds of human/system interactions. In particular, ATHEANA provides this improved capability by:

• more realistically searching for the kinds of human/system interactions that have played important roles in accident responses, including the identification and modeling of errors of commission and dependencies

• taking advantage of, and integrating, advances in psychology, engineering, human factors, and probabilistic risk assessment (PRA) disciplines in its modeling

Motivation for Developing an Improved Human Reliability Analysis Capability

The record of significant incidents in nuclear power plant NPP operations shows a substantially different picture of human performance than that represented by human failure events typically modeled in PRAs. The latter often focus on failures to perform required steps in a procedure (as was seen in the review on individual plant examinations and documented in NUREG-1560,2). In contrast, human performance problems identified in real operational events often involve operators performing actions that are not required for an accident response and, in fact, worsen the plants condition (i.e., EOCs). In addition, accounts of the role of operators in serious accidents, such as those that occurred at Chernobyl 4 (NUREG-1250,3 and NUREG-1251,4), and Three Mile Island, Unit 2 (TMI-2,5), frequently leave the impression that the operator's actions were illogical and incredible. Consequently, the lessons learned from such events often are discounted as being very plant- or event-specific.

---


As a result of the TMI-2 event, numerous modifications and backfits were implemented by all NPPs in the United States, including symptom-based procedures, new training, and new hardware. After the considerable expense and effort to implement these modifications and backfits, the types of problems that occurred in this accident would be expected to be affixed. However, there is increasing evidence that there may be a persistent and generic plant safety problem that was revealed by TMI-2 (and Chernobyl) but not affixed. This safety problem is a result of errors of commission involving the intentional operator bypass of engineered safety features (ESFs). In the TMI-2 event, operators inappropriately terminated high-pressure injection, resulting in reactor core undercooling and eventual fuel damage. NRC's Office of Analysis and Evaluation of Operation Data (AEOD) published "Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features," AEOD/E95-01, July 1995(6), identifying 14 events over the previous 41 months in which an ESF was inappropriately bypassed. The AEOD/E95-01 report concluded that these events, and other similar events, show that this type of "human intervention may be an important failure mode." Events analyses performed to support the ATHEANA development (NUREG/CR-6265,7) and the HSECS database(8) also have identified several errors of commission that result in the inappropriate bypass of ESFs.

In addition, event analyses of power plant accidents and incidents performed for this project show that real operational events typically involve a combination of complicating factors that are not addressed in current PRAs. The following examples illustrate the factors that may complicate operators' responses to events:

- scenarios that deviate from operators expectations, based on their training and experience

- multiple equipment failures and unavailabilities (especially those that are dependent or human-caused) that go beyond those represented in operator training in simulators and assumed in safety analyses

- instrumentation problems for which the operators are not fully prepared and which can cause misunderstandings about the event (this may become increasingly so for digital-based instrumentation systems)

- plant conditions not addressed by procedures

Unfortunately, events involving such complicating factors frequently are interpreted only as an indication of plant-specific operational problems, rather than a general cause for concern for all plants.

The purpose of ATHEANA is to develop an HRA modeling process that can accommodate and represent the human performance found in real NPP events, and that can be used with PRAs or other safety


perspectives to resolve safety questions. On the basis of observations of serious events in the operating history of the commercial nuclear power industry, as well as experience in other technologically complex industries, the underlying premise of ATHEANA is that significant human errors occur as a result of a combination of influences associated with plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel.

In most cases, these error mechanisms are often not inherently bad behaviors, but are usually mechanisms that allow humans to perform skilled and speedy operations. For example, people often diagnose the cause of an occurrence on the basis of pattern matching. This is in many cases an efficient and speedy way to respond to some event. However, when an event actually taking place is subtly different from a routine event, there is a tendency for people to quickly recall and select the nearest similar pattern and act as if the event was the routine one. In the routine circumstance, this rapid pattern matching allows for very efficient and timely responses. However, the same process can lead to an inappropriate response in a nonroutine situation. Other examples of such error mechanisms are discussed below.

Given this assessment of the causes of inappropriate actions, a process is needed that can search for likely opportunities for inappropriately triggered mechanisms to cause unsafe actions. The starting point for this search is a framework (presented in Fig. 1 and described below) that describes the interrelationships among error mechanisms, the plant conditions and performance-shaping factors that set them up, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe. The framework also includes elements from plant operations and engineering, PRAs, human factors engineering, and behavioral sciences. All of these elements contribute to the understanding of human reliability and its associated influences, and have emerged from the review of significant operational events at NPPs by a multidisciplinary project team representing all of these disciplines. The elements included are the minimum necessary to describe the causes and contributions of human errors in, for example, major NPP events.

The human performance-related elements of the framework (i.e., those requiring the expertise of the human factors, behavioral science, and plant engineering disciplines) are performance-shaping factors (PSFs), plant conditions, and error mechanisms. These elements are representative of the level of understanding needed to describe the underlying causes of unsafe actions and explain why a person may perform an unsafe action. The elements relating to the PRA perspective, namely the human failure events and the scenario definition, represent the PRA model itself. The unsafe action and HFE elements represent the point of integration between the HRA and PRA model. A PRA traditionally focuses on the consequences of an unsafe action, which it describes as a human error that is represented by an HFE. The HFE is included in the PRA model associated with a particular plant state that defines the specific accident scenarios that the PRA model represents.

The framework has served as the basis for the retrospective analysis of real operating event histories (NUREG/CR-69039, NUREG/CR-626510, the HSECS database11, and NUREG/CR-635012). That


12 S. E. Cooper, A. Ramey-Smith, J. Wreathall, G. W. Parry, D. C. Bley, J. H. Taylor, W. J. Luckas, A Technique for
retrospective analysis has identified the context in which severe events can occur; specifically, the plant conditions, significant PSFs, and dependencies that set up operators for failure. Serious events appear to involve both unexpected plant conditions and unfavorable PSFs (e.g., situational factors) that comprise an error-forcing context. Plant conditions include the physical condition of the NPP and its instruments. Plant conditions, as interpreted by the instruments (which may or may not be functioning as expected), are fed to the plant display system. Finally, the operators receive information from the display system and interpret that information (i.e., make a situation assessment) using their mental model and current situation model. The operator and display system form the human-machine interface (HMI).

On the basis of the operating events analyzed, the error-forcing context typically involves an unanalyzed plant condition that is beyond normal operator training and procedure-related PSFs. For example, this error-forcing condition can activate a human error mechanism related to an inappropriate assessment of the situation (e.g., a misdiagnosis). This can lead to the refusal to believe or recognize evidence that runs counter to the initial misdiagnosis. Consequently, mistakes (e.g., errors of commission), and ultimately,

![Diagram](image)

**Figure 1. Framework**

an accident with catastrophic consequences, can result. These ideas lead to another way to frame the observations of serious events that have been reviewed:

- The plant behavior is outside the expected range.
- The plant’s behavior is not understood.
- Indications of the actual plant state and behavior are not recognized.
- Prepared plans or procedures are not applicable nor helpful.

From this point of view, it is clear that key factors in these events have not been within the scope of existing PRAs/HRAs. If these events are the contributors to severe accidents that can actually occur, then

---

expansion of the PRA/HRA to model them is essential. Otherwise a PRA may not include the dominant contributors to risk.

Earlier HRA methods have implicitly focused on addressing the question, "What is the chance of random operator error (e.g., operator fails to...) under nominal accident conditions?" Even when performance-shaping factors are included, they are typically evaluated for the nominal event sequence or, at best, for particular cut sets. The analyses have not looked much beyond the hardware modeled in the PRA for specific conditions that could complicate operator response; the only significant exception has been the consideration of the time available for action, which can vary from one set of accident conditions to another. On the basis of review of the operating experience in several industries, a more appropriate question to pursue is, "What is the chance of an error-forcing-context occurring so that operator error is very likely?" This question lies at the core of the new ATHEANA method.

The systematic structuring of the different dimensions influencing human/system interactions that is provided by the multidisciplinary HRA framework, along with the search for cognitively demanding context that is driven by consideration of the elements of cognitive information processing, brings a degree of clarity and completeness to the process of modeling human errors in the PRA process. The absence of this systematic approach in earlier HRA methods has limited the ability to incorporate human errors in PRAs in a way that could satisfy both the engineering and the behavioral sciences. The consequence has been that PRA results are not seen as accurate representations of the contribution of human errors to power-plant safety, particularly when compared with the experience of major NPP accidents and incidents.

The Importance of Plant Conditions and Context in Human Performance

The reviews of accidents and serious incidents performed in developing ATHEANA have led to the identification, development, and ultimately to the confirmation of the principles underlying the method. As discussed above, one of the key aspects of ATHEANA is the recognition that plant conditions are a key influence on operator performance, and that these conditions can be much more varied than current combinations of HRA and PRA tools typically represent. This section further discusses the reasons why ATHEANA has been developed to significantly expand the incorporation of particularly challenging plant conditions and the associated contexts faced by operators, and presents the general principles that underlie the way ATHEANA does this.

Current HRA and PRA Perspective

Most HRA analyses performed in current PRAs provide a limited recognition of the influences of plant behavior on human reliability. This comes about as a consequence of two inter-related features. First, in most applications of PRA models, analyses are performed for classes of initiating events (such as small loss-of-coolant accidents and transient reactor trips) and equipment faults, with only limited consideration given to variations of the initiating event and equipment failures. For example, only complete equipment failures are usually considered. This is partly a result of the use of fundamentally binary success or failure models that lie at the center of almost all PRA modeling methods and that tend to lead to the need for simplifications in the complexity of real plant conditions. In the PRA analysis, the "most challenging" version of the initiating event is often assumed; here most challenging is usually used with respect to the demands made on equipment, such as the largest number of pumps needed and the shortest time scale for them to start to prevent core damage. This approach is often considered to be conservative, and it may well be with respect to demands on equipment performance and physical resources. However, as discussed below, these conditions may well not be the most challenging in terms of the demands on the
operator in responding to the event B especially the operators understanding of the conditions.

Second, most HRA methods currently used are very limited in terms of their ability to take into account different plant conditions. Some methods can take into account differences in the time scales available for operator response. Most other methods can take into account the performance-shaping factors (PSFs) such as the layout of procedures, the location and number of displays, and the experience level of the operators. However, very few of these factors provide the most important variations in the conditions under which people perform and which are found to be very challenging. In summary, both the PRA approach of analyzing wide ranges of conditions using a conservative all-embracing models and assumptions, and the lack of sensitivity of HRA methods to changes in plant conditions, have led to the lack of explicit consideration of ranges of plant conditions in most PRAs. (It is recognized that attempts to consider some ranges of plant conditions have been made in a few PRAs, such as where some accident sequences that have significantly different time scales for actions are addressed separately. However, the insensitivity of the available HRA tools has limited the analysts ability to take into account anything other than simple time-scale differences.)

The Significance of Context

Recent work in the behavioral sciences\(^{13}\)\(^{14}\) has contributed to the understanding of the interactive nature of human errors and plant behavior that characterize accidents in high-technology industries. This understanding suggests that it is essential to analyze both the human centered factors (e.g., PSFs such as human B machine interface design, content and format of plant procedures and training) and the conditions of the plant that call for actions and create the operational causes for human B system interactions (e.g., misleading indicators, equipment unavailabilities, and other unusual configurations or operational circumstances).

The human-centered factors and the influence of plant conditions are not independent of each other. In many major accidents, particularly unusual plant conditions create the need for operator actions and, under those unusual plant conditions, deficiencies in the human-centered factors lead people to make errors in responding to the incident.

Therefore the typical evaluations performed in HRA assessments of PSFs, such as procedures and human/Bmachine interfaces and training (as discussed above) may not identify critical human-performance problems unless consideration is also given to the range of plant conditions under which the controls or indicators may be required. To identify the most likely conditions leading to failure, the analysis of PSFs must recognize that plant conditions can vary significantly within the event-tree or fault-tree definition of a single PRA scenario. Moreover, some plant conditions can be much more demanding of operators than others. Both the conditions themselves and the limitations in PSFs, such as procedures and training, can affect an operators performance during an accident.

For example, a particular layout of indicators and controls may be perfectly adequate for the nominal conditions assumed for a PRA scenario. However, deviations from the conditions implicitly or explicitly assumed for the PRA scenario possibly may occur so that specific features of the layout would influence the occurrence of operator errors in an accident response. An example of such a deviation was the


location of the breach in the Three Mile Island-2 (TMI-2) accident. The typical conditions assumed for a small loss-of-coolant accident (the type of PRA scenario representing the TMI-2 accident) included a falling pressurizer level, but not the position indications of the pressurizer power-operated relief valves (PORVs). However, the deviation created by a leak in the pressurizer PORVs made these indications much more important.

Simply stated, operator failures associated with a PRA scenario are perhaps more likely to result from particular deviations from typical plant conditions that create significant challenges to the operators than they are from random human errors that might occur under the single set of conditions generally assumed by PRA analysts. Analyses of power plant accidents and near-misses support this perspective, indicating that the influence of unusual plant conditions is much more significant than random human errors [NUREG/CR-1275, Vol. 815, NUREG/CR-609316, NUREG/CR-626517, and NUREG/CR-635018]. The need for consideration of context has been a recurrent theme in discussions about improved HRA methods, including those by Hall et al.19, Dougherty20, Woods21, and Hollnagel22.

The significance of unusual contexts derived from incident analyses is consistent with experience described by training personnel. They have observed that operators can be “made to fail” in simulator exercises by creating particular combinations of plant conditions and operator mindset. Examples of difficulties in operator performance in challenging simulator training situations are given in NUREG/CR-620823.

Our review of operating events, particularly those that seem to have the potential for serious degradations of safety, has shown that these events involve various types of deviations that cause significant challenges to the operators. There are several types of such deviations from the typical conditions assumed in the PRA scenarios. Examples include:


261
• Physical deviations, in which the plant behaves differently than is typically expected in the related PRA scenario and which affect the way the plant behaves compared with the operator’s training and expectations. These may cause the indications of the plant condition to be significantly different from the operators’ expectations and may not match those used in development of procedures and operator training.

• Temporal deviations, in which the time scales of the plant conditions are different from those typically assumed in the related PRA scenario and may affect the time scales in which operators must act. These may cause symptoms to occur significantly more slowly or be out of sequence with those assumed in procedures and in training, thus causing doubt about the relevance or effectiveness of the expected responses. Alternatively, the conditions may occur much faster than expected, thereby inducing high levels of stress in the operators or leading to failure while the operators are systematically stepping through their procedures.

• Deviations in the causes of initiating events, in which partial equipment failures or failures in support systems occur, thus creating complex sets of unexpected symptoms that may lead operators to act inappropriately or to delay taking action. When support-system failures are explicitly incorporated in PRA models, they are often focused on complete or single-train losses and are concerned with the impact on plant hardware, not on the operators being confused or misled by the failures.

• Deviations associated with failures in instrumentation systems can make it difficult for operators to understand and plan suitable responses. While some PRAs may incorporate some kinds of instrumentation failures that lead, for example, to automatic equipment not being started when needed or interlocks that prevent correct operator actions, there has been very little consideration of how instrument faults will affect the ability of the operators to understand the conditions within the plant and act appropriately. In addition, failures of the instrumentation and control systems can bring about the kinds of deviations discussed above.

In many cases, these types of deviations can lead operators to fail because of some kind of "mismatch." For example, when a plant behaves in a way that is significantly different from the operators’ expectations (a mismatch between plant behavior and training), and the operators respond in accordance with their expectations, the resultant actions can lead to loss of important equipment operation and functions for the conditions actually taking place. The operators believe that the reactor system was "going solid" at TMI-2 led them to reduce and stop high-pressure injection, which led to the loss of core cooling and damage. More recent examples from operating experience indicate that despite the changes in training, development of procedures, and the like, mismatches are still a concern in operations.

The idea of a mismatch has proved a useful concept for describing several kinds of problems underlying events, and provides one basis for searching for problem scenarios. To provide an effective tool for measuring and controlling risk, a PRA must be able to realistically incorporate those human failures that are caused by off-normal plant conditions, as well as those that occur randomly during nominal accident conditions. In the ATHEANA application process, the concept of mismatches is used to provide a basis for the searches for challenging conditions. Particularly important types of mismatches are used to identify specific contexts that may cause failures. Four specific types of searches are used in the ATHEANA prospective application process:

• searches that use keywords to prompt the analysts to consider types of physical deviations from the standard, or base case, accident conditions (for example; larger, smaller, faster, slower)
searches that examine the key decision points in related procedures to see if deviations from the base case scenario could lead to inappropriate actions (this is similar in concept to the approach developed by Julius, et al.\textsuperscript{24} for full-power applications, though their focus was to identify instrumentation errors that could induce the same kinds of failures)

- searches for possible dependencies between equipment faults and support system failures. Such dependencies can create cognitively challenging situations because:
  - their effects can be very plant specific and therefore operators are unlikely to have learned relevant lessons about them from other plants experiences
  - the consequences of the dependencies will often appear as seemingly independent multiple failures in both balance-of-plant and safety equipment
  - partial failures in support systems can create abnormal conditions in the equipment they support that are difficult to identify and understand

- searches that try to identify other causes of deviations beyond those listed above. This is an attempt at accomplishing relative completeness. ATHEANA provides tables and structures to help the analyst think of causes of EFCs beyond those listed here.

The identification of important mismatches and associated EFCs is largely based on an understanding of the kinds of psychological mechanisms causing human errors that can be set up by particular plant conditions lying within the PRA definitions of accident scenarios. The next section briefly discusses these mechanisms and the way ATHEANA identifies their likely effect on operator behavior.

Human Information Processing

There have been many attempts over the past 30 years to better understand the causes of human error. The main conclusion from these works is that few human errors represent random events; instead, most can be explained on the basis of the ways in which people process information in complex and demanding situations. Thus, it is important to understand the basic cognitive processes associated with plant monitoring, decision-making, and control, and how these can lead to human error. The main purpose of this section is to describe the relevant models in the behavioral sciences, the mechanisms leading to failures, and the contributing elements of error-forcing contexts in power plant operations. The discussion is largely based on the work of Woods\textsuperscript{25}, Roth\textsuperscript{26}, Mumaw\textsuperscript{27}, and Reason\textsuperscript{28,29}.


\textsuperscript{27} R. J. Mumaw & E. M. Roth, "How to be more devious with a training simulator: Redefining scenarios to emphasize cognitively difficult situations." 1992 Simulation MultiConference: Nuclear Power Plant Simulation and Simulators, Orlando, FL, April 6-9, 1992.
The basic psychological model underlying the ATHEANA method is the information processing model that describes the range of human activities required to respond to abnormal or emergency conditions. The model, in the form used in this application, considers actions in response to abnormalities as involving basically four cognitive steps:

1. situation assessment
2. monitoring/detection
3. response planning
4. response implementation

Figure 2 illustrates the major cognitive activities that are assumed to underlie operator performance.

The critical elements of the model can be briefly defined as follows:

**Monitoring/Detection:** The activities involved in extracting information from the environment. Monitoring is checking the state of the plant to determine whether the systems are operating correctly. Detection, in this context, refers to the operator becoming aware that an abnormality exists.

**Situation Assessment:** Situation assessment involves developing and updating a mental representation of the factors known, or thought to be affecting the plant state, at a given point in time. The mental representation resulting from situation assessment is referred to as a situation model.

**Situation Model:** A mental representation of the current plant condition, and the factors thought to be affecting the plant state resulting from the operators situation assessment. The situation model is created by an interpretation of operational data in light of the operators mental model. (An operators situation model is usually updated constantly as new information is received; failure to update a situation model to incorporate new information can be the result of an error mechanism).

**Mental Model:** Mental representations that integrate a persons understanding of how systems and plants work. A mental model enables a person to mentally simulate plant and system performance in order to predict or anticipate plant and equipment behavior.

**Response Planning:** Deciding on a course of action, given a particular situation model. In general, response planning involves identifying plant-state goals, generating one or more alternative response plans, evaluating the response plans, and selecting the response plan that best meets the goals identified.

**Response Implementation:** Taking the specific control actions required to perform a task, in accordance with response planning. Response implementation may involve taking discreet actions (e.g., flipping a switch) or it may involve continuous control activity (e.g., controlling the steam generator level). It may be performed by a single person, or it may require communication and coordination among multiple individuals.

---


Figure 2. Major Cognitive Activities Underlying NPP Operator Performance

The quality of output from the major cognitive activities represented in the model are assumed to be affected by at least three important cognitive factors. They are knowledge, processing resource, and strategic factors. Errors arise when there is a mismatch between the state of these cognitive factors (i.e., the cognitive resources available to the operator) and the demands imposed by the situation. How these cognitive factors affect the operator's cognitive performance and how ATHEANA uses this information to address the relationship between unsafe actions, human error mechanisms, and error-forcing contexts is discussed below.

Knowledge Factors
In considering the influence of knowledge factors on performance, two types of problems need to be considered: content and access. Information content was discussed above with respect to an operator's knowledge, e.g., their mental model. As noted, the operator's knowledge is not necessarily accurate or complete and at times it can be oversimplified. However, even when knowledge is available, it must be accessed by operators and be used to assess a situation and plan a response.

This is known as the memory retrieval process and it is highly context-dependent. That is, contextual cues facilitate the retrieval of information from memory. The more retrieval cues available, the greater the probability that information can be retrieved. Retrieval cues, for example, can be a pattern of information that the operator recognizes as a particular event or situation.

There are other knowledge factors that influence the information retrieval process, making some information more likely to be recalled than other information:
• Recency - operators are biased to recall or bring to mind events that have occurred recently or are the subject of recent operational experience, training, or discussions

• Frequency - operators are biased to recall or bring to mind events that are frequently encountered in operations in situations that appear (even superficially) to be similar to the scenario being analyzed

• Similarity - operators are biased to recall or bring to mind events that have characteristics (event superficial) similar to the scenario, particularly if the event brought to mind is a classic event used in training or discussed extensively by the operators.

These factors may lead to the recall of information that is not entirely appropriate to the situation. For example, if a situation includes features that are similar to an event that recently occurred, an operator might recall that recent event and interpret the current situation to be the same.

In addition, relevant information that the operator may possess may not be recalled. For example, if a situation that rarely occurs has features in common with an event that is more familiar, operators may fail to recognize the rare event when it occurs because they interpret the information as indicative of the familiar event.

Processing Resource Factors

Tasks that operators perform use cognitive processing resources. However, people do not have an infinite amount of cognitive resources, such as attention and memory. Instead, there is a limited amount that must be distributed among the tasks that operators are performing. Tasks differ in terms of their demands for processing resources. If one task requires a great deal of attention and memory resources, then there is little available to perform other tasks. If a set of tasks uses up most of the available processing resources, then new tasks will have to be delayed until resources become available. If a task requires more resources than are available, then its performance may suffer and may be slow, inaccurate, or error prone.

In general, tasks that operators are familiar with and well trained in require fewer resources than those that are unfamiliar and novel. Operators may perform routine procedure-based tasks almost effortlessly, using little of the processing resources available. However, when operators are confronted with a cognitively demanding situation in which the information provided by indications is confusing or contradictory (and where it may be unclear how well the available procedures are addressing the situation), a great deal of processing resources will be expended to analyze the situation and plan appropriate responses. In such situations, the resource limitations can considerably limit the operator’s capabilities to monitor, reason, and solve problems.

It is also important to note that when operators are performing familiar, well-trained tasks, their information processing capabilities appear almost automatic and large amounts of information are processed in parallel. In contrast, when confronted with unfamiliar situations, the effects of limited information processing resources become more apparent. Operators no longer respond in an automatic mode and instead become slow, deliberate, serial processors of information. Information processing comes under much more conscious control. This type of analytic processing rapidly drains resources. To cope with such demanding cognitive situations, operators tend to use cognitive shortcuts that bypass careful, complete analysis of information. These shortcuts, called "heuristics," are methods that reduce
the expenditure of cognitive effort and resources, and reduce the uncertainty of unfamiliar situations. An example is to do only enough analysis to form an initial hypothesis about the cause of the current situation. Once the partial analysis leads to a diagnosis, the information analysis is terminated. The potential problem with this type of heuristic is that a more detailed analysis of information may have revealed the situation to be a similar but less familiar one. In this example, the incomplete situation analysis may lead to an inaccurate situation model and inappropriate response plans.

Strategic Factors

Strategic factors influence choices under uncertain, potentially risky conditions. This can include situations where there are multiple conflicting goals, time pressure, and limited resources.

People often are placed in situations where they have to make choices and tradeoffs under conditions of uncertainty and risk. Situations often involve multiple interacting or conflicting goals that require considering the values or costs placed on different possible outcomes. An example relates to the decision of when to terminate a safety injection. Safety injection is required to mitigate certain types of accidents. On the other hand, if safety injection is left operating too long, it can lead to overfilling of the pressurizer. This creates a conflict situation where multiple safety-related goals must be weighed in determining an appropriate action.

One factor affecting these tradeoffs is the actual perception of risk. Using their knowledge and experience, operators estimate the risk that is associated with various situations. However, there is a common tendency to underestimate risk in low-probability, risk-significant situations in which operators have experience and when they perceive themselves to be in control.

Since their perception of risk is optimistic, plant operators do not expect significant abnormal situations to occur. Thus, they rely on redundant and supplemental information to confirm the unusual condition. Upon verification of several confirmatory indicators, the operator can accept the information as indicating an actual off-normal condition (compared with a spurious condition). However, this process still creates a conflict between the cost to productivity for falsely taking an action that shuts down the reactor versus the cost for failing to take a warranted action.

The above example illustrates another factor that operators often must consider (i.e., the consequences of different types of errors). For example, under conditions of uncertainty, an operator may have to weigh the consequences of failure to take an action that turns out to have been needed against the consequences of taking an action that turns out to be inappropriate.

There are also tradeoffs on when to make the commitment to a particular course of action. Within the constraints of limited processing resources and available time, operators have to decide whether to take corrective action early in a situation on the basis of limited information, or to delay a response until more information is available and a more thorough analysis can be conducted. On the one hand, in dynamic, potentially high-consequence (to risk or productivity) situations, the costs of waiting can be high. On the other hand, the costs of incorrectly making a decision can be high as well.

In summary, operators in abnormal events can be confronted with having to make decisions while facing uncertainty, risk, and the pressure of limited resources (e.g., time pressure, multiple demands for the same resources). The factors that influence operators' choices in such situations include goal tradeoffs, perceived costs and benefits of different options, and perceived risk. When considering the decisions that operators are likely to make, it is necessary to explicitly consider the strategic factors that are likely to
affect performance, including the presence of multiple interacting goals, the tradeoffs being made, and the pressures present that shift the decision criteria for these tradeoffs.

Modeling of Human Error Mechanisms

The characteristics of human information processing discussed above illustrate how cognitive failures can occur during each of the major cognitive activities (monitoring or detection, situation assessment, response planning, and response implementation). Cognitive failures stem from processing mechanisms associated with limitations in knowledge, access to knowledge, processing resources, and strategic factors. However, it is important to remember that not all of the described processing characteristics will necessarily lead to unsafe actions and human failure events. In fact, many of the processes, heuristics, and strategies represent normally efficient and effective means for individuals to evaluate incoming information and to develop and implement appropriate responses. For example, attempting to match a perceived information pattern (such as a pattern of indicators) with an already existing known pattern in memory can facilitate performance in high-demand situations. Alternatively, the use of such a heuristic can also lead to an unsafe action if, for example, an individual's criteria for accepting a match are set too low (possibly due to time constraints) or the indications are actually unreliable. While individuals (and crews) will develop their own set of more or less naturalistic processing strategies over time, it is also the context in which individuals are placed (i.e., the plant conditions and the performance-shaping factors), that determines which processing characteristics are activated or implemented in certain situations and whether or not they are appropriate. As discussed above, when processing mechanisms lead to inappropriate actions with unsafe consequences because of the context in which they are used, they are referred to as error mechanisms.

An important set of context-related factors likely to contribute to the potential for particular error mechanisms becoming operative in accident scenarios is the behavior of the parameters that reflect critical aspects of the plant conditions, e.g., steam generator level and pressure. The behavior of the parameters includes the behavior of individual parameters as perceived by the operators, the behavior of the parameters relative to one another, and the more global or Gestalt behavior of the parameters as perceived or interpreted by the operators. It is proposed that the behavior of critical parameters over time and relative to one another can, in conjunction with relevant PSFs such as operator training and experience, plant procedures, and the nature of the human-machine interface, have a significant impact on the manifestations of human error mechanisms. The basic assumption is that accident scenario characteristics, as represented by the behavior of critical parameters, can elicit or interact with certain human responses (e.g., complacency, anxiety) that facilitate the occurrence of an unsafe action or create situations that make certain processing mechanisms, strategies, or biases (e.g., recency effects, confirmation bias) inappropriate or ineffective. It is further assumed that the behavior of critical parameters can have different impacts, depending on the stage of information processing in which an individual is engaged, i.e., detection, situation assessment, response planning, or response implementation. Moreover, the PSFs that will contribute to the likelihood of an unsafe action occurring will be tied to the specific behavior of the plant and its impact on the operators.

Characteristics of Parameters and Scenarios

A number of aspects regarding the behavior of parameters in an accident scenario have been identified as potentially influencing the likelihood of certain error mechanisms becoming operative and thereby

contributing to an unsafe action. The first set is based on an extension of the guide words and concepts used in HAZOP\textsuperscript{31} analyses. A second set is based on a set of characteristics catalogued by Woods\textsuperscript{32,33,34}, Roth\textsuperscript{35}, Mumaw\textsuperscript{36}, and their colleagues that attempts to describe why problem scenarios are difficult. The basic notion is that scenarios (which by definition evolve over time) contain features that create the opportunity for normal human information processing and action to be inappropriate or ineffective, essentially by creating unusual cognitive demands.

Parametric Influences. A set of descriptors can be used to describe the behavior of parameters that reflect the plant dynamics resulting from a given initiating event and any contributing system failures. It is assumed that the parameters vary (or do not vary) according to the existing plant conditions, and the current focus is on how particular variations in the parameters could interact with characteristics of human information processing to lead to unsafe actions. Relevant aspects of the way the parameters behave include (but are not limited to): the lack of a critical indication (instrumentation failure) or the lack of a compelling indication for an important parameter

- a small or large change in a relevant parameter
- a lower or higher than expected value of a parameter
- a low or higher rate of change in a parameter
- changes in two or more parameters in a short time
- delays in changes in two or more parameters
- one or more false indications
- direction of change in parameter(s) over time is not what is expected
- direction of change in parameters over time relative to each other is not what is expected.
- relative rate of change in two or more parameters is not what is expected
- apparently relevant parameters are actually irrelevant and misleading

Whether such behavior in critical parameters will affect human information processing depends on such things as the operators’ physiological responses to the situation, their current situation model, their expectations regarding what is occurring, the availability of other sources of information, and other PSFs that could be relevant to the scenario. Nevertheless, the way the parameters behave (as represented by plant indicators) has the potential to elicit certain error mechanisms that lead to unsafe actions. For example, a slow rate of change in a parameter may not be detected in a timely manner and even if it is, it may induce complacency during the early stages of an accident. Furthermore, if operators have already formed an expectation about what is occurring in a scenario, a small change in a parameter might be dismissed due to a fixation error, confirmation bias, or other error mechanism. The potential influences


\textsuperscript{34} D.D. Woods & E.S. Patterson, (in press). \textit{How Unexpected Events Produce An Escalation Of Cognitive And Coordinative Demands}\textsuperscript{34} P.A. Hancock and P.A. Desmond (Eds.), Stress Workload and Fatigue. Lawrence Erlbaum, Hillsdale NJ.


269
of such variations in parameters in the context of the different information processing stages, likely error mechanisms, and contributing PSFs are examined in applying the ATHEANA method.

Scenario Influences. Woods\textsuperscript{37,38,39}, Roth\textsuperscript{40}, Mumaw\textsuperscript{41}, and their colleagues described a class of scenario-related conditions that can contribute to operators taking unsafe actions. The basic thesis is that the characteristics of the evolution of a scenario (including the behavior of critical parameters) can complicate operator performance during the different stages of information processing. For example, a scenario that starts out appearing to be a simple problem (based on strong but incorrect or incomplete evidence) can lead operators to take apparently appropriate actions, but then make them resistant to change or insensitive to correct information that appears later. Such a scenario is referred to as a garden path problem, since the operators get set up to form a strong but incorrect hypothesis that prevents them from appropriately considering later information. Once again, underlying error mechanisms such as simplifying, fixation, recency effects, and confirmation bias can contribute to operators taking unsafe actions. Other types of complicating scenarios catalogued by Woods and others include those that:

- contain missing or misleading information
- require unexpected late changes
- create dilemmas, impasses, or double-binds
- require choices that have tradeoffs
- induce plant-related side effects
- contain red herrings
- contain activities by other agents or automatic systems that mask key evidence
- induce multiple (all seemingly valid) lines of reasoning
- require multiple tasks to be performed at a high tempo
- contain events that seem to be escalating the problem
- contain events in which the operators responses lead to new problematic events
- contain events that interact to create complex symptoms

As with the parametric influences discussed in the preceding section, whether scenarios with such characteristics will affect human information processing and lead to unsafe actions depends on a number of factors, but certainly, reasonably possible accident scenarios should be examined to see if they contain these or similar characteristics. Detailed descriptions of these types of scenarios and guidance on how to consider other potential influences such as PSFs are provided in the ATHEANA documentation.

Overview of the ATHEANA Process

The information presented above discusses the principles and concepts underlying ATHEANA. This section summarizes the two ATHEANA application processes:


\textsuperscript{39} "Op. cit., 34, D.D. Woods & E.S. Patterson, (in press)".

\textsuperscript{40} "Op. cit., 23, E. M. Roth, R. J. Mamaw, and P. M. Lewis NUREG/CR-6208 (1994)".

\textsuperscript{41} "Op. cit., 27, R. J. Mamaw & E. M. Roth (1992)".

270
(1) retrospective analyses of past operational events
(2) prospective analyses (or HRA analyses) to support PRA or other risk studies

Summary of Retrospective ATHEANA Analysis

The retrospective analysis initially was developed to support the development of the prospective ATHEANA analysis. However, as the retrospective analysis matured, it became evident that this approach was useful beyond the mere development of the ATHEANA prospective approach. The results of retrospective analyses are powerful tools in illustrating and explaining ATHEANA principles and concepts. Also, the ATHEANA approach for retrospective analysis was used to train third-party users of ATHEANA in an earlier demonstration of the method. In this training, not only example event analyses, but actual experience in performing such analyses helped new users develop the perspective required to apply the prospective ATHEANA process. Finally, the results of event analyses using the ATHEANA approach are useful in themselves.

The retrospective approach can be applied broadly, using the ATHEANA framework described above. Both nuclear and non-nuclear events can be easily analyzed using this framework and its underlying concepts. A more detailed approach has been developed for nuclear power plant events, although it can be generalized for other technologies. This more detailed approach is more closely tied to the ATHEANA prospective analysis than general use of the framework. NUREG-1624, Rev. 1\textsuperscript{42} provides examples of event analyses using the framework approach and guidance for performing the more detailed analyses.

In performing retrospective analysis, the basic objective is to gain an understanding of the causes of human failures in risk-significant operational events. To do so, the analysts must answer such question as:

(1) What happened?
(2) What were the consequences?
(3) Why did it happen (i.e., what were the causes)?

Important features of the detailed retrospective analysis approach include:

- a summary of what happened in the event
- identification of the important functional failures
- an event timeline
- a summary of important human actions and their apparent causes a summary of the important contextual factors (i.e., plant conditions and performance-shaping factors) before, during, and after the event
- an event diagnosis log showing plant conditions and operator responses to them as a function of time

Potential users of the ATHEANA retrospective analysis should be cautioned that this approach has been developed to take advantage of the amount of information typically provided in detailed accounts of events. Experience has shown that there are limited benefits in applying this approach to event reports containing incomplete information. In these cases, the analysts must be willing to do the research necessary to obtain the information needed.

\textsuperscript{42} "Op. cit., 1, NUREG-1624, Rev. 1".
Summary of Prospective ATHEANA Analysis

The prospective ATHEANA process is illustrated in Figure 3, which identifies and summarizes ten major steps in the process (following preparatory tasks, such as assembling and training the analysis team. NUREG-1624, Rev. 143 provides detailed guidance on how to perform Steps 1 through 10 and illustrative examples of how to apply all ten of the process steps are given in Appendixes B through E, of NUREG-1624, Rev. 144.

The ten steps in the prospective ATHEANA process are:

Step 1: Define and interpret the issue

The purpose of this first step is to define the objectives of the analysis being undertaken, i.e., why it is being performed. ATHEANA can support a wide range of HRA applications, from complete PRAs to special studies focused on specific issues. In the nuclear power industry, because most plants have already performed a PRA, the issues for which the PRA will be extended using ATHEANA will usually focus on the significance of human contributions to risk and safety that are particular areas of concern to the NRC or plant management. In such applications, the issue to be addressed usually defines a relatively narrow scope of analysis. In this step, the issue is defined to provide the basis for bounding the scope of the analysis (Step 2) and for other analysis steps.

Step 2: Define the scope of the analysis

This step limits the scope of the analysis by applying the issue defined in Step 1 and, if necessary for practical reasons, further limits the scope by setting priorities on the characteristics of event sequences. Although ATHEANA can be used for both PRA and non-PRA applications, the process for setting priorities is based upon plant-specific PRA models and general concepts of risk significance. The first limitation is to select the initiating event classes and associated, relevant initiators to be analyzed. Later scope restrictions are then considered for each selected initiator, balancing analysis resources against specific project needs.

Step 3: Describe the base case scenario

In this step, the base case scenario is defined and characterized for a chosen initiator(s).

The base case scenario:

- represents the most realistic description of expected plant and operator behavior for the selected issue and initiator
- provides a basis from which to identify and define deviations from such expectations (which will be performed in Step 6)

---

43 "Op. cit., 1, NUREG-1624, Rev. 1”.
44 "Op. cit., 1, NUREG-1624, Rev. 1”.

272
Figure 3. ATHEANA Prospective Search Process
In the ideal situation, the base case scenario:

- has a consensus operator model (COM)
- is well defined operationally
- has well-defined physics
- is well documented in public or proprietary references
- is realistic

Operators and operator trainers provide the information to describe the consensus operator model. This model exists if a scenario is well defined and consistently understood among all operators. Procedures and operator training help to describe the scenario operationally. Documented reference analyses [e.g., plant-specific final safety analysis reports (FSARs) or other detailed engineering analyses of the neutronics and thermal hydraulics of a scenario] can assist in defining the scenario operationally and the scenario physics. The most relevant reference analyses are those that closely match the consensus operator model. The reference analyses may need to be modified to match the consensus model or to be more realistic.

The consensus operator model and reference analyses together form the basis for defining the base case scenario. In the ideal case, the description of the base case scenario should include:

- a list of assumed causes of the initiating event
- a brief, general description of the expected sequence of events, starting before reactor trip (considering key functional parameters such as reactor power, electric power, RCS level and pressure, and core heat removal)
- a description of the assumed initial conditions of the plant
- a detailed description of the expected sequence and timing of plant behavior (as evidenced by key functional parameters) and plant system and equipment response
- the expected trajectories of key parameters, plotted over time, that are indications of plant status for the operators
- any assumptions with respect to the expected plant behavior and system or equipment and operator response (e.g., equipment assumed to be unavailable, single failures of systems assumed to have occurred)
- key operator actions expected during the scenario progression

The description of the base case scenario is the basis for defining deviation scenarios in Step 6. However, in practice, the available information for defining a base case scenario is usually less than ideal.

Step 4: Define HFE(s) and/or UAs

Possible human failure events and/or unsafe actions can be identified and defined in this step. However, Step 1 may have already defined an HFE or UA as being of interest. Alternatively, the deviation analysis, recovery analysis, or quantification performed in later steps may identify the need to define an HFE or UA. Also, recovery analysis or quantification may require development and definition of operator actions at a different level (e.g., unsafe action versus HFE). Consequently, the ATHEANA analysis may require iteration back to this step. To the extent possible, the information
that would be needed in any of these cases is provided in this step.

HFE definitions are based upon the critical functions required to mitigate the accident scenario, expected operator actions, operator actions that could degrade critical functions, and features of the plant-specific PRA model. Unsafe actions are the specific operator actions inappropriately taken or not taken when needed that result in a degraded plant state. Several tables and associated guidance are provided to assist in the definition of HFEs and UAs.

Step 5: Identify potential vulnerabilities in the operators' knowledge base

This is a preliminary step to the searches for the deviations from the base case scenario that are identified in Steps 6 and 7. In particular, analysts are guided to find potential vulnerabilities in the operators' knowledge base for the initiating event or scenario(s) of interest that may result in the HFEs or UAs identified in Step 4. For example, they identify the implications of operator expectations and the associated potential pitfalls (i.e., traps) inherent in the initiating event or scenario(s) that may represent vulnerabilities in operator response.

The information that is obtained in this step should be put on a mental or literal blackboard for use in later steps, especially Step 6. In this way, analysts will be reminded of and guided to the more fruitful areas for deviation searches, based upon the inherent vulnerabilities in the operators knowledge base for the initiator or scenario of interest.

Potential traps inherent in the ways operators may respond to the initiating event or base case scenario are identified through the following:

- investigation of potential vulnerabilities in operator expectations for the scenario
- understanding of a base case scenario timeline and any inherent difficulties associated with the required response
- identification of operator action tendencies and informal rules
- evaluation of formal rules and emergency operating procedures expected to be used in response to the scenario

Step 6: Search for deviations from the base case scenario

The record has shown that no serious accidents have occurred for a base case (or expected) scenario. On the contrary, past experience indicates that only significant deviations from the base case scenario are troublesome for operators. Thus, in Step 6, the analysts are guided in the identification of deviations from the base case scenario that are likely to result in risk-significant unsafe action(s). In serious accidents, these deviations are usually combinations of various types of unexpected plant behavior or conditions.

The search schemes in this step guide the analysts in finding physical or "physics" deviations, which are real deviations in plant behavior and conditions. Analysts may identify performance-shaping factors and explanations for human behavior (e.g., error mechanisms), along with these plant conditions.

Four somewhat overlapping search schemes are used to identify characteristics that should be contained in a deviation scenario. However, each search scheme has a slightly different perspective regarding significant plant or human concerns. These four search schemes are:
(1) identify physical deviations from the base case scenario (e.g., how can the initiator be different?)

(2) evaluate rules with respect to possible deviations

(3) use system dependency matrices to search for possible additional causes of the initiator or the scenario development

(4) identify what operator tendencies and error types match the HFEs and UAs of interest.

After each of the search schemes has been exercised, the analysts should review and summarize the characteristics of a deviation scenario (or potentially important deviations) that were identified in the searches. In ATHENA, the combination of plant conditions (including the deviations), along with resident or triggered human factors concerns, defines the error-forcing context for a human failure event that is composed of one or more unsafe actions. With these combined results, the analysts then develop descriptions of deviation scenarios and associated HFEs or UAs. These deviations also become the initial error-forcing context for the HFEs or UAs. Step 7, builds upon or refines this initial EFC definition by identifying other possible complicating factors (including possible hardware failures) and resident or triggered human factors concerns (e.g., mismatches between deviant plant behavior or conditions and procedures or other job aids).

Step 7: Identify and evaluate complicating factors and links to PSFs

This step expands and further refines the EFC definition begun in Step 6 by considering:

- performance-shaping factors
- additional physical conditions, such as:
  - hardware failures, configuration problems, or unavailabilities
  - indicator failures
  - plant conditions that can confuse operators
  - factors not normally considered in PRAs

Like Step 6, this step may need to be performed iteratively with quantification (Step 9). In particular, the judgments that analysts will need to make regarding how many complicating factors to add to the EFC are best based upon the quantification considerations.

Step 8: Evaluate the potential for recovery

In this step, the definitions of HFEs and the associated EFCs are completed by considering the opportunities for recovering from the initial error(s) (or more precisely not recovering from initial errors). Performance of this step, perhaps even more so than previous search steps, is linked to issues considered in quantification. Consequently, some iteration between this step and the quantification step is possible. Also, since the consideration of the opportunities for recovery will involve extending the context defined in previous deviation search steps, recovery analysis also is iterative with Steps 6 and 7. The analysts are provided with guidance to identify the additional contextual factors (e.g., new cues for action or new plant symptoms) that might aid operators in recovering from their initial inappropriate actions. If an HFE can be ensured to be recovered, the analysis stops and proceeds to issue resolution. If recovery cannot be ensured, then the analysis proceeds according Step 9.
Step 9: Quantify the HFE probability

In this step, the probabilities of the human failure events (and associated unsafe actions) that have been identified and defined in the previous steps are quantified. ATHEANA requires a somewhat different approach for quantification from those used in earlier HRA methods. Where most existing methods have assessed the chance of human error occurring under nominal accident conditions (or under the plant conditions specified in the PRAs event trees and fault trees), quantification in ATHEANA becomes principally a question of evaluating the probabilities of specific classes of error-forcing contexts within the wide range of alternative conditions that could exist in the scenario, and then evaluating the conditional likelihood of the unsafe action occurring, given the occurrence of the EFC. The overall probability of the HFE also takes into account the potential for recovery and its associated contextual factors and potential mismatches.

Human failure events are quantified by considering three separate but interconnected stages:

(1) the probability of the EFC in a particular accident scenario
(2) the conditional likelihood of the UAs that can cause the human failure event
(3) the conditional likelihood that the UA is not recovered prior to the catastrophic failure of concern (typically the onset of core damage as modeled in the PRA)

Step 10: Incorporate the HFE into the PRA

After human failure events are identified, defined, and quantified, they must be incorporated into a PRA. When using ATHEANA, this process is generally identical to that already performed in state-of-the-art HRAs. Guidance for certain ATHEANA-specific incorporation issues is provided.